SOC-ELK.

Documentación, implementación y puesta en marcha de un Servicio SOC para ayuntamientos.

Juan Miguel Rosa Mondragón

Máster en ciberseguridad y privacidad.

Seguridad en redes y sistemas.

Erik de Luis Gargallo
Jordi Serra Ruiz

Universitat Oberta de Catalunya

Enero de 2024

A) Creative Commons:

B) GNU Free Documentation License (GNU FDL)

C) Copyright

AGRADECIMIENTOS

“Porque la gratitud, aun siendo un ingrediente secreto, en silencio no sirve a nadie”.

A mi queridísima mujer Maitane Uranga, por todo el apoyo, la paciencia y el amor infinito dedicado a hacerme feliz y por ser mi inspiración en los momentos más difíciles. Tu compañía y tiempo es mi mayor tesoro.

A mis abuelos, padres y hermano, por estar siempre firmes en la proeza que supone caminar por la vida. Por su amor incondicional, su guía y su ejemplo constante de fortaleza y sabiduría.

A mi querido amigo y estimado socio Fernando Romero, por su incondicional apoyo, confianza y trabajo en equipo. Por caminar juntos en cada reto, alineando visiones y convirtiendo cada desafío en una posibilidad de crecimiento.

A aquellos que nos han dejado, permanecerán eternamente en nuestros recuerdos y en lo más profundo de nuestros corazones.

A todos ellos, mi más profundo agradecimiento.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*SOC – ELK. Documentación, implementación y puesta en marcha de un servicio SOC para ayuntamientos.*
Nombre del autor:	*Juan Miguel Rosa Mondragón.*
Nombre del consultor/a:	*Erik de Luis Gallardo.*
Nombre del PRA:	*Jordi Serra Ruiz.*
Fecha de entrega (mm/aaaa):	*01/2024*
Titulación o programa:	*Máster Universitario en Ciberseguridad y Privacidad.*
Área del Trabajo Final:	*Seguridad en redes y sistemas.*
Idioma del trabajo:	*Castellano.*
Palabras clave	*SOC, ELK, Ciberdefensa.*

Resumen del Trabajo

En la era digital contemporánea, la Administración Pública, en particular los ayuntamientos, gestiona un volumen creciente de información sensible relacionada con sus ciudadanos. La necesidad de proteger esta información de amenazas cibernéticas es primordial. Sin embargo, al igual que las PYMEs, muchos ayuntamientos enfrentan limitaciones presupuestarias, lo que dificulta la adopción de soluciones de seguridad sofisticadas.

El SOC (Centro de Operaciones de Seguridad) es una instalación donde se monitorizan y gestionan las amenazas de seguridad en tiempo real.

En este trabajo, se documenta, implementa e implanta un servicio SOC utilizando la “ELK Stack”, compuesta por los productos “Elasticsearch”, “Logstash” y “Kibana” y especialmente diseñado para ayuntamientos. ELK proporciona una plataforma robusta y escalable para analizar, monitorizar y visualizar datos en tiempo real, permitiendo a los ayuntamientos detectar y responder rápidamente a amenazas potenciales.

A través de esta implementación, se busca fortalecer la infraestructura de TI de los ayuntamientos, proporcionando herramientas para prevenir brechas de seguridad y garantizar la confidencialidad, integridad y disponibilidad de los datos ciudadanos. Esta propuesta es una respuesta proactiva a las crecientes amenazas cibernéticas, asegurando una Administración Pública más resiliente y confiable.

Abstract

In today's digital era, public administration, particularly municipalities, manages a growing volume of sensitive information related to its citizens. The need to safeguard this information from cyber threats is paramount. However, much like SMEs, many municipalities face budgetary constraints, making it challenging to adopt sophisticated security solutions.

The SOC (Security Operations Center) is a facility where security threats are monitored and managed in real-time. In this paper, we document, implement, and launch a SOC service using the ELK stack (Elasticsearch, Logstash, and Kibana) specially designed for municipalities. ELK provides a robust and scalable platform to analyze, monitor, and visualize real-time data, allowing municipalities to detect and rapidly respond to potential threats.

Through this implementation, the aim is to bolster the IT infrastructure of municipalities, offering tools to prevent security breaches and ensure the confidentiality, integrity, and availability of citizen data. This proposal is a proactive response to the rising cyber threats, ensuring a more resilient and trustworthy public administration.

Índice

Lista de figuras

1. Introducción.

Los Sistemas de Operaciones de Seguridad (SOC) han evolucionado para convertirse en una herramienta indispensable para organizaciones, incluidos los gobiernos locales y municipales. Así pues, su objetivo principal es proporcionar una visión en tiempo real de la seguridad y supervisar activamente las amenazas, facilitando una respuesta oportuna a cualquier incidente de seguridad.

Cabe destacar que los SOC de los ayuntamientos actualmente enfrentan el desafío de integrar diversas fuentes de datos y alertas de seguridad en una plataforma unificada y eficaz. Además, la falta de una solución integrada impide una respuesta rápida y eficiente a las amenazas, lo que puede conducir a vulnerabilidades y posibles infracciones de seguridad.

El “Elastic Stack”, a partir de ahora en este documento referido como ELK por sus componentes principales: Elasticsearch, Logstash y Kibana, ha ganado un puesto relevante en el panorama de los SOC gracias a su capacidad para procesar, analizar y visualizar grandes volúmenes de datos en tiempo real. Estas características son esenciales para cualquier SOC que busque identificar patrones y correlaciones entre distintos eventos de seguridad, ya que permiten a las organizaciones combinar múltiples fuentes de datos en un solo punto, mejorando la eficiencia en la detección y respuesta a amenazas. Adicionalmente, hay que decir que la integración de sistemas IDS e HIDS complementan la eficacia del ELK, proporcionando una nueva capa de seguridad.

En el contexto de los ayuntamientos se pueden destacar los siguientes puntos:

1. **Adopción**: A medida que los ayuntamientos se digitalizan y se vuelven más dependientes de las infraestructuras de TI, la necesidad de un SOC se vuelve evidente. La implantación de herramientas como ELK se está considerando cada vez más como una solución escalable y rentable para las entidades públicas.
2. **Desafíos específicos**: Los ayuntamientos manejan una cantidad significativa de datos personales y otras informaciones sensibles, lo que los convierte en objetivos atractivos para los ciberdelincuentes. Además, con limitaciones presupuestarias y de personal, la implementación de un SOC puede ser desafiante. ELK, por su naturaleza de código abierto y flexibilidad, supone una solución adecuada y asequible para enfrentarse a estos desafíos.
3. **Normativas y regulaciones**: Con la creciente preocupación por la privacidad de los datos y la ciberseguridad, han surgido regulaciones y directrices específicas en diferentes regiones. Estas regulaciones pueden influir en cómo se implementa y opera un SOC dentro de un ayuntamiento. Por ello, se deberá cumplir con el Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD).

Mientras que muchas organizaciones han adoptado soluciones basadas en la nube, los enfoques híbridos o el enfoque "on-premise" sigues siendo relevantes, especialmente para entidades gubernamentales que pueden tener preocupaciones de seguridad y privacidad específicas. En este contexto, el TFM propuesto no solo se alinea con las tendencias actuales en ciberseguridad, sino que también aborda las necesidades específicas y desafíos de los ayuntamientos.

En cuanto al estado del arte de SOC ELK en ayuntamientos, se desarrollará en el siguiente punto de este documento en profundidad. Aunque sigue habiendo desafíos, especialmente en lo que respecta a la adopción y la formación, y aparecerán nuevos, la tendencia indica un movimiento hacia una mayor adopción de este tipo de soluciones en el entorno municipal.

Figura 1: Elasticsearch, Logstash, and Kibana.

1.1. Análisis del estado del arte actual sobre la monitorización de alertas en el ámbito público.

A lo largo de la última década, la digitalización y la informatización de la Administración Pública han crecido exponencialmente. Los ayuntamientos, en especial, se han visto en la necesidad de actualizar sus sistemas para responder a las necesidades de una población cada vez más orientada hacia lo digital. Esta evolución ha llevado a una creciente necesidad de herramientas que monitoricen y gestionen las vastas cantidades de datos y alertas generadas por estos sistemas digitales.

A continuación, se exponen los aspectos más relevantes que trazan la historia y evolución hasta el presente del estado del arte en cuestión.

a) Antecedentes históricos.

La transformación digital de las administraciones públicas ha sido un proceso gradual y complejo. Durante la mayor parte del siglo XX, la mayoría de las instituciones gubernamentales operaban en plataformas analógicas y manuales. Estos sistemas tradicionales, aunque eficientes para su tiempo, carecían de la capacidad de integrarse entre sí y solían ser propensos a errores y demoras.

Con el inicio del siglo XXI y principalmente por la entrada en vigor de los siguientes decretos Ley y leyes:

- El Real Decreto Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en la que se contempla el registro electrónico de apoderamientos, el registro electrónico, el registro de empleados públicos habilitados, el punto de acceso general electrónico de la Administración y archivo único electrónico.
- La Ley 39/2015, de 1 de octubre, se refiere, entre otras, a cuestiones tales como los derechos de las personas en sus relaciones con las AA.PP; la asistencia en el uso de medios electrónicos; los registros electrónicos; los sistemas de identificación de los interesados en el procedimiento; la práctica de las notificaciones a través de medios electrónicos; la emisión de documentos por las AA.PP. ; la validez y eficacia de las copias realizadas por las AA.PP.; los documentos aportados por los interesados; y el archivo de documentos.
- El Real Decreto Ley 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

Se reconoció el derecho de las personas a relacionarse con las AA.PP. por medios telemáticos. Este reconocimiento del derecho supuso una obligación de las AA.PP. de proveer de los medios necesarios para que las personas puedan ejercer su derecho.

Esto obligó a prácticamente todos los organismos públicos a integrarse a marchas forzadas con el software que ofrece la Administración General del Estado (AGE) o a desarrollar con la misma urgencia todas las herramientas necesarias contempladas en la legislación (Registro, Sede Electrónica, mecanismos de Notificación Telemática, mecanismos de firma digital, etc.)

En paralelo, con la digitalización creciente de las operaciones, el aumento en el volumen de datos y la complejidad de los sistemas se hizo patente. Esta evolución desencadenó una necesidad imperante de herramientas capaces de supervisar, analizar y administrar estos datos eficazmente. Sumado a ello, el aumento de amenazas cibernéticas y la exigencia de una mayor transparencia subrayaron la imperiosa demanda de sistemas de monitorización avanzados.

En este escenario, surgen herramientas como ELK (Elasticsearch, Logstash, Kibana), que ofrecen soluciones integradas para el análisis, búsqueda y visualización de datos en tiempo real. Estas herramientas no solo proporcionan una visión detallada del estado de los sistemas, sino que también permiten una rápida detección de incidentes y amenazas.

b) Evolución en el ámbito público.

La transformación tecnológica, al ser obligatoria, no pudo obviarse en el ámbito público. Los municipios se vieron impulsados a integrar soluciones que cumplieran con la legalidad vigente y mucho más sofisticadas que las que tenían

en ese momento. En este escenario, ELK, como conjunto de herramientas integradas, surgió como una respuesta eficiente para explorar y analizar extensos volúmenes de datos. Las administraciones locales empezaron a percibir las ventajas de ELK, especialmente en la detección proactiva de riesgos, la gestión del flujo vehicular y la reacción inmediata ante situaciones adversas.

Esta adopción de ELK en el sector público se reflejó en ciertos casos de éxito, como por ejemplo el caso de "Aragón open data" del Gobierno de Aragón (Alcober Fuertes, 2020), u otras ciudades que implementaron ELK para monitorizar la eficiencia energética, optimizar los sistemas de transporte público y anticipar escenarios de crisis.

A continuación, se detalla brevemente las dos fases más destacadas en cuanto a la evolución en el ámbito público.

- **Inicios (2000-2010):** Durante este periodo, las instituciones públicas se enfocaron en el cumplimiento del RDL 11/2007, creando oficinas virtuales, sedes electrónicas, informatizando procedimientos y poniéndolos a disposición del ciudadano. En contados casos, como puede ser Hacienda, cuya informática ha aventajado siempre al resto de la Administración, siguieron trabajando en el análisis de grandes volúmenes de datos para encontrar casos de posible fraude. Las soluciones existentes resultaban costosas y poco intuitivas. Sin embargo, ELK, aún en sus fases iniciales, se destacó por su naturaleza de código abierto y su capacidad para gestionar grandes volúmenes de información.
- **Expansión y consolidación (2011-2018):** Con el incremento sustancial de datos originados por los servicios municipales, emergió la necesidad de herramientas más eficaces y específicas. Durante este periodo, ELK no solo avanzó en sus funcionalidades, sino que también incorporó características de seguridad más avanzadas, facilitando su integración efectiva y segura en sectores críticos como el de la administración gubernamental.

La tendencia hacia la digitalización trajo consigo retos adicionales:

- **Cumplimiento de reglamentación pública:** En concreto del Esquema Nacional de Seguridad (ENS) en el nivel que aplique y del Esquema Nacional de Interoperabilidad.
- **Conciencia sobre la seguridad:** Los ciberataques, al volverse más sofisticados, revelaron la importancia de sistemas de monitorización avanzados. Soluciones como ELK brindaron a las entidades públicas la capacidad de detectar y responder a amenazas en tiempo real, garantizando la protección de datos vitales.
- **Demanda de transparencia:** En un mundo interconectado, los ciudadanos exigieron mayor transparencia y rendición de cuentas. Las herramientas de monitorización, como ELK, proporcionaron una visión sin parangón de las operaciones internas de las administraciones municipales. Esta transparencia facilitó una toma de decisiones informada y reforzó la confianza con la comunidad. A través de la visualización de

datos y métricas en tiempo real, los residentes pudieron tener un acceso más directo y comprensible a la información pública, fomentando la participación ciudadana y la colaboración con la administración.

- **Adaptabilidad y versatilidad de ELK:** La dinámica singular de cada municipalidad requería soluciones que pudieran adaptarse a diferentes contextos. ELK demostró ser una herramienta versátil, siendo implementada tanto en pequeñas localidades como en extensas ciudades cosmopolitas. Su capacidad para ajustarse a diferentes volúmenes de datos y requerimientos específicos hizo que se destacara entre otras herramientas del mercado.

A medida que avanzaba la digitalización, las administraciones públicas reconocieron la imperativa necesidad de evolucionar con ella. Las soluciones como ELK no solo respondieron a la demanda de analizar y gestionar vastos conjuntos de datos, sino que también abordaron problemas emergentes en seguridad y transparencia. La adopción de tales herramientas simboliza un paso adelante hacia una administración más eficiente, transparente y participativa.

c) Casos de uso y aplicaciones.

A continuación, se muestran los casos de uso y aplicaciones del estado del arte actual:

- **Seguridad y prevención:** Los ayuntamientos utilizan ELK para detectar patrones anómalos y posibles brechas de seguridad en tiempo real, lo que permite una respuesta rápida a las amenazas.
- **Gestión de servicios públicos:** La monitorización de servicios como la gestión de residuos, transporte público y suministros municipales se ha simplificado con ELK, permitiendo un análisis detallado y la optimización basada en datos.
- **Transparencia y rendición de cuentas:** Algunos ayuntamientos han empleado ELK para analizar y presentar datos públicos en dashboards accesibles a los ciudadanos, promoviendo la transparencia y la participación cívica.

d) Relación con la investigación actual.

La evolución de las tecnologías y la creciente complejidad de los sistemas han subrayado la importancia de la monitorización de sistemas y redes en las últimas décadas. Este énfasis se ve reforzado por la urgencia de desarrollar soluciones avanzadas capaces de manejar y analizar grandes volúmenes de datos.

El enfoque de investigación en monitorización siempre ha apuntado hacia la optimización de la detección de eventos atípicos o anómalos, buscando mejorar en términos de eficiencia, rapidez y precisión. Paralelamente, se ha observado un incremento en investigaciones que buscan integrar la inteligencia artificial y el aprendizaje automático con el propósito de anticipar y reconocer amenazas en tiempo real.

Otro aspecto a tener en cuenta en cuanto a la adopción de las nuevas tecnologías es que, aunque el sector privado ha adoptado rápidamente las innovaciones tecnológicas, la Administración Pública ha avanzado de manera más cautelosa en este aspecto. Sin embargo, se observa una tendencia positiva en la adopción de herramientas avanzadas de monitorización por parte de la Administración Pública, aunque cabe destacar que existe una falta notable de investigación y estudios concretos sobre cómo se está adaptando y utilizando ELK en el sector público, ya que debido a las regulaciones especiales, necesidades de privacidad y requerimientos de transparencia que lo caracteriza, se necesita un análisis más profundo y específico para aplicar estas tecnologías en dicho ámbito.

Así pues, el propósito de esta investigación y de sus trabajos futuros es abarcar no sólo aspectos técnicos de implementación, sino también identificar y comprender los desafíos a nivel organizativo, político y social inherentes a la incorporación de estas herramientas en la Administración Municipal. Cabe destacar que:

- Los ayuntamientos, con sus distintos desafíos y requisitos, necesitan soluciones a medida. Así pues, esta investigación servirá para conocer la adaptabilidad que presenta ELK ante las demandas generales de los ayuntamientos.
- Con el paso del tiempo, herramientas como ELK han experimentado una constante evolución, ampliando sus características y optimizando su funcionalidad. Así pues, es esencial en esta investigación el comprender cómo estos avances pueden ser utilizados para el beneficio de los ayuntamientos.

e) Aportación de la investigación.

El proyecto "Master SOC on BOX" tiene como objetivo cubrir las carencias presentes tanto en la literatura como en la práctica actual, adaptando y personalizando las funcionalidades del ELK Stack para atender de manera específica las necesidades de los ayuntamientos.

Si bien existen numerosos estudios y aplicaciones del ELK Stack en diferentes industrias, hay una falta relativa de investigación enfocada específicamente en su aplicación en el ámbito público y, más concretamente, en el nivel municipal. Este proyecto, por lo tanto, puede servir de precedente y tomarse como modelo para otros ayuntamientos y entidades gubernamentales a nivel local.

Al incorporar las mejores prácticas y los últimos avances en monitorización y respuesta a alertas, este proyecto no sólo mejorará la seguridad y eficiencia de las operaciones del ayuntamiento, sino que también contribuirá a la literatura académica y profesional proporcionando un estudio de caso detallado y resultados empíricos sobre la implementación y eficacia de ELK en un entorno público.

En cuanto a desafíos y soluciones que se aportarán durante la investigación, y reflejan las complejidades inherentes al despliegue de sistemas avanzados en un entorno público, destacan los siguientes:

- **Seguridad y privacidad de datos:** Establecer protocolos de seguridad robustos y encriptación de datos. Además, llevar a cabo auditorías de seguridad regulares y fomentar una cultura de privacidad.
- **Escalabilidad y adaptabilidad:** Poner de manifiesto soluciones que permitan escalabilidad y adaptabilidad según las necesidades cambiantes de la administración.
- **Limitaciones presupuestarias:** Hacer uso de soluciones de código abierto o modelos de licencia flexible.
- **Diversidad de datos y fuentes:** Implementar distintas herramientas para la obtención de datos de distinta índole, y para el procesamiento de los mismos.
- **Mantenimiento y actualizaciones:** Establecer un procedimiento para llevar a cabo el mantenimiento y las actualizaciones del ecosistema.

En cuanto a futuras direcciones de esta investigación, destacan las siguientes:

- **Integración multidisciplinaria:** Explorar cómo otras disciplinas, como la sociología, la psicología y la gestión del cambio, pueden influir y enriquecer la adopción y adaptación de herramientas como ELK en la Administración Pública. Esta interacción podría proporcionar una visión importante sobre cómo los usuarios finales interactúan y se adaptan a nuevas tecnologías.
- **Desarrollo de casos de uso específicos:** Investigar casos de uso específicos para la implementación de ELK en diferentes entornos municipales. Esto podría incluir áreas como la gestión de residuos, servicios públicos y gestión del tráfico.
- **Comparativa internacional:** Realizar estudios comparativos sobre la adopción de herramientas de monitorización en ayuntamientos de diferentes países. Esto podría arrojar luz sobre cómo diferentes culturas, regulaciones y estructuras gubernamentales influyen en la adopción tecnológica.
- **Desarrollo sostenible:** Investigar cómo la implementación de herramientas de monitorización puede contribuir a los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas, especialmente en áreas relacionadas con la innovación, infraestructura y ciudades sostenibles.
- **Privacidad y ética:** Abordar cuestiones de privacidad y ética en la implementación de soluciones de monitorización en el ámbito público, especialmente en lo que respecta a la recopilación, almacenamiento y análisis de datos ciudadanos.
- **Evaluación de impacto:** Desarrollar metodologías para evaluar el impacto real de la implementación de sistemas de monitorización en la eficiencia, seguridad y satisfacción ciudadana.
- **Adaptabilidad y escalabilidad:** Examinar cómo las soluciones de monitorización como ELK pueden adaptarse y escalarse para satisfacer

las cambiantes demandas y necesidades de la Administración Pública en el futuro.

- **Colaboración público-privada:** Explorar oportunidades y desafíos de la colaboración entre el sector público y privado en el desarrollo y adaptación de herramientas de monitorización.

Las direcciones anteriores ayudarán a guiar investigaciones futuras, brindando un marco más amplio y una visión más profunda de cómo las herramientas de monitorización, como ELK, pueden ser implementadas y optimizadas en la Administración Pública.

1.2. Contexto y justificación del Trabajo.

- **Necesidad a cubrir:** Con la creciente dependencia de soluciones tecnológicas por parte de los ayuntamientos, se hace necesario el garantizar una infraestructura segura y resistente a los ataques cibernéticos. Esta necesidad se intensifica al considerar la sensibilidad de los datos manejados por estas entidades.
- **Relevancia del tema:** Las consecuencias de un ataque cibernético a un ayuntamiento pueden ser devastadoras, no solo en términos financieros, sino también en la confianza pública y la integridad de datos. Así pues, se concluye que proteger la información es proteger la esencia de la Administración Pública.
- **Estado actual del problema:** Al iniciar el trabajo, muchas municipalidades carecen de soluciones de seguridad avanzadas, y su infraestructura de TI suele ser heterogénea y desactualizada, lo que las convierte en blancos fáciles para los ciberataques.
- **Resultado deseado:** A través de la implementación de un SOC utilizando la ELK Stack, se busca establecer una línea de defensa robusta y proactiva que detecte amenazas y ofrezca soluciones en tiempo real para mitigar riesgos.

1.3. Objetivos del Trabajo.

El objetivo principal de este Trabajo Fin de Máster (TFM) es el de desarrollar e implementar un Centro de Operaciones de Seguridad (SOC) para ayuntamientos, utilizando la ELK Stack, adaptada a las particularidades de la Administración Pública, y mejorando así su capacidad de respuesta y defensa contra amenazas cibernéticas. Para ello se deberá:

- Implementar el Elastic ELK Stack en un servidor “on-premise” para integrarse en el SOC del Ayuntamiento, creando el "Master SOC on Box".
- Integrar diversas fuentes de datos en el ELK, incluyendo antivirus, firewall, sistemas operativos y otras soluciones de protección.
- Incorporar sistemas de detección de intrusiones como Suricata y Wazuh para mejorar la vigilancia y respuesta a amenazas.

Para alcanzar una ejecución exitosa de este trabajo, es esencial satisfacer los siguientes objetivos:

1.3.1 Objetivos de la investigación.

- Entender y definir con precisión qué es un Sistema de Operaciones de Seguridad (SOC).
- Identificar las principales amenazas y desafíos que enfrentan los ayuntamientos en términos de ciberseguridad.
- Reconocer las principales fuentes y vectores de ataques dirigidos a infraestructuras municipales.
- Establecer y proponer las medidas de protección adecuadas que los ayuntamientos pueden implementar, considerando sus recursos y capacidades.
- Elaborar un protocolo estándar para la gestión de incidentes cibernéticos en un entorno municipal.
- Detallar las consecuencias y repercusiones para un ayuntamiento al enfrentar un incidente cibernético.
- Concluir con reflexiones y recomendaciones basadas en el análisis realizado.

1.3.2 Metas de presentación.

- Ejecutar y completar entregas parciales, presentándolas de manera adecuada y en los plazos establecidos.
- Elaborar el informe conclusivo del proyecto final de máster.
- Organizar la presentación del análisis llevado a cabo y la elaboración de un video ilustrativo.
- Realizar el montaje de un laboratorio de pruebas bajo máquinas virtualizadas que sirva como prueba de concepto (PoC) del producto final obtenido.

1.4. Impacto en sostenibilidad, ético-social y de diversidad.

1.4.1 Sostenibilidad.

- **Positivo:** Al implementar soluciones de ciberseguridad como el SOC con la ELK Stack en ayuntamientos, se garantiza una Administración Pública más eficiente y resiliente. Esta resiliencia a largo plazo puede reducir costos asociados con incidentes de seguridad, lo que puede traducirse en una asignación más sostenible de recursos financieros.
- **Negativo:** La puesta en marcha de estas soluciones implica un gasto inicial significativo y aumenta el consumo energético de los centros de datos y servidores involucrados.

1.4.2 Ético-social.

- **Positivo:** La protección de datos personales es un deber legal y ético fundamental. Al robustecer la ciberseguridad, se salvaguarda la

privacidad y la integridad de la información de los ciudadanos, evitando su uso indebido o malintencionado. Además, cabe destacar que se genera confianza en la Administración Pública y se refuerza el compromiso con el bienestar de la sociedad.

- **Negativo:** Si no se gestionan adecuadamente, las soluciones de monitorización y seguridad podrían ser utilizadas de forma no ética para el seguimiento y vigilancia invasiva de individuos, violando derechos fundamentales.

1.4.3 Diversidad.

- **Positivo:** Al establecer protocolos de ciberseguridad robustos, se asegura que todos los ciudadanos, independientemente de su origen, género, edad o capacidad, tengan acceso equitativo a servicios públicos digitales seguros. Esto promueve la inclusión y garantiza que no haya discriminación en el acceso a la información o en la protección de datos.
- **Negativo:** La implementación técnica podría no tener en cuenta la diversidad si no se diseñan interfaces y protocolos accesibles considerando las diferentes necesidades y capacidades de los ciudadanos. Esto podría generar barreras inadvertidas para ciertos grupos e incumplir con la legislación en este aspecto.

1.5. Metodología y enfoque adoptado.

Este TFM se enfoca en el diseño de un plan de implementación y puesta en marcha del “Master SOC on Box”, un Centro de Operaciones de Seguridad para ayuntamientos, así como en la investigación y evaluación de objetivos concretos para la elaboración de dicho plan.

Este proceso se llevará a cabo siguiendo normas, modelos y prácticas que aseguren el éxito de su planificación, desarrollo y puesta en marcha, independientemente de la organización municipal que desee implementarlo. En vista de la necesidad de actuar y reaccionar en entornos impredecibles, la estrategia más efectiva consiste en apoyarse en los principios y prácticas recomendadas de métodos ágiles de probada efectividad que ofrecen soluciones efectivas tanto a nivel tecnológico como empresarial.

Para este propósito, se empleará la metodología ágil Scrum, ya que esta metodología promueve la flexibilidad, la colaboración intensiva y la capacidad de adaptarse a cambios rápidos, lo cual es esencial para el ciclo de vida de la implementación de un SOC. Scrum permitirá dividir el trabajo en “sprints”, períodos de trabajo de dos semanas - un mes, facilitando una iteración rápida y eficiente y la posibilidad de adaptar y mejorar constantemente el plan basado en retroalimentación y cambios emergentes. En cuanto al análisis de los objetivos específicos, se utilizará un enfoque que incorporará técnicas de la metodología ágil Lean para maximizar el valor y minimizar los desperdicios, lo cual es crucial para una investigación orientada a resultados precisos y accionables. Con esta combinación metodológica, se espera alcanzar los más altos estándares de satisfacción en el proyecto sin comprometer la calidad de este.

En referencia a la metodología para el análisis de objetivos particulares y definidos, se empleará una integración de enfoques exploratorios y descriptivos. Así pues, la metodología exploratoria se empleará para profundizar en el contexto de la investigación, clarificar problemas, establecer prioridades y formular posibles hipótesis. Por otro lado, el enfoque descriptivo se utilizará para detallar las particularidades de la investigación, recolectar datos cuantificables y realizar estudios de observación, proporcionando así un análisis más enfocado y detallado de las situaciones estudiadas.

En referencia a la estrategia a llevar a cabo para la realización de este trabajo de implementación de un SOC en ayuntamientos mediante la ELK Stack, se han contemplado los siguientes supuestos:

1. **Desarrollo de un producto completamente nuevo**: Crear un SOC desde cero, diseñado específicamente para ayuntamientos, teniendo en cuenta sus particularidades y necesidades únicas.
2. **Adaptar un producto existente**: Tomar una solución SOC ya existente en el mercado y personalizarla para que se ajuste a las necesidades de un ayuntamiento.
3. **Integración de múltiples productos existentes**: Combinar características de diferentes soluciones SOC disponibles en el mercado para crear una solución compuesta que se ajuste a las necesidades de los ayuntamientos.
4. **Adquisición de una solución SaaS (“*Software as a service*”)**: Optar por una solución SOC como servicio, que se adapte y escale según las necesidades del ayuntamiento, sin la necesidad de gestionar la infraestructura subyacente.

Después de un análisis cuidadoso, optamos por la segunda opción de las indicadas anteriormente, adaptar un producto existente. Esta decisión se basa en las siguientes justificaciones:

- **Costo-eficiencia**: Desarrollar un producto desde cero puede ser costoso y llevar mucho tiempo. Al adaptar una solución ya existente, podemos aprovechar las inversiones y desarrollos previos, reduciendo el costo y el tiempo de implementación.
- **Fiabilidad**: Las soluciones existentes han sido probadas y utilizadas en diversos escenarios, lo que significa que son más confiables y estables que una solución recién creada.
- **Personalización**: Aunque las soluciones existentes están diseñadas para un público más amplio, la adaptación nos permite personalizarla según las necesidades específicas de los ayuntamientos.
- **Soporte y comunidad**: Las soluciones ya existentes normalmente tienen una comunidad activa y de soporte continuo, lo que facilita la resolución de problemas y la adquisición de mejoras.

De esta manera, al adaptar un producto existente se opta por uno de los escenarios que presentan menor riesgo, a la vez que estamos en una posición óptima para conseguir los objetivos del TFM de manera eficiente, confiable y

personalizada, garantizando a su vez un alto nivel de seguridad y operatividad para los ayuntamientos.

1.6. Planificación del Trabajo.

1.6.1. Recursos necesarios.

- **Hardware:**
  - Servidores informáticos de alta capacidad para la instalación de las herramientas que conformarán el “Master SOC on Box”. Detalles del tipo de servidor de altas capacidades aconsejado: “DELL T7810 Workstation 20Cores/40T, 2x Xeon E5-2660 V3, 128GB RAM, SSD, GPU”.

Figura 2: Servidor tipo que albergará la instalación de los productos.

  - Dispositivo “Mikrotik RouterOS”: Es el dispositivo que proporcionará funcionalidades de canalización y enrutamiento de tráfico de red. Presenta una interfaz de configuración intuitiva con gran cantidad de funcionalidades que aprovechar en términos de seguridad de redes empresariales.

Figura 3: Mikrotik RouterOS para labores relativas al tráfico de red.

- **Sistema Operativo:** Basado en Linux para el servidor principal y maquinas adicionales con Windows y Linux para monitorización.
- **Herramientas principales:** Elastic Stack (Elasticsearch, Logstash, Kibana), Suricata como IDS (Sistema de Detección de Intrusos), Wazuh como HIDS (Sistema de Detección de Intrusos en un Host), FortiGate o PfSense como firewall, ElastAlert2 como generador de alertas.
- **Licencias y/o accesos a las soluciones:** Elastic, Logstash, Kibana, Suricata, Wazuh, solución Sophos (Antivirus, XDR, solución de protección a la navegación), Firewall FortiGate o PfSense, sistemas operativos Windows y Linux.

1.6.2. Tareas a realizar.

A lo largo de este proyecto, se llevarán a cabo distintas entregas que conformarán el Trabajo Fin de Máster centrado en la implementación de un SOC (Centro de Operaciones de Seguridad) basado en ELK para ayuntamientos. Los componentes entregables son:

- **PEC 1 - Plan de trabajo**: Esta entrega inicial recogerá las razones para desarrollar un SOC ELK específico para ayuntamientos y los objetivos previstos. Se especificará el enfoque y la estrategia de desarrollo e implementación, y se proporcionará un punto de partida del proyecto.
- **PEC 2 - Entrega de seguimiento**: En esta fase, se abordará la infraestructura del SOC (preparación y configuración del servidor on-premise), y cómo ELK puede ser utilizado para monitorizar y gestionar las amenazas de seguridad en el contexto municipal. Se realizará la instalación y configuración del Elastic Stack, así como la integración de fuentes de datos.

- **PEC 3 - Entrega de seguimiento**: Aquí se profundizará en la implementación del SOC. Se describirá la respuesta adecuada a incidentes de seguridad en un ayuntamiento y cómo el SOC ELK ayuda en la detección y mitigación de estos incidentes. También se tratará la generación y configuraciones de alertas con Suricata, Wazuh y ElastAlert2, así como el diseño de dashboards en Kibana para la visualización de datos.
- **PEC 4 - Memoria final**: En esta entrega, se realizarán pruebas de penetración y análisis de respuestas. De esta manera se discutirán las ventajas y desafíos de mantener un SOC ELK en un ayuntamiento, analizando las implicaciones económicas, operativas y de seguridad básicas. Se presentarán las conclusiones, recomendaciones finales y líneas de trabajo futuras..
- **PEC 5**: Esta entrega se centra en la preparación y grabación de la presentación del proyecto, con miras a su defensa y divulgación posterior.

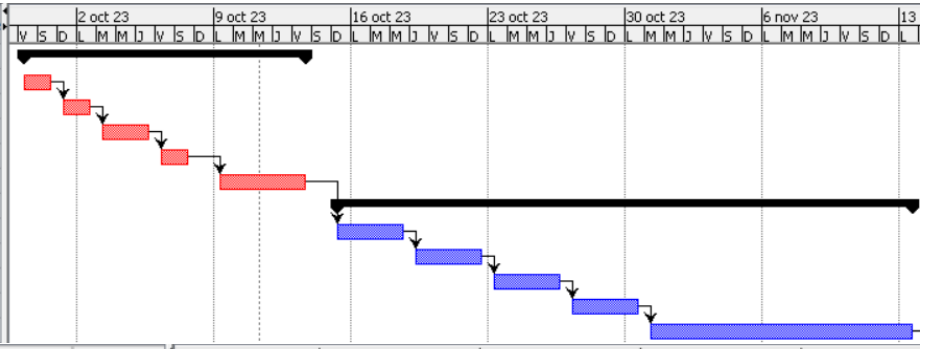
1.6.3. Diagrama de Gantt.

A continuación, se muestra el diagrama de Gantt generado para llevar a cabo los trabajos de este TFM.

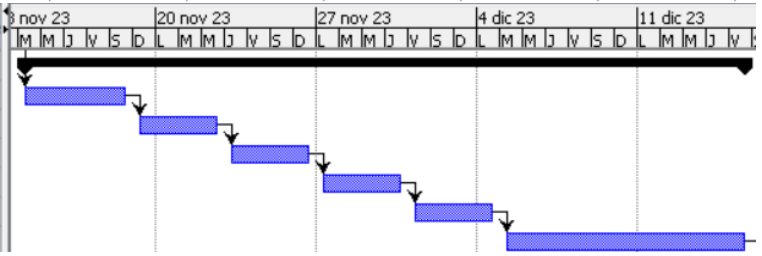
	Nombre	Duracion	Inicio	Terminado
1	**PEC 1 - Plan de trabajo**	**15 days**	**29/09/23 8:...**	**13/10/23 17:00**
2	1. Investigación y documentación	2 days	29/09/23 8:00	30/09/23 17:00
3	2.- Definición de objetivos	2 days	1/10/23 8:00	2/10/23 17:00
4	3.- Determinación del enfoque y estrategia	3 days	3/10/23 8:00	5/10/23 17:00
5	4.- Análisis inicial	2 days	6/10/23 8:00	7/10/23 17:00
6	5.- Elaboración y entrega	5 days	9/10/23 8:00	13/10/23 17:00
7	**PEC 2 – Entrega de seguimiento**	**30 days**	**15/10/23 8:...**	**13/11/23 17:00**
8	1. Diseñoy desarrollo del Master SOC on Box para ayuntamientos	4 days	15/10/23 8:00	18/10/23 17:00
9	2. Preparación y configuración del servidor	4 days	19/10/23 8:00	22/10/23 17:00
10	3. Instalación, configuración e integración del Elastic Stack (Elasticsearch, Logstash, Kibana)	4 days	23/10/23 8:00	26/10/23 17:00
11	4. Instalación, configuración e integración de Wazuh, Suricata y PfSense	4 days	27/10/23 8:00	30/10/23 17:00
12	5. Integración de fuentes de datos	14 days	31/10/23 8:00	13/11/23 17:00
13	**PEC 3 - Entrega de seguimiento**	**32 days**	**14/11/23 8:...**	**15/12/23 17:00**
14	1. Profundización en la implementación	5 days	14/11/23 8:00	18/11/23 17:00
15	2. Descripción de respuesta a incidentes	4 days	19/11/23 8:00	22/11/23 17:00
16	3. Configuración de alertas con ElastAlert2, Firewall, Suricata y Wazuh	4 days	23/11/23 8:00	26/11/23 17:00
17	4. Pruebas de penetración, de malware y funcionamiento del ecosistema	4 days	27/11/23 8:00	30/11/23 17:00
18	5. Documentación de resultados de evidencias obtenidas del punto anterior	4 days	1/12/23 8:00	4/12/23 17:00
19	6. Diseño de dashboards en Kibana	11 days	5/12/23 8:00	15/12/23 17:00
20	**PEC 4 - Memoria final**	**22 days**	**16/12/23 8:...**	**10/01/24 17:00**
21	1. Análisis de las evidencias obtenidas	5 days	16/12/23 8:00	20/12/23 17:00
22	2. Análisis global de los resultados obtenidos en el TFM	4 days	21/12/23 8:00	26/12/23 17:00
23	3. Discusión sobre ventajas y desafíos futuros	5 days	27/12/23 8:00	31/12/23 17:00
24	4. Análisis de implicaciones	3 days	2/01/24 8:00	4/01/24 17:00
25	5 .Conclusiones y recomendaciones	5 days	5/01/24 8:00	10/01/24 17:00
26	**PEC 5 - Preparación y grabación**	**7 days**	**11/01/24 8:...**	**17/01/24 17:00**
27	1. Diseño de la presentación	1 day	11/01/24 8:00	11/01/24 17:00
28	2. Elaboración del guion	1 day	12/01/24 8:00	12/01/24 17:00
29	3. Grabación de la presentación	3 days	13/01/24 8:00	15/01/24 17:00
30	4. Revisión y edición del video	2 days	16/01/24 8:00	17/01/24 17:00
31	**Defensa del TFM**	**9 days**	**18/01/24 8:...**	**26/01/24 17:00**
32	1. Preparación de los materiales y ensayos.	7 days	18/01/24 8:00	24/01/24 17:00
33	2. Revisión final y ajustes.	1 day	25/01/24 8:00	25/01/24 17:00
34	3. Defensa del TFM.	1 day	26/01/24 8:00	26/01/24 17:00

Figura 4: Detalle de planificación de trabajo.

Nombre	Duracion	Inicio	Terminado	Nombre
PEC 1 - Plan de trabajo	15 days	**29/09/23 8:...**	**13/10/23 17:00**	
1. Investigación y documentación	2 days	29/09/23 8:00	30/09/23 17:00	
2.- Definición de objetivos	2 days	1/10/23 8:00	2/10/23 17:00	
3.- Determinación del enfoque y estrategia	3 days	3/10/23 8:00	5/10/23 17:00	
4.- Análisis inicial	2 days	6/10/23 8:00	7/10/23 17:00	
5.- Elaboración y entrega	5 days	9/10/23 8:00	13/10/23 17:00	
PEC 2 – Entrega de seguimiento	30 days	**15/10/23 8:...**	**13/11/23 17:00**	
1. Diseñoy desarrollo del Master SOC on Box para ayuntamientos	4 days	15/10/23 8:00	18/10/23 17:00	
2. Preparación y configuración del servidor	4 days	19/10/23 8:00	22/10/23 17:00	
3. Instalación, configuración e integración del Elastic Stack	4 days	23/10/23 8:00	26/10/23 17:00	
4. Instalación, configuración e integración de Wazuh, Suricata y PfSense	4 days	27/10/23 8:00	30/10/23 17:00	
5. Integración de fuentes de datos	14 days	31/10/23 8:00	13/11/23 17:00	



Nombre	Duracion	Inicio	Terminado	Nombre
PEC 3 - Entrega de seguimiento	32 days	**14/11/23 8:...**	**15/12/23 17:00**	
1. Profundización en la implementación	5 days	14/11/23 8:00	18/11/23 17:00	
2. Descripción de respuesta a incidentes	4 days	19/11/23 8:00	22/11/23 17:00	
3. Configuración de alertas con ElastAlert2, Firewall, Suricata y Wazuh	4 days	23/11/23 8:00	26/11/23 17:00	
4. Pruebas de penetración, de malware y funcionamiento del ecosistema	4 days	27/11/23 8:00	30/11/23 17:00	
5. Documentación de resultados de evidencias obtenidas del punto anterio	4 days	1/12/23 8:00	4/12/23 17:00	
6. Diseño de dashboards en Kibana	11 days	5/12/23 8:00	15/12/23 17:00	



Nombre	Duracion	Inicio	Terminado	Nombr
PEC 4 - Memoria final	22 days	**16/12/23 8:...**	**10/01/24 17:00**	
1. Análisis de las evidencias obtenidas	5 days	16/12/23 8:00	20/12/23 17:00	
2. Análisis global de los resultados obtenidos en el TFM	4 days	21/12/23 8:00	26/12/23 17:00	
3. Discusión sobre ventajas y desafíos futuros	5 days	27/12/23 8:00	31/12/23 17:00	
4. Análisis de implicaciones	3 days	2/01/24 8:00	4/01/24 17:00	
5 .Conclusiones y recomendaciones	5 days	5/01/24 8:00	10/01/24 17:00	
PEC 5 - Preparación y grabación	7 days	**11/01/24 8:...**	**17/01/24 17:00**	
1. Diseño de la presentación	1 day	11/01/24 8:00	11/01/24 17:00	
2. Elaboración del guion	1 day	12/01/24 8:00	12/01/24 17:00	
3. Grabación de la presentación	3 days	13/01/24 8:00	15/01/24 17:00	
4. Revisión y edición del video	2 days	16/01/24 8:00	17/01/24 17:00	
Defensa del TFM	9 days	**18/01/24 8:...**	**26/01/24 17:00**	
1. Preparación de los materiales y ensayos.	7 days	18/01/24 8:00	24/01/24 17:00	
2. Revisión final y ajustes.	1 day	25/01/24 8:00	25/01/24 17:00	
3. Defensa del TFM.	1 day	26/01/24 8:00	26/01/24 17:00	

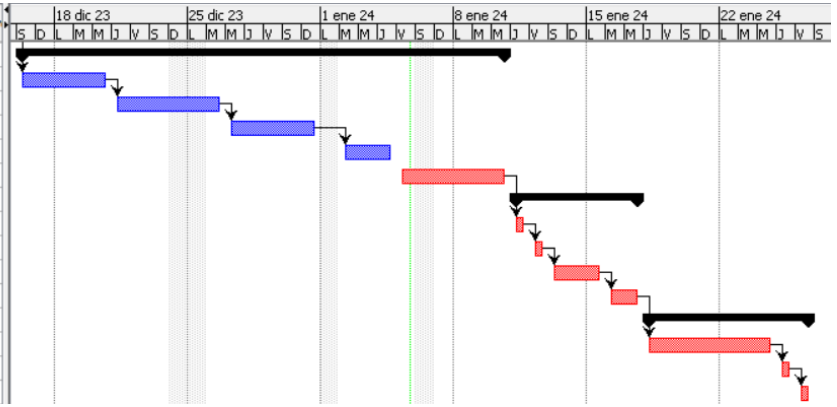


Figura 5: Diagrama de Gantt.

1.7 Estudio económico de la implementación y montaje del "Master SOC on Box".

En los siguientes puntos se presenta el informe económico y su posterior valoración.

1.7.1 Informe económico: Implementación del "Master SOC on Box".

A continuación, se muestra un resumen con los detalles del informe económico realizado para llevar a cabo el proyecto.

Ítem	Coste inicial primer año	Coste anual siguientes años	Amortización anual (5 años)
Infraestructura			
4 Servidores "Master SOC on Box" con SO Linux	€ 14.000,00	€ 0,00	€ 2.800,00
Mikrotik RouterOS	€ 500,00	€ 0,00	€ 100,00
Switch	€ 500,00	€ 0,00	€ 100,00
Licencias de Software			
ELK Stack (ElasticSearch, Logstash, Kibana)	Gratuito	Gratuito	Gratuito
FortiGate-60F. Licencia 24x7 12meses	€ 1.500,00	€ 1.500,00	
PfSense (Firewall / Navegación segura / IPS)	Gratuito	Gratuito	Gratuito
Suricata (IDS)	Gratuito	Gratuito	Gratuito
Wazuh (HIDS)	Gratuito	Gratuito	Gratuito
Elastalert2 (Alertador)	Gratuito	Gratuito	Gratuito
Sophos Antivirus con protección a la navegación - 50 licencias anual	€ 1.900	€ 1.900	-
Sophos EDR (Detección y Respuesta ante Amenazas) licencia anual protección 50 endpoints	€ 4.000,00	€ 4.000,00	-
Trabajos			
Integración y mantenimiento	€ 20.000,00	€ 10.000,00	-
Capacitación y formación - 50 empleados	€ 15.000,00	€ 10.000,00	-
Coste total implementación y primer año	**€ 57.400,00**		
Coste anual años siguientes	-	**€ 27.400,00**	

Figura 6: Detalles económicos del proyecto.

A continuación, se explican los costes y la amortización calculada:

1. **Ítem**: Se refiere a los diferentes componentes o servicios que forman parte del proyecto. Estos se dividen en tres categorías principales: La infraestructura necesaria para llevar a cabo el proyecto, las licencias de software y los trabajos a realizar.
2. **Coste inicial primer año**: Es la inversión inicial necesaria para implementar el proyecto. Incluye el precio de los ítems que requieren un pago único o la primera anualidad en el caso de las licencias recurrentes.
3. **Coste anual siguientes años**: Representa los gastos recurrentes que deberán afrontarse año tras año. Aquí se encuentran, por ejemplo, las

renovaciones de licencias anuales y otros gastos operativos recurrentes, como mantenimiento y formación.

4. **Amortización anual en 5 años**: Se refiere al proceso de distribuir el coste de un activo a lo largo de su vida útil. En este caso, se ha tomado un período estándar de 5 años. Esto significa que, por ejemplo, si compras cuatro servidores por 14.000 euros, en lugar de contabilizar esos 14.000 euros en un solo año, se divide o "amortiza" a lo largo de 5 años, resultando en 2.800 euros al año.

A continuación, se incluye una explicación desglosada de los distintos ítems:

- **Infraestructura**:
    - **Servidores "Master SOC on Box" con SO Linux**: Se tratan de los servidores donde se instalarán las soluciones “ELK Stack”, “FortiGate” o “PfSense”, “Suricata”, “Wazuh”, y “ElastAlert2”. Tiene un coste inicial de 15.500 euros y se amortiza en 3.100 euros anualmente durante 5 años.
    - **Mikrotik RouterOS + Switch**: Son los dispositivos que proporcionarán funcionalidades de enrutamiento de tráfico de red. Tiene un coste inicial de 1000 euros y se amortiza en 200 euros anualmente durante 5 años.

- **Licencias de software**:
    - **ELK Stack, Suricata, Wazuh, ElastAlert2, PfSense**: Estas son soluciones gratuitas, por lo que no tienen coste asociado ni necesitan amortización.
    - **Solución Sophos (Antivirus + EDR + protección a la navegación), FortiGate**: Son licencias anuales. Esto significa que se pagan cada año, por lo que no se amortizan.

- **Trabajos:**
    - **Integración y mantenimiento**: Coste asociado a la integración de las soluciones y el mantenimiento continuo.
    - **Capacitación y formación**: Inversión en formar a los empleados en las nuevas soluciones implementadas.

Cabe destacar que no se han incluido costes asociados con la continuidad y disponibilidad del servicio, bastionado del servidor, y cumplimientos normativos, ya que se considera que estos aspectos están cubiertos por las soluciones y configuraciones del ayuntamiento.

Por último, hay que aclarar que es posible que surjan costes adicionales no previstos, dependiendo de las necesidades específicas del ayuntamiento y cualquier cambio en las condiciones de licencia o precios de los proveedores tanto de software como de hardware.

1.7.2 Valoración económica del proyecto.

A partir del estudio económico proporcionado en el punto “1.7.1 Informe económico: Implementación del Master SOC on Box”, se pueden extraer diversas conclusiones sobre la viabilidad financiera y operativa del proyecto que se detallan a continuación:

- **Gastos iniciales y mantenimiento**: El proyecto tiene un coste inicial de 57.400 euros que cubre la infraestructura necesaria y la implementación inicial. Sin embargo, en los años siguientes, este coste se reduce significativamente a 27.400 euros anuales, lo que representa más de un 50% de reducción en comparación con el primer año.
- **Amortización**: La amortización, aplicada principalmente a la infraestructura de hardware, posibilita la distribución del coste inicial a lo largo de un período de 5 años. Esta estrategia mejora la gestión financiera al evitar un elevado gasto en un único año.
- **Licencias de software**: Un punto a destacar es que la mayoría de las soluciones de software utilizadas son gratuitas. Esto reduce significativamente los costes recurrentes. Las licencias pagadas, como la solución Sophos (Antivirus y el EDR), y la solución FortiGate (Firewall) representan gastos anuales recurrentes, pero no conllevan otros gastos adicionales.
- **Formación e integración**: Una parte importante del presupuesto se destina a la formación y la integración. Esto subraya la importancia de asegurarse de que los empleados estén bien capacitados y que las soluciones se integren adecuadamente.
- **Viabilidad**: Desde un punto de vista financiero, el proyecto es viable, especialmente si se considera la reducción de costes en años posteriores al primero, y teniendo en cuenta que la implantación del SOC es fundamental para asegurar el correcto desarrollo de las actividades del ayuntamiento, tanto en términos de seguridad como de eficiencia operativa.
- **Posibles gastos adicionales**: Es crucial tener en cuenta que podrían surgir costes adicionales no previstos. Esto podría ser debido a cambios en las licencias, actualizaciones de hardware o software, o necesidades adicionales del ayuntamiento.

De todo lo anterior se concluye que el proyecto representa una inversión inicial modesta y bien justificada con el objetivo final de llegar a obtener una infraestructura de seguridad robusta y capacidades mejoradas para el ayuntamiento, que brinda un servicio esencial a los ciudadanos. Así pues, como se indica en el estudio, la planificación financiera es esencial para garantizar la sostenibilidad y viabilidad del proyecto a largo plazo, por lo que es recomendable que el ayuntamiento realice revisiones periódicas de los costes y beneficios para asegurar que el proyecto siga siendo viable y beneficioso a lo largo del tiempo.

1.8 Breve sumario de productos obtenidos.

Al concluir el proyecto, este Trabajo de Fin de Máster (TFM) se convertirá en un manual documentado para la implementación y activación de un Servicio de Operaciones de Seguridad (SOC) dirigido a ayuntamientos, así como para cualquier entidad que, de acuerdo con sus requisitos y juicios particulares, desee llevar a cabo dicha implementación.

A continuación, se presenta un desglose de los diversos productos que se entregarán:

- Memoria final del Trabajo de Fin de Máster (TFM).
- Documentación de implementación y puesta en marcha de un SOC para ayuntamientos.
- Laboratorio virtualizado del "Master SOC on Box" como prueba de concepto (PoC) desarrollado en este Trabajo de Fin de Máster (TFM).
- Presentación de diapositivas del Trabajo de Fin de Máster.
- Presentación en vídeo del Trabajo de Fin de Máster donde se mostrará el correcto funcionamiento del Master SOC on Box mediante la ejecución de pruebas de intrusión, e introducción de malware tipo troyano y ransomware, a la infraestructura del laboratorio.

1.9 Breve descripción de los otros capítulos de la memoria.

Este apartado proporciona un sumario de cada uno de los capítulos que componen la totalidad de este Trabajo de Fin de Máster.

1.9.1 Capítulo 2: Diseño y desarrollo del Master SOC on Box.

En este capítulo se detallan los materiales y las metodologías aplicadas en el diseño y construcción del proyecto. Se discutirán las decisiones adoptadas y los fundamentos que guiaron estas elecciones, delineando la ruta seguida para desarrollar el Master SOC on Box. Del mismo modo, se expondrá una guía que facilitará la implementación y el despliegue de un Servicio de SOC específicamente diseñado para entidades municipales.

1.9.2 Capítulo 3: Resultados.

Este capítulo presenta los resultados finales obtenidos, reflejando el cumplimiento de los objetivos de este Trabajo de Fin de Máster. Se expondrán detalladamente las evidencias obtenidas de las distintas pruebas de penetración e introducción de malware (troyanos, ransomware, etc.) realizadas a la infraestructura del ayuntamiento. Estos resultados pondrán de manifiesto el correcto funcionamiento del Master SOC on BOX.

1.9.3 Capítulo 4: Conclusiones y trabajos futuros.

En este capítulo se reflexiona sobre las inferencias extraídas del trabajo realizado, subrayando las contribuciones significativas y proponiendo líneas de investigación y desarrollo para continuar con la expansión del proyecto.

1.9.4 Capítulo 5: Glosario.

Este capítulo recopila los términos técnicos y especializados utilizados a lo largo del trabajo, proporcionando definiciones claras y concisas para facilitar la comprensión del lector.

1.9.5 Capítulo 6: Bibliografía.

En este capítulo se listan las referencias bibliográficas y fuentes de información que han fundamentado la investigación y servido de soporte teórico y práctico al trabajo desarrollado.

1.9.6 Capítulo 7: Anexos.

Este último capítulo incluye material complementario, documentación adicional y recursos auxiliares que respaldan el contenido y las conclusiones del trabajo.

2. Diseño y desarrollo del "Master SOC on Box" para Ayuntamientos.

El concepto de "Master SOC on box" alude a un diseño concentrado de un Centro de Operaciones de Seguridad (SOC) en el que se integran todas las funcionalidades y herramientas críticas de un SOC convencional en una infraestructura reducida, lo que se traduce en una reducción de costes tanto en la instalación como en la operativa, gracias a su simplificación estructural, manteniendo al mismo tiempo la integridad y seguridad propias de un entorno SOC distribuido.

Así pues, a continuación, se detallan los puntos necesarios para la construcción y puesta en marcha del modelo de SOC propuesto, abarcando desde sus tecnologías, diseños de infraestructura y flujos de la operativa, hasta la implementación práctica y configuración de los sistemas.

2.1 Modelo de SOC propuesto para ayuntamientos.

Teniendo en cuenta los distintos modelos de SOC existentes en el mercado, se considera que, para un ayuntamiento, conociendo sus funciones, la gestión de datos sensibles y la necesidad de garantizar la confidencialidad, integridad y disponibilidad de su información, así como la importancia de garantizar la seguridad de sus ciudadanos y operaciones, se recomienda un modelo de “SOC híbrido”, el cual combina la gestión interna de seguridad con servicios externos especializados. Este enfoque equilibra el conocimiento local con recursos y tecnologías avanzadas, mejorando la protección y respuesta a incidentes de seguridad, a la vez que se controlan costos y se mantiene una gestión eficiente.

Este tipo de SOC cumple los siguientes puntos:

- **Flexibilidad y control**: Un ayuntamiento necesita tener control sobre su información y las operaciones de seguridad para proteger datos sensibles y cumplir con regulaciones locales. Un SOC híbrido permite a la organización mantener el control de ciertos aspectos críticos mientras se beneficia de la experiencia de un proveedor de servicios de seguridad gestionados (MSSP).
- **Costo-eficiencia**: Mantener un SOC dedicado con personal a tiempo completo es costoso. Un SOC híbrido ofrece monitorización 24x7 a un costo reducido, aprovechando tanto los recursos internos como los de un proveedor de servicios de seguridad gestionados (MSSP).
- **Acceso a expertise especializado**: Un proveedor de servicios de seguridad gestionados (MSSP) cuenta con la experiencia de trabajar con múltiples clientes y tener una visión global del panorama de amenazas. Esto es muy valioso para cualquier cliente, ya que podría no contar con ese nivel experiencia de manera interna.
- **Automatización y respuesta rápida**: Como se mencionó anteriormente, la integración de automatización en un SOC híbrido permite una detección

y respuesta más rápidas a incidentes, lo cual es crucial para proteger los datos y servicios públicos.

- **Adaptabilidad a cambios**: Los ayuntamientos pueden experimentar cambios en sus necesidades de seguridad en función de los cambios políticos, reglamentarios o tecnológicos. Un SOC híbrido ofrece la flexibilidad de adaptarse a estos cambios sin tener que realizar grandes inversiones en reestructuraciones internas.
- **Protección de datos sensibles**: Los ayuntamientos manejan información sensible de ciudadanos, por lo que es esencial tener un sistema robusto y seguro. Un SOC híbrido, con la combinación de control interno y expertise externo, puede ofrecer una protección adecuada.

Por todo lo anterior, un SOC híbrido puede ser la opción más adecuada para un ayuntamiento, proporcionando un equilibrio entre control, flexibilidad, expertise y costo-eficiencia. No obstante, la elección entre los distintos modelos de SOC existentes dependerá, como se ha indicado en los puntos anteriores, de factores como el presupuesto disponible, la infraestructura tecnológica del ayuntamiento, y el nivel de experiencia y formación de su personal.

2.2 Tecnologías necesarias para el montaje e implementación del "Master SOC on Box".

A continuación, se detallan las tecnologías de las que constará el SOC en cuestión para llevar a cabo sus labores de operación, vigilancia e inteligencia de amenazas, las cuales se representan en el siguiente esquema.

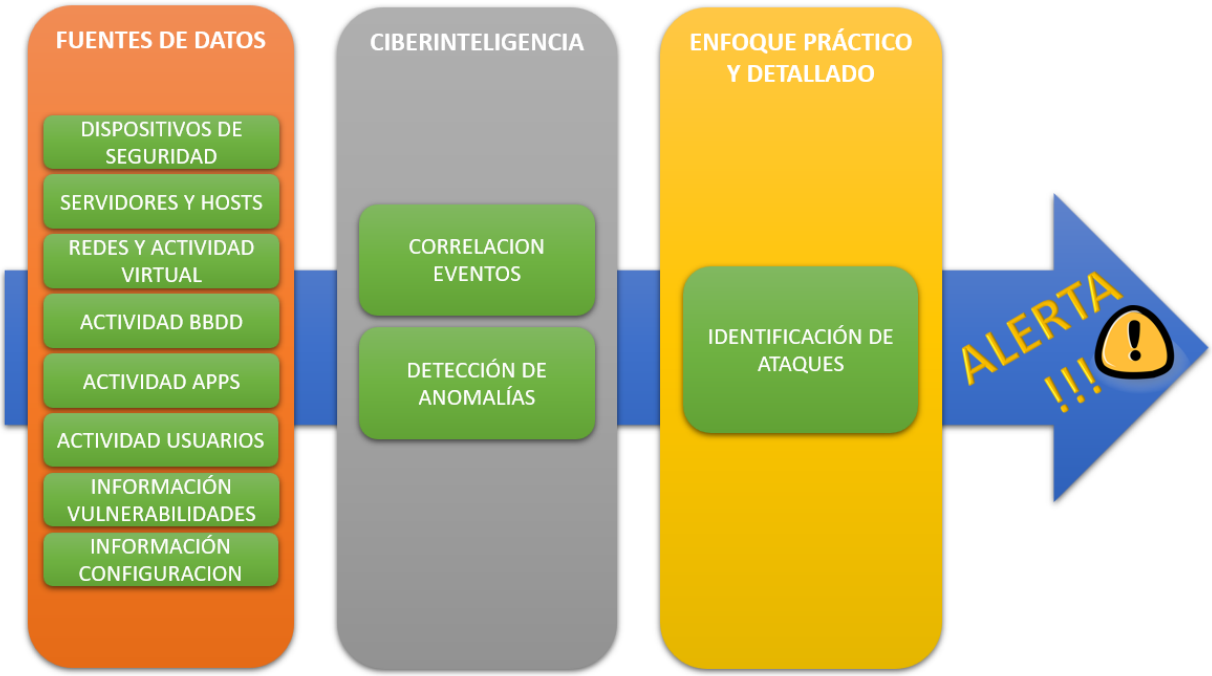


Figura 7: Detalle operacional del SOC.

2.2.1 Sistemas de gestión de información y eventos de seguridad con sistema de alertas (SIEM) – ELK Stack + ElastAlert2.

El elemento SIEM es esencial en la infraestructura del "Master SOC on Box", desempeñando un papel clave en la recolección, estandarización y análisis de información de seguridad originada en distintos puntos de la red municipal. En este contexto, se implementa el ELK Stack, que combina las capacidades de Elasticsearch para un almacenamiento y recuperación de datos óptimos, Logstash como motor de procesamiento y enriquecimiento de eventos, y Kibana para facilitar una visualización dinámica y un análisis exhaustivo en tiempo real.

Además, en la solución anterior se implementa la herramienta “ElastAlert2” para reforzar el sistema con una robusta funcionalidad de alerta, permitiendo la detección proactiva y la notificación de actividades sospechosas o anómalas conforme ocurren.

A continuación, se detalla en mayor profundidad cada uno de los componentes del ELK Stack:

2.2.1.1 Elasticsearch.

Elasticsearch es un potente motor de búsqueda y análisis distribuido de código abierto y construido sobre Apache Lucene. Además, está programado en Java y expone una interfaz REST que interactúa con datos en formato JSON. Este servidor no solo es el núcleo del ELK Stack, sino que también es el eje sobre el que giran Logstash para el procesamiento de datos y Kibana para la visualización y análisis de datos, como veremos en los siguientes puntos.

Elasticsearch constituye el eje central del ELK Stack, ya que gestiona la indexación de datos y su recuperación eficiente a través de búsquedas complejas. Además de su capacidad para manejar grandes volúmenes de datos en tiempo real, destaca por su naturaleza distribuida, donde un clúster se compone de múltiples nodos que pueden alojar índices divididos en “shards”, facilitando así la escalabilidad y la resiliencia. Los índices en Elasticsearch son la unidad básica de almacenamiento que Kibana utiliza para extraer y visualizar datos, proporcionando insights significativos.

Además de lo anterior, cabe destacar que permite realizar operaciones de administración de clústeres y manipulación de índices mediante su API. De este modo, los usuarios pueden ejecutar comandos a través de la línea de comandos o mediante la consola Dev Tools de Kibana, lo que permite realizar tareas como la monitorización del estado del clúster, la gestión de índices y la ejecución de consultas de búsqueda complejas. Además, su robusta arquitectura admite estrategias de particionamiento y réplica, asegurando la integridad y disponibilidad de los datos frente a fallos de nodos.

Para finalizar, conviene decir que la flexibilidad y la eficiencia de Elasticsearch lo hacen ideal para aplicaciones que requieren análisis de logs, búsqueda de texto completo y soluciones de inteligencia de negocios, siendo así una elección

preferente para sistemas SIEM en entornos empresariales y gubernamentales como los ayuntamientos.

2.2.1.2 Logstash.

Logstash es un potente servidor de procesamiento de datos de código abierto que forma parte del ELK Stack. Su arquitectura está diseñada para realizar la captura de datos de diversas fuentes, aplicar transformaciones y filtros a estos datos y, finalmente, enviarlos a Elasticsearch para su almacenamiento y posterior análisis.

Además, Logstash es muy flexible gracias a su capacidad para unir múltiples fuentes y tipos de datos y procesarlos en un flujo unificado, por lo que cabe destacar que, aunque herramientas como Filebeat se han popularizado para la recolección y transferencia directa de logs a Elasticsearch, la herramienta Logstash sigue siendo crucial cuando se requiere un procesamiento más complejo y un enriquecimiento de datos antes de su indexación.

Uno de los aspectos más destacados de Logstash es su sistema de plugins extensible, que incluye más de 200 plugins para conectar y procesar diferentes tipos de datos. Entre ellos, el filtro “grok” de Logstash es especialmente valioso, ya que permite a los usuarios escribir expresiones regulares personalizadas para desestructurar y convertir texto no estructurado en datos estructurados, facilitando así la identificación y el análisis de patrones específicos dentro de los logs.

Además de “grok”, Logstash ofrece otros filtros como “mutate”, “geoip” y “date”, que permiten modificar, enriquecer y transformar los datos a medida que pasan por el pipeline de procesamiento. Esto resulta en una capacidad de análisis más profunda y una integración más rica en el proceso de toma de decisiones basado en datos.

Para finalizar, decir que la flexibilidad de Logstash lo hace ser versátil y eficiente en entornos donde la comprensión precisa y oportuna de los datos es crítica, como en los ayuntamientos, donde puede contribuir a mejorar la seguridad, el rendimiento y la toma de decisiones.

2.2.1.3 Kibana.

Kibana es una herramienta de visualización de datos de código abierto que actúa como la interfaz de usuario del ELK Stack y que es esencial para la interpretación de los datos almacenados en los índices de Elasticsearch. De esta manera, Kibana permite a los usuarios crear visualizaciones complejas y dashboards interactivos a través de una interfaz gráfica intuitiva.

Esta herramienta ofrece funcionalidades adicionales que mejoran la interacción con los datos, como por ejemplo la posibilidad de configurar actualizaciones automáticas, lo que permite a Kibana refrescar y buscar nueva información periódicamente. Asimismo, Kibana posibilita la definición de rangos de tiempo específicos para concentrarse en datos relevantes de un período determinado.

También cabe destacar que Kibana enriquece la experiencia analítica con su consola de comandos propia, accesible a través de las "Dev Tools", que permite ejecutar consultas avanzadas en Elasticsearch y facilitar la gestión de índices o la supervisión del estado del clúster. Así pues, la diversidad de tipos de visualizaciones que Kibana ofrece permite a los usuarios adaptar la visualización a las necesidades específicas de su análisis.

Para finalizar, hay que decir que integrar Kibana dentro del "Master SOC on Box" permite a cualquier organización monitorizar su seguridad de red y operaciones con gran detalle, así como responder a incidentes de seguridad de manera rápida y basada en datos, manteniendo de este modo una postura de seguridad robusta y proactiva.

2.2.1.4 ElastAlert2.

ElastAlert2 es una herramienta de código abierto que proporciona un sistema eficaz para la generación de alertas sobre anomalías, picos o patrones de interés detectados en los datos de Elasticsearch. Cabe destacar que este software se caracteriza por su compatibilidad con todas las versiones de Elasticsearch y por su enfoque en la simplicidad y modularidad.

Esta herramienta, desarrollada para complementar las capacidades de visualización y consulta de datos de Kibana, surge como una solución a la necesidad de alertar sobre inconsistencias detectadas en los datos en tiempo real, por lo que se puede decir que es la herramienta ideal para aquellos escenarios en los que se requiere una notificación inmediata cuando los datos ingresados en Elasticsearch coinciden con ciertos patrones predefinidos.

Además, cabe destacar su diseño confiable y su facilidad de configuración y puesta en marcha, ya que se basa en una estructura de "reglas", que se encargan de definir las consultas a Elasticsearch, establecer los criterios de coincidencia mediante tipos de reglas y determinar las acciones de alerta a ejecutar cuando se detectan dichas coincidencias.

Dentro de ElastAlert2, se incluyen diversos tipos de reglas que abordan paradigmas comunes de monitorización, tales como la detección de frecuencias específicas de eventos, la identificación de aumentos o disminuciones significativas en la tasa de eventos y la observación de la ausencia de eventos durante un período determinado, entre otros. Del mismo modo, ofrece diferentes tipos de alertas como notificaciones por correo electrónico, integraciones con sistemas de gestión de incidentes como “JIRA” y “OpsGenie”, y opciones de mensajería como “Slack” y “Telegram”.

Además, ElastAlert2 se enriquece con características adicionales que amplían su utilidad, como la posibilidad de enlazar alertas con dashboards de Kibana, realizar recuentos agregados de campos específicos, generar informes periódicos y segmentar alertas por campos clave. También se ofrece la capacidad de interceptar y enriquecer los datos antes de que se generen las alertas, permitiendo una respuesta más informada y precisa.

Para finalizar, se puede concluir que ElastAlert2 se establece como una herramienta complementaria indispensable dentro de un ecosistema ELK Stack, permitiendo una respuesta ágil y adecuada ante eventos críticos y asegurando un monitorización continuo y efectivo de los sistemas.

2.2.2 Firewall (PfSense / FortiGate).

El "Master SOC on Box" constará de un firewall “PfSense” o “FortiGate” encargado de filtrar el tráfico de red, controlar los accesos y proteger el perímetro de la red interna de ataques externos. El Firewall también podrá utilizarse para la creación de VPNs y gestión de ancho de banda. Se integrará con el SIEM para centralizar el reporte, la alerta y gestión de incidentes, así como la visualización de los logs que genera.

Como alternativas de firewall a implementar se proponen las siguientes, en base a las necesidades que puedan presentar los ayuntamientos: Cisco ASA, o Check Point.

2.2.3 Sistemas de detección de intrusos (IDS) – Surikata.

El "Master SOC on Box" constará de un IDS que monitorizará el tráfico de red para detectar actividades sospechosas o maliciosas. Suricata está diseñado para trabajar con reglas de detección específicas que permitirán alertar en tiempo real de posibles incidencias. Se integrará con el SIEM para centralizar la alerta y gestión de incidentes.

Como alternativa se propone la siguiente, en base a las necesidades que puedan presentar los ayuntamientos: Snort.

2.2.4 Sistemas de detección de intrusos de host (HIDS) – Wazuh.

El "Master SOC on Box" constará de un HIDS que supervisará y analizará los sistemas host para detectar indicadores de compromiso, cambios no autorizados y vulnerabilidades. Wazuh se integrará con el SIEM para centralizar la alerta y gestión de incidentes.

Como alternativas se proponen las siguientes, en base a las necesidades que puedan presentar los ayuntamientos: OSSEC, Tripwire o AIDE.

2.2.5 Herramientas de protección de puntos finales (EPP) – Antivirus Sophos.

El "Master SOC on Box" constará de soluciones EPP que proporcionarán defensa contra malware, ransomware y otras amenazas en los dispositivos de los usuarios. Estas herramientas incluirán capacidades de prevención, detección y remediación.

Como alternativas se proponen las siguientes, en base a las necesidades que puedan presentar los ayuntamientos: Symantec Endpoint Protection, McAfee Endpoint Security o Bitdefender GravityZone.

2.2.6 Sistemas de protección a la navegación – Incluida en la solución Sophos.

El "Master SOC on Box" constará de sistemas especializados en la seguridad de la navegación web que filtrarán y detectarán páginas web maliciosas y de baja reputación, y protegerán contra malware. A esta solución se le podrá añadir la función de protección de email.

Como alternativas se proponen las siguientes, en base a las necesidades que puedan presentar los ayuntamientos: Confense, Ironscales o Avanan.

2.2.7 Herramientas de detección y respuesta – Sophos EDR.

El "Master SOC on Box" constará de sistemas de detección y respuesta que complementarán al EPP con capacidades avanzadas como análisis de comportamiento, detección de amenazas persistentes y herramientas de investigación y respuesta a incidentes.

En la detección y respuesta se pueden integrar herramientas como CrowdStrike Falcon, SentinelOne, Carbon Black Response o OpenEDR.

2.2.8 Cortafuegos de aplicaciones web (WAF).

El "Master SOC on Box" constará de un WAF integrado en un servidor “Nginx” que se encargará de proteger las aplicaciones web, como Kibana, de ataques tipo inyecciones SQL, Cross-Site Scripting (XSS) y falsificación de solicitudes entre sitios (CSRF), entre otros, mediante el filtrado y monitorización del tráfico HTTP/HTTPS.

2.3 Componentes que integran el “Master SOC on Box”.

A continuación, se enumeran los distintos componentes que integran el “Master SOC on Box”.

1. **Recolección de logs y datos:** Recolecta y almacena logs y eventos de diferentes fuentes, como servidores, aplicaciones, firewalls, dispositivos de red, etc.
2. **Motor de análisis (correlación y reglas):** Analiza los datos recolectados en busca de patrones que puedan indicar un incidente de seguridad.
3. **Gestión de alertas y notificaciones:** Administra las alertas generadas y notifica al personal de seguridad apropiado.
4. **Dashboard y visualización (SIEM):** Proporciona una interfaz gráfica para visualizar eventos, alertas e informes.
5. **Inteligencia de amenazas (Threat Intelligence):** Recopila y utiliza información sobre amenazas emergentes mediante indicadores de

compromiso (IOCs) y TTPs (Tácticas, Técnicas y Procedimientos) de atacantes.

6. **Backup y recovery:** Asegura que los datos del SOC estén respaldados y se puedan recuperar en caso de fallos.
7. **Configuración y mantenimiento:** Herramientas para configurar y mantener el SOC, actualizaciones, parches, etc.

Es importante destacar que, si bien un "Master SOC on Box" puede ser más fácil de implementar y gestionar que un SOC tradicional, puede no ser adecuado para organizaciones muy grandes o con requisitos de seguridad muy específicos. La elección entre un SOC tradicional y un "Master SOC on box" debe basarse en las necesidades y capacidades específicas de la organización, como bien se ha indicado en puntos anteriores.

2.4 Diseño de la Infraestructura para el “Master SOC on box” .

En este apartado se definirá la infraestructura necesaria para implementar en un ayuntamiento el “Master SOC on box”, para monitorizar, analizar y responder a incidentes de ciberseguridad en sus sistemas de TI. Esta infraestructura presentará de manera resumida el siguiente gráfico, el cual se desarrollará en mayor profundidad en los siguientes subapartados.

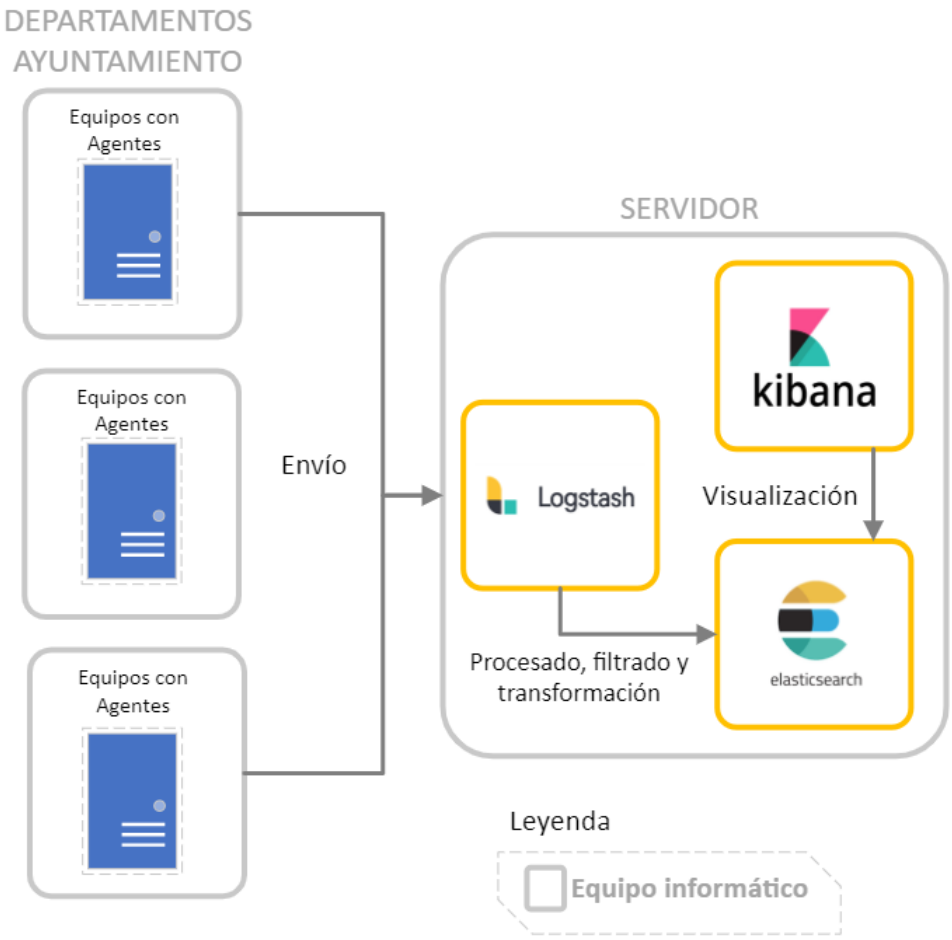


Figura 8: Diagrama básico de infraestructura de “Master SOC on Box”.

Para ello, primeramente, se va a realizar un estudio de los departamentos que consta un ayuntamiento, con la finalidad de poder ajustar de manera adecuada el alcance del SOC.

2.4.1 Descripción de áreas de interés de un ayuntamiento.

Los ayuntamientos pueden variar considerablemente en tamaño y estructura, pero la gran mayoría incluyen una serie de áreas o departamentos comunes que son fundamentales para su funcionamiento.
Así pues, a continuación, se describen los departamentos más comunes y relevantes que deberán ser protegidos mediante la implantación del "Master SOC on Box".

1. **Departamento de informática/Tecnologías de la Información (TI)**: Este departamento gestiona la infraestructura tecnológica del ayuntamiento, incluyendo la red, los servidores y las estaciones de trabajo.
2. **Departamento de administración y servicios financieros**: Este departamento gestiona la contabilidad, la facturación, los pagos y las nóminas.
3. **Departamento de Recursos Humanos (RRHH)**: Este departamento es el responsable de la gestión del personal, reclutamiento, formación y políticas de empleo.
4. **Departamento de seguridad ciudadana y protección civil**: Incluye la policía local, seguridad vial y protección civil, por lo que trabaja con sistemas de vigilancia, control de accesos y sistemas de comunicación de emergencia.
5. **Departamento de urbanismo y obras públicas**: Este departamento se encarga de la planificación urbanística, construcción y mantenimiento de infraestructuras. Consta de sistemas de información geográfica (GIS), permisos de construcción y sistemas de seguimiento de obras.
6. **Departamento de servicios sociales**: Este departamento se encarga de programas de bienestar, asistencia social, y servicios comunitarios. Consta de sistemas de gestión de casos, registros de asistencia y plataformas de interacción ciudadana.
7. **Departamento de educación y cultura**: Este departamento gestiona bibliotecas, centros educativos, eventos culturales y actividades recreativas.
8. **Registro civil y estadística**: Este departamento se encarga de llevar los registros de la población, certificados y estadísticas vitales. Así pues, contienen accesos a bases de datos de registros civiles y solicitudes de documentos.

Cada uno de estos departamentos constituirá un nodo que enviará sus logs a través de agentes seguros hacia el sistema centralizado ELK. En dicho sistema, Elasticsearch almacenará e indexará los logs, Logstash los procesará, y Kibana permitirá visualizarlos y analizarlos. Así pues, las herramientas "Wazuh" y "Suricata" contribuirán con la detección de intrusiones y análisis de seguridad,

mientras que “ElastAlert2” gestionará la alerta en caso de detección de incidentes.

2.4.2 Infraestructura de hardware y red.

A continuación, se muestra el diagrama detallado de la infraestructura propuesta.

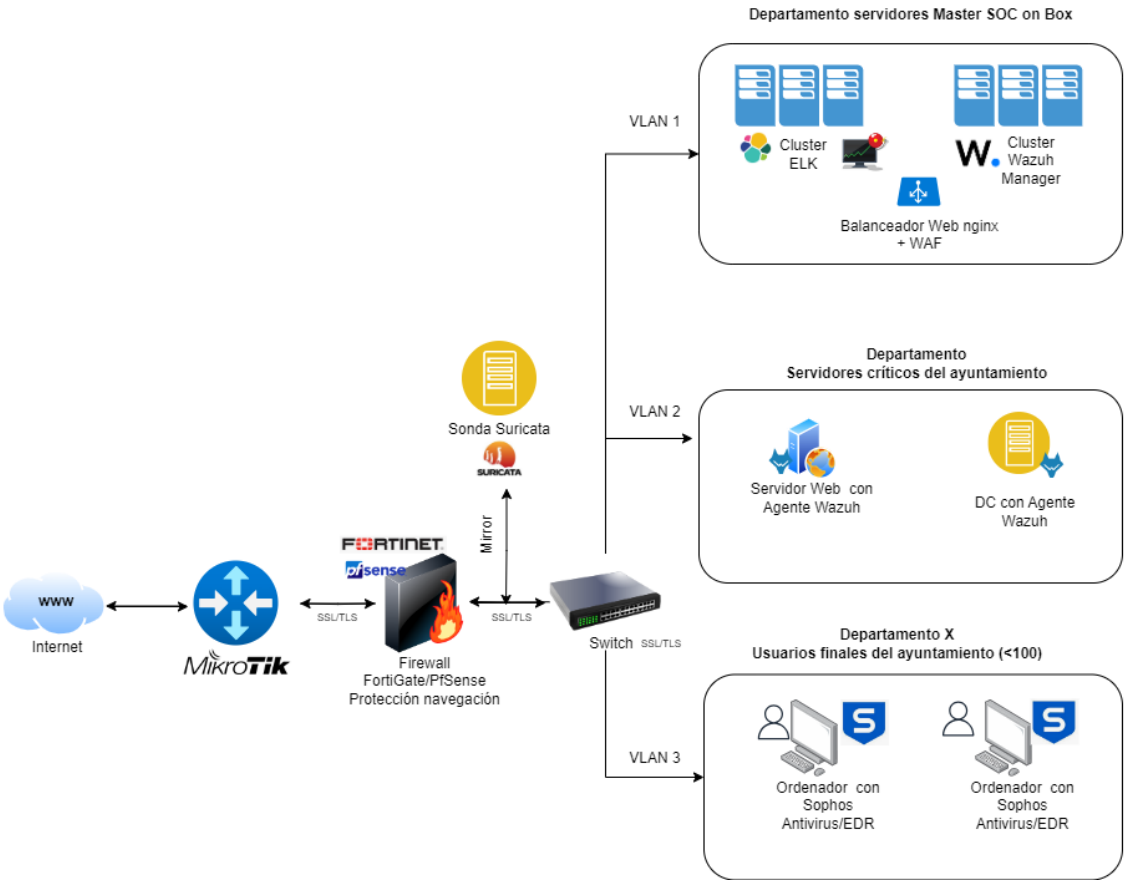


Figura 9: Diagrama de infraestructura de “Master SOC on Box”.

En los siguientes puntos se detallan los distintos componentes que conforman el diagrama de la infraestructura presentada.

2.4.2.1 Componentes principales.

El “Master SOC on Box” constará de clústeres idénticos en cuanto a prestaciones, que garanticen redundancia y alta disponibilidad del SOC en caso de posible fallo.

A continuación, se describen las herramientas instaladas en los distintos clústeres definidos en el diagrama de infraestructura, así como el nodo Suricata para la monitorización de la red municipal.

- **Clúster ELK:**
  - **Elasticsearch:** Este componente actúa como el motor de búsqueda y análisis que proporciona un almacenamiento de

datos escalable y rápido, permitiendo realizar búsquedas complejas en tiempo real y proporcionar visualizaciones de datos para monitorización. Configurado con la herramienta "ElastAlert2" para generar alertas basadas en anomalías o patrones de datos predefinidos.
    - **Logstash:** Funciona como un pipeline de procesamiento de datos en el lado del servidor, que ingiere datos de múltiples fuentes simultáneamente, los transforma y luego los envía a Elasticsearch.
    - **Kibana:** Es la interfaz de usuario de la suite Elastic Stack que permite visualizar datos de Elasticsearch. Ofrece capacidades de visualización y análisis, ayudando a los operadores a comprender los datos complejos a través de gráficos y tableros interactivos.

- **Clúster Wazuh Manager:**
    - **Wazuh Manager:** Encargado de la gestión y análisis de los agentes Wazuh, que ofrecen capacidades de detección de intrusiones y monitorización de integridad, entre otras. Los agentes Wazuh se despliegan en los servidores críticos del ayuntamiento para monitorizar y enviar datos al Wazuh Manager.

- **Nodo Suricata:** Al tratarse de un sistema de detección y prevención de intrusiones (IDS/IPS), este componente necesita interfaces de red de alta velocidad y procesadores rápidos para la monitorización de tráfico en tiempo real, análisis de protocolos y detección de amenazas. Su objetivo es monitorizar el tráfico de la red del ayuntamiento para detectar amenazas y anomalías.

2.4.2.2 Componentes y configuraciones de la arquitectura de red distribuida.

Todos los sistemas definidos en el punto anterior se encuentran interconectados a través de una red segura, con switches gestionables que permiten una configuración detallada de distintas VLAN (virtual LAN) y políticas de seguridad. Además, están monitorizados constantemente para detectar y responder a cualquier indicio de fallo o anomalía en el sistema.

Así pues, a nivel de red la infraestructura se presenta una arquitectura distribuida. Se segmentan los diferentes departamentos del ayuntamiento para proporcionar un aislamiento adecuado y, dentro del propio departamento del SOC, se diferencian entre el servidor que aloja el Elastic Stack y aquellos que ejecutan Wazuh y Suricata. Esta organización se refleja claramente en el diagrama proporcionado y se compone de los siguientes elementos y configuraciones:

- **Router Mikrotik:** Mediante el cual se dirige el tráfico de red de manera eficiente y segura. A través de este dispositivo se aplican políticas de

enrutamiento que fortalecen la seguridad del SOC y se facilita la conexión segura entre los diferentes departamentos y el SOC.

- **Firewalls:** Se implementan firewalls de alto rendimiento para filtrar el tráfico de entrada y salida, creando una barrera robusta contra ataques externos. Además, se utiliza un WAF (Web Application Firewall) integrado con “Nginx” para una capa adicional de protección que salvaguarda el acceso a aplicaciones críticas como Kibana.
- **Switches:** Equipos de networking con funcionalidades avanzadas de administración, configurados para segmentar la red mediante distintas VLAN, lo que permite separar y gestionar el tráfico de la red de manera efectiva, ofreciendo un mejor rendimiento y seguridad.
- **Segmentación:** Se utiliza una VLAN o una red dedicada exclusivamente para el SOC, asegurando que la operación de monitorización y análisis de seguridad esté aislada del tráfico general de la red municipal, minimizando así la superficie de ataque y mejorando el rendimiento.
- **Cifrado de datos:** Se implementa el cifrado TLS/SSL para proteger los datos en tránsito entre los endpoints y el SOC, así como la encriptación de disco para asegurar la información almacenada en los servidores del SOC.
- **Autenticación robusta:** Se integran mecanismos de autenticación fuertes, como LDAP o Active Directory, para verificar las credenciales de los usuarios y administrar el acceso a los sistemas del SOC de manera centralizada.
- **Monitorización de integridad:** Utilización de Wazuh para la constante verificación de la integridad de los sistemas dentro del SOC, lo que permite detectar cambios inesperados o no autorizados en los archivos y configuraciones críticas.
- **Protección de endpoints:** Despliegue de soluciones de protección de punto final (EPP) y herramientas de detección y respuesta (EDR) para prevenir, detectar y responder a amenazas en las estaciones de trabajo y dispositivos conectados a la red municipal.

De esta manera el "Master SOC on Box" ofrecer una vigilancia de seguridad integral, desde la monitorización de amenazas en tiempo real hasta la respuesta rápida ante incidentes, todo ello bajo un entorno controlado y seguro.

2.4.2.3 Redundancia y alta disponibilidad.

Se realiza la configuración de los sistemas del SOC para ofrecer redundancia y alta disponibilidad, incluyendo el balanceo de carga y la duplicación de servicios críticos para asegurar la continuidad operativa ante posibles fallos del sistema. Así pues, se presentan integrados en la infraestructura los siguientes componentes:

- **Balanceadores de carga:** Para distribuir la carga entre servidores y asegurar la disponibilidad del servicio.
- **Clústeres ELK y Wazuh Manager:** Configurados para redundancia y balanceo de carga.

- **Configuración en caliente/frío:** Algunos nodos Elasticsearch pueden estar optimizados para alta carga de trabajo ("calientes") y otros para almacenamiento de datos a largo plazo ("fríos").

En lo que concierne a la escalabilidad, se prevé que para los ayuntamientos el total de endpoints a implementar no excederá los cien. Por tanto, esta cantidad encaja dentro de las capacidades de la infraestructura sugerida, asegurando que se pueda manejar eficientemente sin necesidad de recursos adicionales.

Así pues, se considera que la infraestructura propuesta es sólida y está bien fundamentada para la monitorización de seguridad, análisis de incidentes y respuesta a amenazas en el entorno de un ayuntamiento.

2.5 Diagrama de flujo.

A continuación, se muestra el diagrama de flujo de datos de la infraestructura.

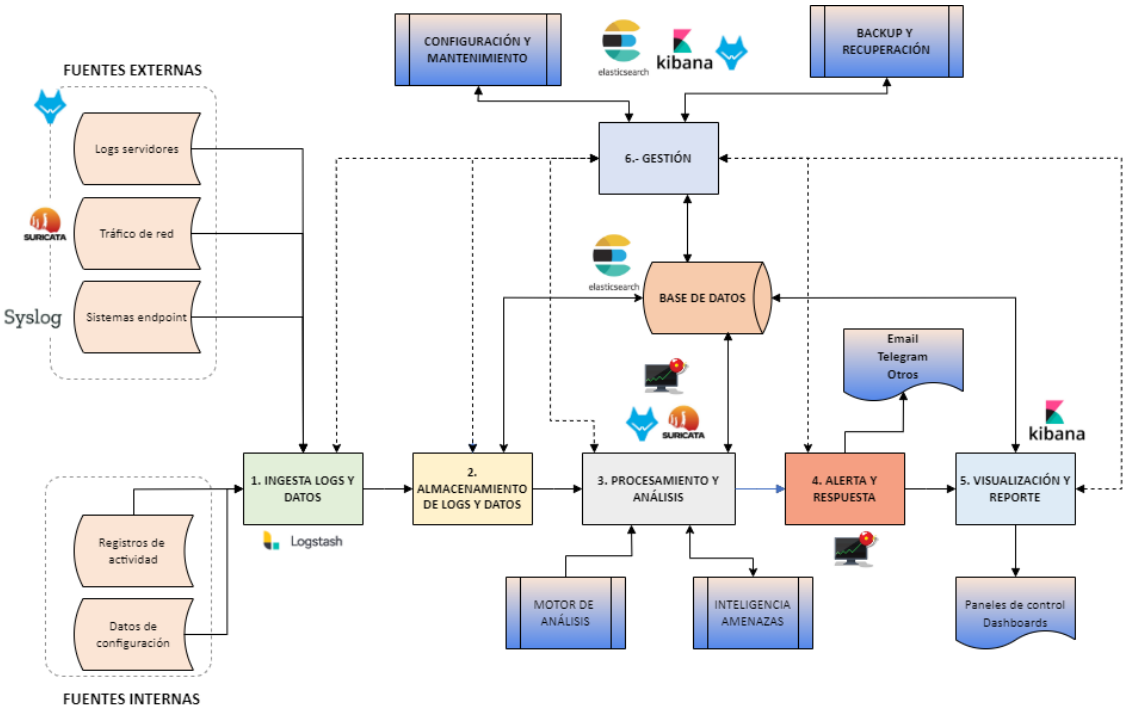


Figura 10: Diagrama de flujo de "Master SOC on Box".

A continuación, se explican los distintos componentes, procesos y elementos lógicos que conforman el diagrama anterior.

1. Entrada de datos: Ingestión inicial de logs y datos.

- **Fuentes externas:** Se trata de logs de servidores, dispositivos de red, sistemas endpoint, aplicaciones, entre otros.
- **Fuentes internas:** Se trata de información generada dentro del SOC, como registros de actividad, datos de configuración, entre otros.

- **Herramientas implicadas:** Wazuh, Suricata, SYSLOG, Antivirus, XDR, FortiGate/PfSense.

2. Recolección y almacenamiento: Agregación y almacenamiento de datos en un formato optimizado.

- **Recolección de datos:** Aquí, se reúnen los datos de las distintas fuentes y se consolidan.
- **Almacenamiento:** Base de datos o solución de almacenamiento centralizado donde se guardarán los datos recolectados.
- **Herramientas:** Elasticsearch.

3. Procesamiento y análisis: Análisis en profundidad de los datos para identificar patrones y amenazas.

- **Motor de análisis:** Procesa la información y busca patrones, correlaciones o eventos inusuales.
- **Threat Intelligence:** Añade información actualizada sobre las últimas amenazas conocidas para mejorar el análisis.
- **Herramientas:** Logstash, Wazuh, Suricata, Sophos.

4. Alerta y respuesta: Alertas basadas en el análisis del paso anterior.

- **Gestión de alertas:** Una vez detectada una amenaza, se generan alertas pertinentes con las que poder dar una respuesta.
- **Herramientas:** ElastAlert2.

5. Visualización y reporte: Representación gráfica de los datos y generación de informes.

- **Dashboard / SIEM:** Interfaz gráfica donde se muestran resúmenes, alertas, métricas y otras informaciones relevantes.
- **Reportes:** Generación automática o manual de informes detallados sobre la actividad y las alertas.
- **Herramientas:** Kibana.

6. Gestión: Administración y monitorización de la salud del sistema.

- **Configuración y mantenimiento:** Herramientas y procesos para mantener actualizado el sistema, realizar ajustes y optimizaciones.
- **Backup y recuperación:** Salvaguardar la información y los datos esenciales y proporcionar mecanismos de restauración en caso de pérdida o corrupción.
- **Herramientas:** Elasticsearch, Kibana, Wazuh.

2.6 Implantación del “Master SOC on BOX”: Preparación, configuración e integración de fuentes de datos.

La preparación y configuración del "Master SOC on BOX" requiere una planificación meticulosa y una implementación detallada, adaptada a las particularidades del entorno municipal, para asegurar que el sistema sea robusto, seguro y adecuado para dicho entorno.

Este apartado se enfoca en establecer un SOC robusto que atienda tanto a las demandas técnicas, como a las políticas de seguridad y transparencia, regulaciones de protección de datos y necesidades específicas del entorno municipal.

Así pues, y como ya se ha mencionado en puntos anteriores de este TFM, la configuración de este SOC incluirá la integración de los componentes clave de seguridad de TI, ajustados para la monitorización precisa y la gestión de alertas en tiempo real, fundamentales para la operativa diaria del ayuntamiento. Del mismo modo, se tomarán medidas específicas para proteger la infraestructura crítica y los datos sensibles, manteniendo un equilibrio entre seguridad y accesibilidad, para facilitar los servicios públicos sin comprometer la privacidad de los ciudadanos.

A continuación, se presentan las directrices clave para este proceso.

2.6.1 Análisis de la implantación en servidores físicos.

La implantación del "Master SOC on Box" en servidores físicos presenta los siguientes beneficios:

- **Control total:** Al alojar el SOC en hardware dedicado, el ayuntamiento tiene control absoluto sobre la infraestructura física, lo que puede mejorar la seguridad y la capacidad de gestión.
- **Rendimiento mejorado:** Los servidores físicos pueden configurarse y optimizarse específicamente para las cargas de trabajo del SOC, proporcionando un rendimiento predecible y de alta velocidad para el procesamiento de datos y el análisis de seguridad.
- **Aumento de la seguridad:** La infraestructura en servidores físicos es, a menudo, menos susceptible a ataques virtuales comunes, como los que afectan a entornos virtualizados o a la nube, debido a la falta de una capa de hipervisor que pueda ser explotada.
- **Personalización de hardware:** Permite la selección de componentes de hardware específicos que se ajusten a las necesidades y requisitos del SOC, como almacenamiento seguro, procesadores rápidos o hardware de red especializado.
- **Independencia de proveedores de terceros:** No hay dependencia de proveedores de servicios en la nube para la operatividad o la disponibilidad de recursos, eliminando el riesgo de interrupciones del servicio externas.
- **Conformidad y regulaciones:** Facilita el cumplimiento de políticas de seguridad estrictas y regulaciones de datos que pueden ser más difíciles de garantizar en entornos compartidos o públicos, como el de los ayuntamientos.

- **Recuperación ante desastres (Disaster recovery):** Permite diseñar e implementar soluciones personalizadas de recuperación ante desastres que se adapten a las necesidades específicas del ayuntamiento sin depender de las opciones limitadas de un proveedor de nube.
- **Disponibilidad y resiliencia:** Posibilidad de diseñar la arquitectura para alta disponibilidad y redundancia, garantizando así la continuidad del servicio incluso en caso de fallos de hardware, como se ha visto en puntos anteriores de este TFM.

La arquitectura final de los servidores físicos puede verse en el punto "2.4.2 Infraestructura de hardware y red", y dicha configuración se mantendrá inalterable, sin verse afectada por la cantidad de endpoints sujetos a monitorización.

Los servidores físicos donde se instalarán las distintas herramientas de las que consta el SOC, constarán de un sistema operativo Linux Ubuntu Server en su última versión, correspondiente a la versión 22.04 en el momento de realizar este TFM. Este sistema operativo destaca por ser seguro y confiable, y por presentar una buena base para todas las operaciones que requiere el "Master SOC on Box" del SOC. Las instrucciones de instalación del sistema operativo indicado se presentan en el anexo A de este documento.

Una vez se tengan los servidores operativos, actualizados y configurados con una dirección IP fija accesible para el resto de los dispositivos del ayuntamiento, se iniciará la instalación de las herramientas del SOC como se detalla en los siguientes puntos.

2.6.2 Instalación, configuración y securización del servidor ELK Stack.

La instalación del ELK Stack se realiza en varias fases que aseguran su correcta ejecución y configuración para el funcionamiento óptimo del sistema.

- **Instalación de Elasticsearch**: Se descarga y configura Elasticsearch, el motor de búsqueda y análisis. Se ajustan los parámetros de configuración, incluyendo la definición del clúster, nodos y configuraciones de red, y se asegura que el servicio se ejecute al inicio del sistema.
- **Instalación de Logstash**: A continuación, se instala Logstash, el componente encargado de procesar los logs y otros datos entrantes. Se definen los flujos de procesamiento, filtrado y salida de datos.
- **Instalación de Kibana**: Por último, se instala Kibana, que ofrece la interfaz de usuario para visualizar y trabajar con los datos indexados en Elasticsearch. Se configura para que se comunique con el nodo de Elasticsearch y se protege su acceso a través de un navegador web.

Durante todo el proceso, se presta especial atención a la configuración de la seguridad y la optimización del rendimiento. Esto incluye ajustes en el archivo de configuración de Elasticsearch ("elasticsearch.yml"), la creación de certificados y claves para la comunicación segura entre nodos y la instalación de "plugins" adicionales como "X-Pack" para seguridad integrada.

Finalmente, se realizan pruebas de conectividad y funcionamiento entre los distintos componentes que conforman la pila ELK y se verifica el correcto funcionamiento del sistema de indexación y visualización de datos. Una vez confirmado que todo está operativo, se procede con la integración de fuentes de datos y la configuración final del SOC.

Las instrucciones de instalación, configuración y securización del ELK Stack se presentan en el anexo B de este documento.

2.6.3 Instalación, configuración e integración del HIDS Wazuh.

Las instrucciones de instalación, configuración e integración de Wazuh en el "Master SOC on Box" se presentan en el anexo C de este documento.

2.6.3.1 De Wazuh Manager (Gestor Wazuh).

Las instrucciones de instalación, configuración e integración del gestor Wazuh en un servidor con Sistema Operativo Linux Ubuntu 22.04 se presentan en el anexo C.1 de este documento.

2.6.3.2 De Wazuh Agent (Agente Wazuh).

Las instrucciones de instalación, configuración e integración del agente Wazuh en un servidor a monitorizar con Sistema Operativo Windows se presentan en el anexo C.2 de este documento.

2.6.3.3 Instalación de Filebeat. Configuración de seguridad entre Wazuh y Elasticsearch mediante el agente Filebeat.

Aunque en el proyecto actual se ha elegido utilizar Logstash por sus altas capacidades como parseador y reenviador de registros a Elasticsearch, es importante proporcionar instrucciones sobre la instalación y configuración segura de la herramienta "Filebeat". Esto se debe a que el uso de "Filebeat" será beneficioso para municipios que necesiten realizar tareas específicas, adaptadas a las decisiones de su personal de tecnologías de la información (IT).

Las instrucciones de instalación y configuración de seguridad entre Wazuh y Elasticsearch mediante "Filebeat" se presentan en el anexo C.3 de este documento.

2.6.4 Instalación, configuración e integración del IDS Suricata.

Las instrucciones de instalación, configuración e integración de Suricata se presentan en el anexo D de este documento.

2.6.5 Instalación, configuración e integración del Firewall.

Las instrucciones de instalación, configuración e integración del firewall PfSense y FortiGate se presentan en el anexo E de este documento.

2.6.6 Integración de endpoints (Antivirus/EDR/Protección navegación).

El objetivo de esta tarea es establecer una integración efectiva de las soluciones de seguridad de endpoints definidas en este TFM, en el entorno del SOC para aportar una visibilidad completa y una respuesta rápida a las amenazas.

Dentro del esquema establecido para este SOC, se ha seleccionado como solución para ser implementada y configurada en los endpoints una solución que integra sistema de antivirus, capacidades de EDR y protección en la navegación. Concretamente se ha elegido utilizar una solución de Sophos por sus características integradas y su compatibilidad con el sistema “Master SOC on Box”.

Aunque Sophos ofrece una variedad de soluciones adicionales (protección de correo electrónico, entre otras) para mejorar la seguridad de endpoints, en este Trabajo se limitará a explorar exclusivamente Sophos “Intercept X Advanced with XDR”. Cabe destacar que esta solución particular no presenta diferencias significativas con respecto a otras opciones ofrecidas por Sophos.

Para la implementación de esta solución en el SOC, se utilizarán sistemas de registro SYSLOG, apoyados en distintas API y conectores, para facilitar la integración de estas soluciones de endpoints con el sistema de gestión de información y eventos de seguridad (SIEM) del SOC. Esto implicará configurar la recopilación automatizada de logs y alertas procedentes de los endpoints, permitiendo así un análisis centralizado y eficiente.

La estrategia incluye la personalización de reglas en las soluciones de XDR y antivirus, adaptándolas al perfil de riesgo específico y las características del entorno operativo. Asimismo, se podrán configurar políticas de protección en la navegación web para bloquear el acceso a categorías de sitios considerados de cierto riesgo y gestionar el control de descargas de archivos, reforzando así la seguridad en el uso de internet en la organización.

Las instrucciones de instalación, configuración e integración de la solución Sophos se presentan en el anexo F de este documento.

2.6.7 Instalación, configuración y creación de reglas de ElastAlert2.

Las instrucciones de instalación, configuración y creación de reglas de ElastAlert2 se presentan en el anexo G de este documento.

2.6.8 Montaje de escenario Web básico para ataques de inyecciones.

Se propone realizar una aplicación Web bajo entorno Apache en una máquina con S.O. Windows 10, con la intención de poder realizar ataques de inyecciones, tales como SQLi o XSS, para probar la eficacia del Master SOC on Box.

Las instrucciones del montaje del entorno de la aplicación Web y de la propia elaboración de la aplicación Web se encuentran en el anexo H de este documento “Montaje de Web vulnerable a SQLi”.

2.6.9 Montaje de dashboards de Kibana.

Las instrucciones del montaje de paneles gráficos en Kibana se presentan en el anexo I de este documento.

3. Resultados.

A continuación, se presentarán las evidencias y resultados generados por las diversas aplicaciones que componen el Master SOC on Box. Inicialmente, se expondrán los resultados individuales de cada aplicación, confirmando su funcionamiento adecuado. Posteriormente, se realizarán pruebas independientes, tales como escaneos de puertos, ataques web y ataques de fuerza bruta, entre otros. Este proceso evidenciará la correcta implementación de todos los componentes conforme al diagrama simplificado que se muestra en la siguiente imagen, así como la capacidad y eficacia de la solución desarrollada en este Trabajo de Fin de Máster.

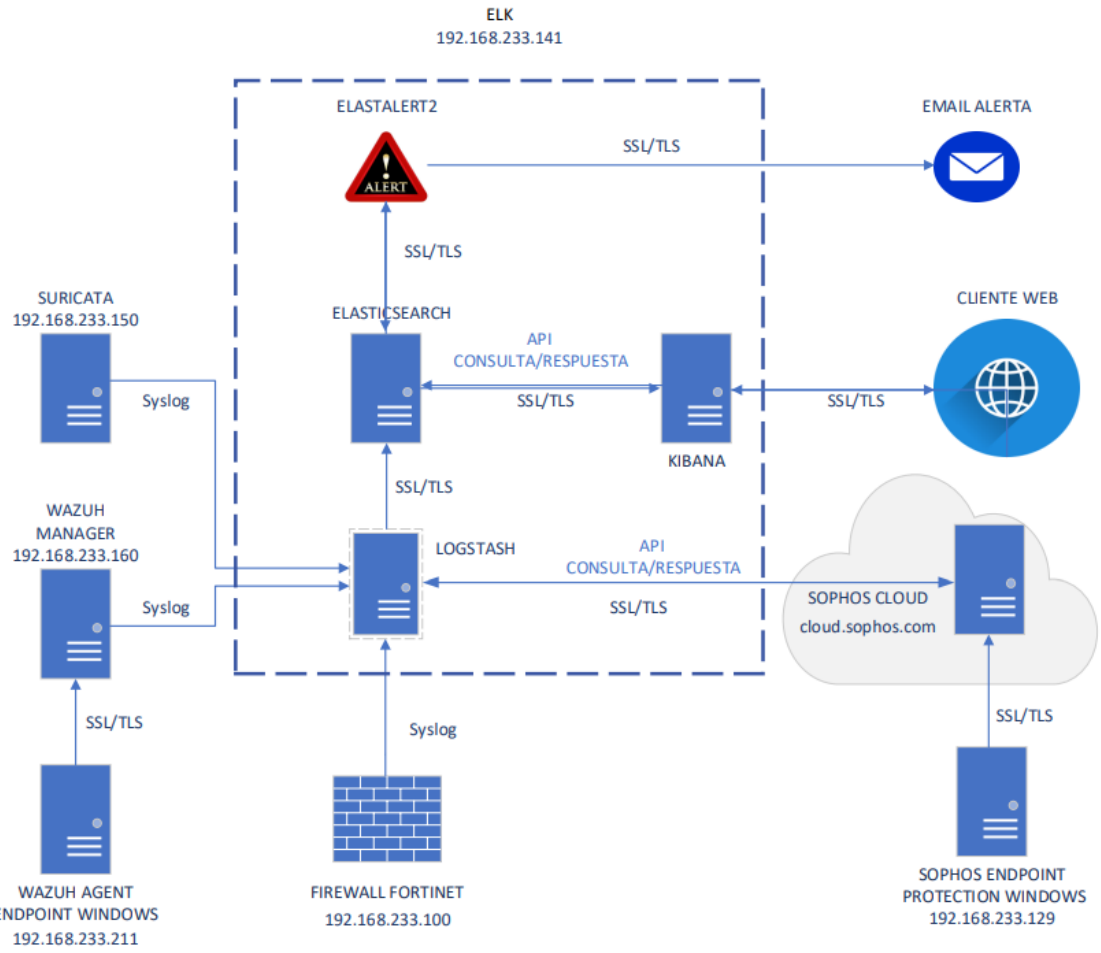


Figura 11: Diagrama de componentes simplificado de “Master SOC on Box”.

El diagrama anterior muestra de manera simple el funcionamiento de la solución, que bien se puede resumir como sigue:

1. **FIREWALL (192.168.233.100)**: Actúa como una barrera entre la red interna y externa, filtrando el tráfico y protegiendo la red contra accesos no autorizados y otras amenazas de Internet. Envía los logs mediante SYSLOG por protocolo UDP y puerto 514.

2. **SURICATA (192.168.233.150)**: Sistema de detección de intrusiones que supervisa todo el tráfico de red para detectar posibles amenazas. Envía los logs mediante SYSLOG por protocolo UDP puerto 5144.
3. **WAZUH MANAGER (192.168.233.160)**: Parte del sistema de gestión de seguridad de Wazuh que recoge datos de los agentes de Wazuh desplegados en los endpoints y ejecuta análisis y correlación de eventos. Envía los logs mediante SYSLOG por protocolo UDP puerto 5000.
4. **WAZUH AGENT (192.168.233.211)**: Instalado en un endpoint Windows, se encarga de recopilar datos de seguridad y los envía al Wazuh Manager para su análisis. Envía los logs mediante SSL/TLS por protocolo TCP puertos 1514 y 1515.
5. **SOPHOS CLOUD (cloud.sophos.com)**: Es el panel de control que se encuentra en la nube, de la solución Sophos instalada en los endpoints. Alberga los registros de eventos de seguridad que se transmiten mediante un cifrado SSL/TLS desde la solución Sophos instalada en el endpoint de Windows, la cual ofrece protección de punto final y administración de políticas de seguridad. Envía los logs al SIEM mediante SSL/TLS vía API a través del puerto 443 (HTTPS).
6. **SOPHOS ENDPOINT PROTECTION (192.168.233.129)**: Se trata de un software de seguridad implementado en un sistema operativo Windows, diseñado para salvaguardarlo contra software malicioso y ransomware, asegurar una experiencia de navegación web segura, entre otras protecciones. Este programa envía registros de seguridad a Sophos Cloud utilizando una conexión cifrada SSL/TLS vía API a través del puerto 443 (HTTPS).
7. **ELK (Elasticsearch, Logstash, Kibana) (192.168.233.141)**: El motor principal encargado de la gestión de logs y eventos de seguridad.
    - **Elasticsearch**: Es la base de datos que almacena y permite la búsqueda de grandes volúmenes de datos. El puerto por el que recibe y brinda información es el 9200 y trabaja bajo protocolo seguro SSL/TLS.
    - **Logstash**: Procesa y transforma datos antes de enviarlos a Elasticsearch. Recibe los logs por distintas vías (SSL/TLS, SYSLOG) y puertos, según se haya configurado en su archivo de configuración, y envía los datos por SSL/TLS a Elasticsearch a su puerto 9200.
    - **Kibana**: Proporciona una interfaz de usuario para visualizar y explorar datos en Elasticsearch. Mediante API solicita a Elasticsearch los datos a visualizar vía SSL/TLS al puerto 9200, y Elasticsearch se los devuelve también vía SSL/TLS. Kibana presenta los datos a través de su interfaz Web en el puerto 5601.
    - **ElastAlert2**: Solicita datos a Elasticsearch y este se los devuelve vía SSL/TLS, de manera que pueda llevar a cabo la generación de alertas según la configuración establecida, y de enviar un correo electrónico con los detalles de dichas alertas a los destinatarios pertinentes, utilizando también una conexión segura SSL/TLS.
8. **CLIENTE WEB**: Representa a un usuario o sistema accediendo a los servicios web de Kibana para consultar los datos de seguridad del SOC a través del puerto 5601, que está configurado para utilizar el protocolo seguro HTTPS.

3.1 Evidencias del correcto funcionamiento de la implementación de las aplicaciones que conforman el Master SOC on BOX.

Para llevar a cabo este punto se hará uso, entre otras, de la solución “Anti-Malware Testing Standards Organization” (AMTSO), ya que facilita distintos tipos de pruebas diseñadas para verificar la protección en tiempo real contra malware, bloqueo de descargas maliciosas, entre otras.

3.1.1 Evidencias de obtención de logs de Wazuh, Suricata, Firewall y solución Sophos por parte de la herramienta Logstash y presentados en Kibana.

3.1.1.1 Evidencias de obtención de logs de Wazuh.

La siguiente imagen proporcionada de Kibana muestra registros provenientes de Wazuh, evidenciando que la implementación de Wazuh, incluyendo el manager y el agente, está operando adecuadamente. Estos registros se han creado a partir de acciones como iniciar y cerrar sesión en el sistema donde está instalado el agente de Wazuh, así como la creación de archivos y otras actividades. Dado que el agente de Wazuh rastrea casi todas las acciones en el sistema en el que está instalado, es crucial ejercer prudencia al configurar alertas con ElastAlert2 para evitar alertas innecesarias que no correspondan a incidentes relevantes de ciberseguridad. Cabe destacar que los registros recopilados son extremadamente útiles para el análisis forense digital en caso de incidentes de seguridad.

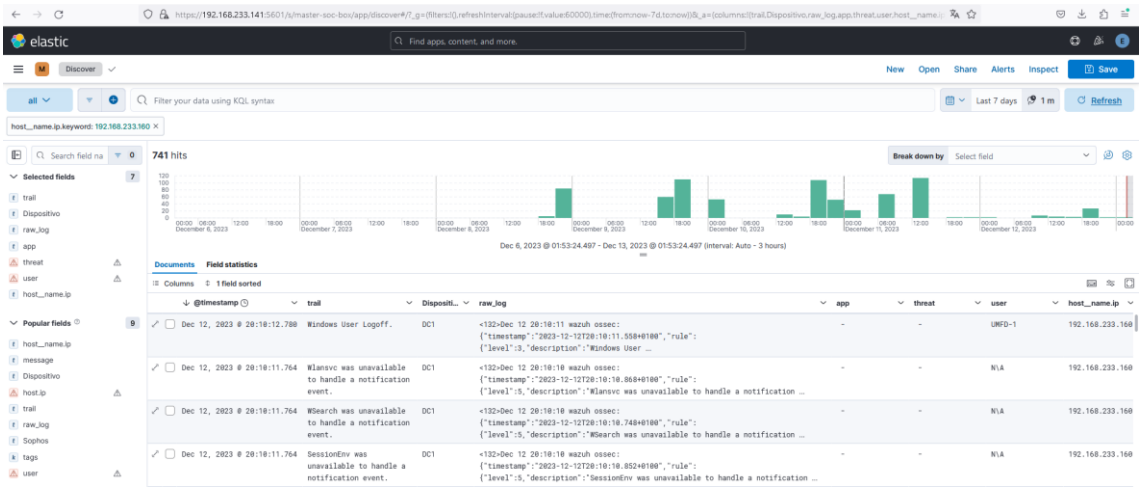


Figura 12: Detalle de logs de Wazuh en Kibana.

3.1.1.2 Evidencias de obtención de logs de Suricata.

La imagen de Kibana adjunta (Figura 14) muestra registros generados por Suricata, demostrando que su implementación está operando de manera efectiva. Estos registros fueron generados tras ejecutar el comando que se puede apreciar en la captura de pantalla siguiente.

```
root@sonda:/home/tfm# curl http://testmyids.org/uid/index.html
root@sonda:/home/tfm#
```

Figura 13: Detalle del comando para testar Suricata.

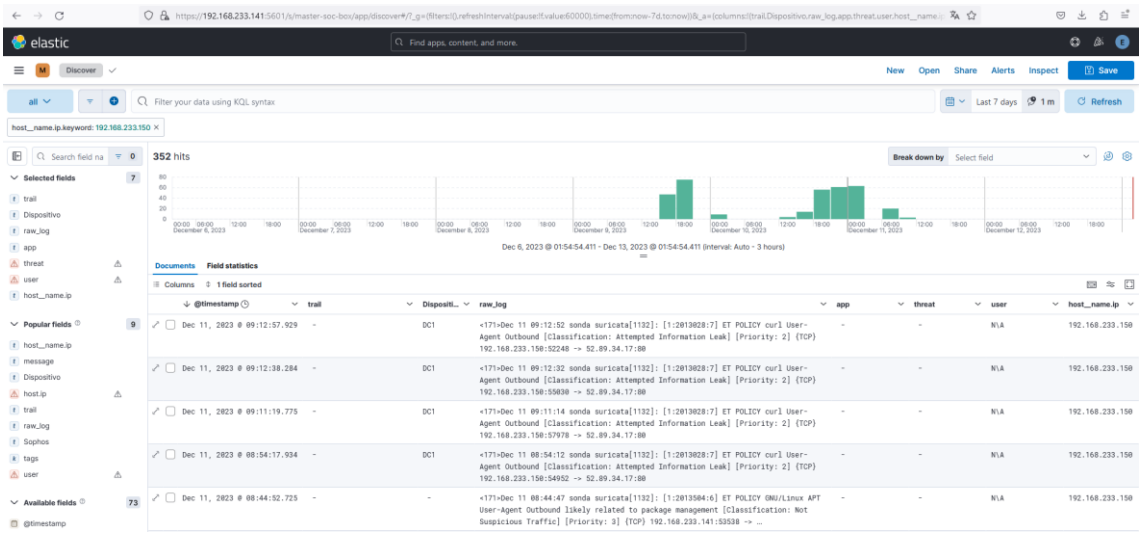


Figura 14: Detalle de logs de Suricata en Kibana.

3.1.1.3 Evidencias de obtención de logs del Firewall.

La imagen de Kibana adjunta presenta registros del Firewall, en este caso FortiGate, recibidos a través de SYSLOG, lo cual indica que la implementación de esta solución de firewall está funcionando de manera adecuada.

Documents | Field statistics

Columns | 1 field sorted

@timestamp	flow	trail	ref	proto	type
Dec 13, 2023 @ 14:23:35.592	192.168.13.153:64367 ===> 192.168.4.4:161	Traffic deny	FG-forward	UDP	syslog
Dec 13, 2023 @ 14:23:24.902	192.168.13.153:64367 ===> 192.168.4.4:161	Traffic deny	FG-forward	UDP	syslog
Dec 13, 2023 @ 14:22:59.387	192.168.13.153:52260 ===> 192.168.1.44:53	Traffic accept	FG-forward	UDP	syslog
Dec 13, 2023 @ 14:22:58.738	192.168.13.153:56331 ===> 192.168.1.44:53	Traffic accept	FG-forward	UDP	syslog
Dec 13, 2023 @ 14:22:46.365	192.168.13.153:59128 ===> 192.168.1.40:445	Traffic accept	FG-forward	TCP	syslog
Dec 13, 2023 @ 14:22:46.363	192.168.13.153:59103 ===> 192.168.1.47:445	Traffic accept	FG-forward	TCP	syslog

Figura 15: Detalle de logs del Firewall en Kibana.

Del mismo modo, en el firewall se pueden observar todos los registros del tráfico de red que pasa por él.

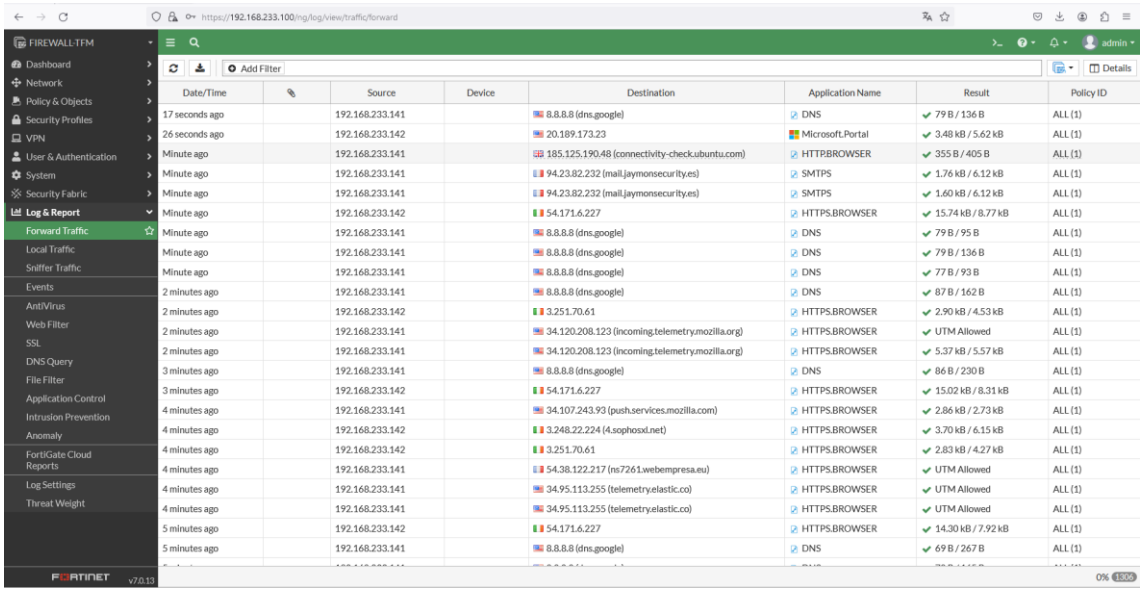


Figura 16.1: Detalle de logs del Firewall.

También se puede observar su funcionamiento ante intento de descarga de archivo malicioso.

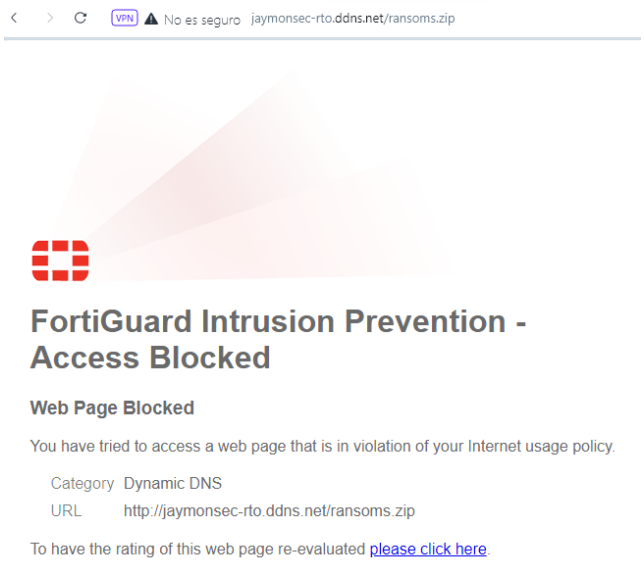


Figura 17.2: Detalle de acción IPS del Firewall.

3.1.1.4 Evidencias de obtención de logs de la solución Sophos.

Para recopilar los logs generados por la solución Sophos, que se almacenan en el cloud de Sophos, es necesario ejecutar el script “siem.py” que se muestra en la siguiente captura, y cuya configuración se detalla en el anexo “F. Instalación, configuración e integración en SOC de solución Sophos”. Este proceso permitirá que los logs se guarden en el archivo denominado “result.txt”, desde donde los obtendrá el SIEM.

Figura 18: Detalle de ejecución del script de Sophos para descargar logs del cloud.

La captura de pantalla de Kibana que se adjunta muestra registros de la solución Sophos, lo que confirma que la implementación de dicha solución está funcionando correctamente.

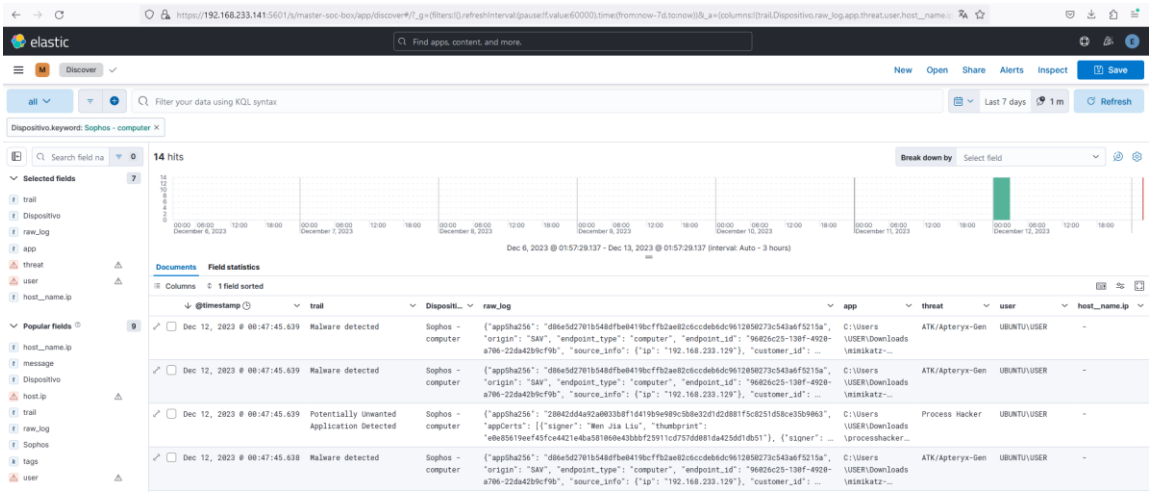


Figura 19: Detalle de logs de Sophos en Kibana.

3.1.1.5 Evidencia del funcionamiento de ElastAlert2.

En la siguiente captura se puede observar cómo se ejecuta “ElastAlert2” y se recibe una alerta en base a sus reglas, que posteriormente envía por Email.

Figura 20: Detalle de ejecución de ElastAlert2 y envío de alerta.

A continuación, se muestra cómo se ha recibido la alerta por correo electrónico, lo que confirma que la implementación de “ElastAlert2” está funcionando correctamente.

Figura 21: Detalle del email de alerta recibido por ElastAlert2.

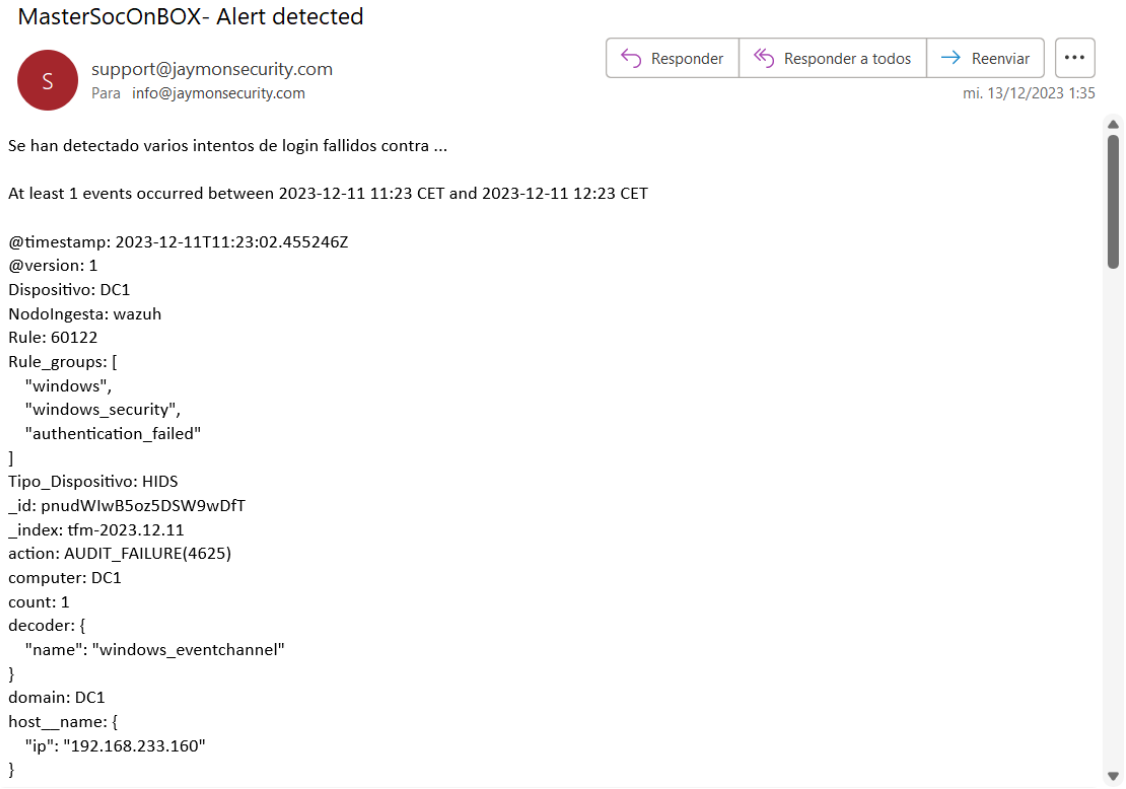


Figura 22: Detalle del email de alerta recibido por ElastAlert2.

3.1.2 Resultados de pruebas específicas.

A continuación, se llevarán a cabo distintas pruebas de seguridad enfocadas en distintos tipos de ciberataques comunes.

3.1.2.1 Detección y alerta de escaneo de puertos con “nmap”.

Para llevar a cabo la detección de un escaneo de puertos realizado con la herramienta “nmap”, muy utilizada en el ámbito de la ciberseguridad para escanear máquinas y puertos en una red, se deberá crear la siguiente regla en Suricata.

```
root@sonda:/etc/suricata/rules# tail -3 app-layer-events.rules

#alert nmap scan
alert tcp any any -> any any (msg:"SYNSTEALTH SCAN DETECTED"; flow:stateless; flags:S,12; reference:arachnids,198; classtype:
attempted-recon;sid:2100624; priority:5; rev:8; threshold: type threshold, track by_src, count 50, seconds 1;)
root@sonda:/etc/suricata/rules#
```

Figura 23: Detalle de la regla de Suricata.

Una vez creada la regla anterior, se deberá ejecutar el comando “suricata-update” para verificar que la regla ha sido cargada satisfactoriamente y sin errores.

```
15/12/2023 -- 00:57:22 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
15/12/2023 -- 00:57:22 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
15/12/2023 -- 00:57:22 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
15/12/2023 -- 00:57:22 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
15/12/2023 -- 00:57:22 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
15/12/2023 -- 00:57:22 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
15/12/2023 -- 00:57:22 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
15/12/2023 -- 00:57:23 - <Info> -- Ignoring file rules/emerging-deleted.rules
15/12/2023 -- 00:57:26 - <Warning> -- Found duplicate rule SID 2100624 with same revision, keeping the first rule seen.
15/12/2023 -- 00:57:26 - <Info> -- Loaded 46596 rules.
15/12/2023 -- 00:57:27 - <Info> -- Disabled 14 rules.
15/12/2023 -- 00:57:27 - <Info> -- Enabled 0 rules.
15/12/2023 -- 00:57:27 - <Info> -- Modified 0 rules.
15/12/2023 -- 00:57:27 - <Info> -- Dropped 0 rules.
15/12/2023 -- 00:57:27 - <Info> -- Enabled 133 rules for flowbit dependencies.
15/12/2023 -- 00:57:27 - <Info> -- Backing up current rules.
15/12/2023 -- 00:57:31 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 46595; enabled: 36105; added: 1; r
emoved 0; modified: 0
15/12/2023 -- 00:57:32 - <Info> -- Writing /var/lib/suricata/rules/classification.config
15/12/2023 -- 00:57:32 - <Info> -- Testing with suricata -T.
15/12/2023 -- 00:59:12 - <Info> -- Done.
```

Figura 24: Detalle de la actualización de reglas de Suricata.

En caso de no haber ocurrido errores en el comando anterior, se deberá reiniciar el servicio de Suricata con el comando “systemctl restart suricata”.

```
root@sonda:/etc/suricata/rules# systemctl restart suricata
root@sonda:/etc/suricata/rules#
```

Figura 25: Detalle del reinicio del servicio de Suricata.

Llegados a este punto, se procede a realizar el escaneo de puertos de la máquina con dirección IP 192.168.233.150 con la herramienta “nmap”, desde la máquina atacante con dirección IP 192.168.233.141.

```
tfm@tfm-elk:~$ sudo su
[sudo] contraseña para tfm:
root@tfm-elk:/home/tfm# nmap 192.168.233.150
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-15 00:31 CET
Nmap scan report for 192.168.233.150
Host is up (0.00029s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
514/tcp open  shell
MAC Address: 00:0C:29:A5:0F:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@tfm-elk:/home/tfm#
```

Figura 26: Detalle de escaneo con nmap.

En la máquina “sonda” donde se encuentra instalado Suricata, es conveniente monitorizar en tiempo real lo que va sucediendo en “SYSLOG”. Esto se puede realizar mediante el comando “tail -f /var/log/SYSLOG”. Como se puede observar en la siguiente captura, Suricata ha detectado el escaneo de puertos satisfactoriamente.

```
Dec 15 00:31:03 sonda suricata[24240]: [1:2100624:8] SYNSTEALTH SCAN DETECTED [Classification: Attempted Information Leak] [Priority: 5] {TCP} 192.168.233.141:52780 -
> 192.168.233.150:10180
Dec 15 00:31:03 sonda suricata[24240]: [1:2100624:8] SYNSTEALTH SCAN DETECTED [Classification: Attempted Information Leak] [Priority: 5] {TCP} 192.168.233.141:52780 -
> 192.168.233.150:2492
Dec 15 00:31:03 sonda suricata[24240]: [1:2100624:8] SYNSTEALTH SCAN DETECTED [Classification: Attempted Information Leak] [Priority: 5] {TCP} 192.168.233.141:52780 -
> 192.168.233.150:8291
Dec 15 00:31:03 sonda suricata[24240]: [1:2100624:8] SYNSTEALTH SCAN DETECTED [Classification: Attempted Information Leak] [Priority: 5] {TCP} 192.168.233.141:52780 -
> 192.168.233.150:18101
Dec 15 00:31:03 sonda suricata[24240]: [1:2100624:8] SYNSTEALTH SCAN DETECTED [Classification: Attempted Information Leak] [Priority: 5] {TCP} 192.168.233.141:52780 -
> 192.168.233.150:3827
```

Figura 27: Detalle del SYSLOG.

En la siguiente captura de Kibana se muestran los logs de Suricata de la detección del escaneo de puertos.

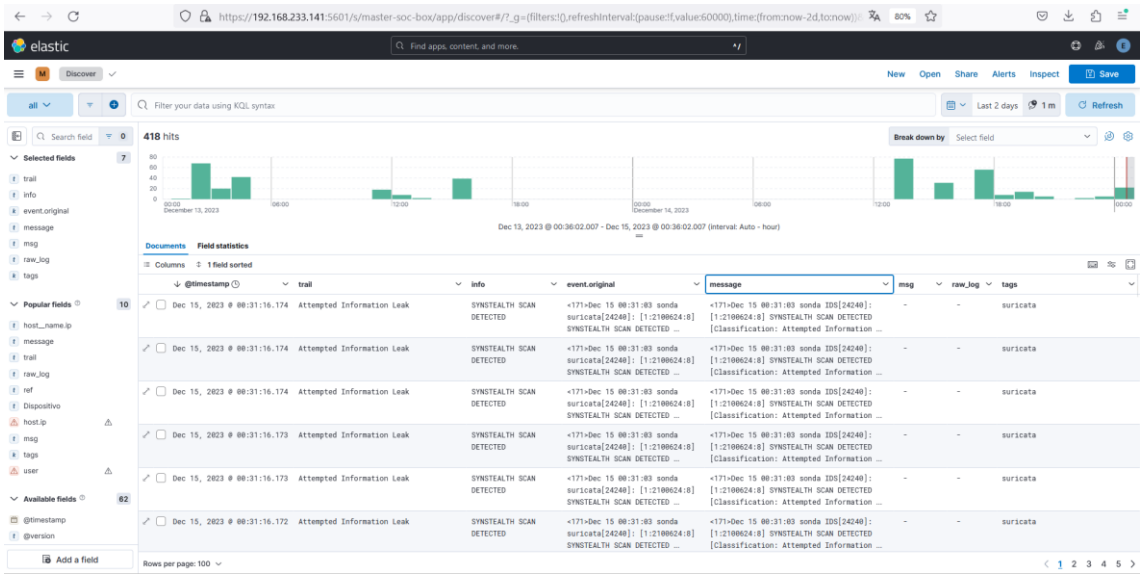


Figura 28: Detalle del Kibana.

De manera paralela, se realiza la ejecución de ElastAlert2, que detecta un patrón coincidente en su regla “scanports.yaml” y emite una alerta por correo electrónico.

```
root@tfm-elk:/home/tfm/elastalert2# python -m elastalert.elastalert --verbose --rule custom_rules/scanports.yaml --config config.yaml --start 2023-12-14
INFO:elastalert:1 rules loaded
INFO:elastalert:Starting up
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.99983 seconds
INFO:elastalert:Queried rule Scan ports rule from 2023-12-14 01:00 CET to 2023-12-14 01:15 CET: 0 / 0 hits
INFO:elastalert:Queried rule Scan ports rule from 2023-12-14 01:15 CET to 2023-12-14 01:30 CET: 0 / 0 hits
INFO:elastalert:Queried rule Scan ports rule from 2023-12-15 00:30 CET to 2023-12-15 00:41 CET: 19 / 19 hits
INFO:elastalert:Sent email to ['info@jaymonsecurity.com']
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ignoring match for silenced rule Scan ports rule
INFO:elastalert:Ran Scan ports rule from 2023-12-14 01:00 CET to 2023-12-15 00:41 CET: 19 query hits (0 already seen), 19 matches, 1 alerts sent
```

Figura 29: Detalle de la ejecución de ElastAlert2.

A continuación, se muestra el correo electrónico de la alerta que “ElastAlert2” ha enviado con los detalles correspondientes.

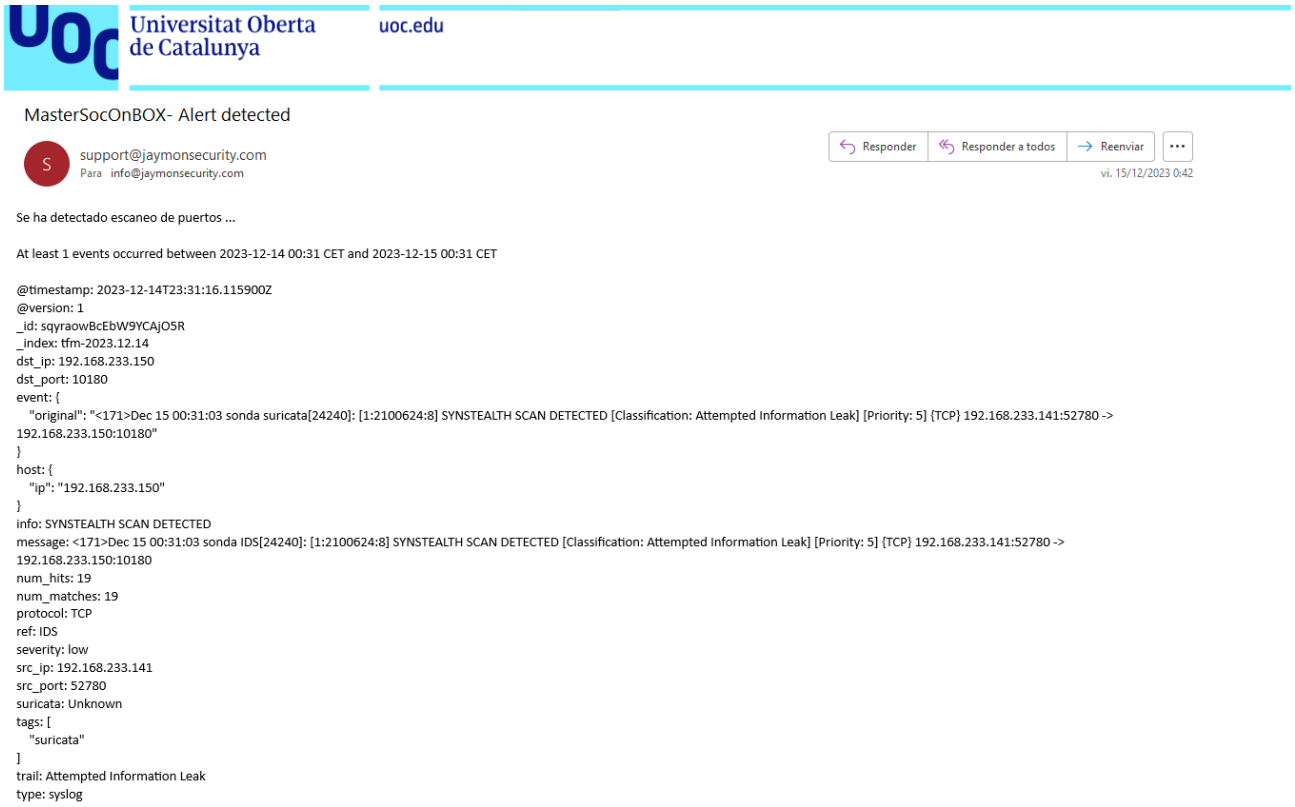


Figura 30: Detalle del email enviado por ElastAlert2.

3.1.2.2 Detección y alerta de ataque por diccionario o fuerza bruta a un servidor SSH.

Para llevar a cabo esta prueba, se deja corriendo un servidor SSH debidamente configurado en el sistema víctima. En este caso será la máquina con dirección IP 192.168.233.150.

```
root@sonda:/home/tfm# service sshd status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-12-09 17:42:05 CET; 5 days ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 955 (sshd)
      Tasks: 1 (limit: 4556)
     Memory: 3.1M
        CPU: 313ms
     CGroup: /system.slice/ssh.service
             └─955 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

dic 09 17:42:05 sonda systemd[1]: Started OpenBSD Secure Shell server.
dic 09 17:42:05 sonda sshd[955]: Server listening on :: port 22.
dic 10 17:50:53 sonda sshd[7393]: Accepted password for tfm from 192.168.233.141 port 58346 ssh2
dic 10 17:50:53 sonda sshd[7393]: pam_unix(sshd:session): session opened for user tfm(uid=1000) by (uid=0)
dic 10 17:50:53 sonda sshd[7393]: pam_unix(sshd:session): session closed for user tfm
dic 15 00:58:10 sonda sshd[24381]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1  user=root
dic 15 00:58:12 sonda sshd[24381]: Failed password for root from 127.0.0.1 port 45388 ssh2
dic 15 00:58:15 sonda sshd[24381]: Connection closed by authenticating user root 127.0.0.1 port 45388 [preauth]
dic 15 00:58:28 sonda sshd[24385]: Accepted password for tfm from 127.0.0.1 port 42864 ssh2
dic 15 00:58:28 sonda sshd[24385]: pam_unix(sshd:session): session opened for user tfm(uid=1000) by (uid=0)
root@sonda:/home/tfm#
```

Figura 31: Detalle del servicio SSH.

Para llevar a cabo la detección del ataque de fuerza bruta realizado con la herramienta “Hydra”, de deberá crear la siguiente regla en Suricata.

```
root@sonda:/etc/suricata/rules# tail -3 app-layer-events.rules
#alerta fuerza bruta SSH
alert tcp any any -> any any  (msg:"Ataque de fuerza bruta SSH"; flow:to_server,established; content:"authentication failed"; nocase;
 threshold:type threshold,track by_src,seconds 60,count 5; classtype:attempted-admin; sid:1000001; rev:1;)
```

Figura 32: Detalle de la regla de Suricata.

Una vez creada la regla anterior, se deberá ejecutar el comando “suricata-update” para verificar que la regla ha sido cargada satisfactoriamente y sin errores. En caso de no haber habido errores en el comando anterior, se deberá reiniciar el servicio de Suricata con el comando “systemctl restart suricata”.

Llegados a este punto, se procede a realizar el ataque de fuerza bruta al servidor SSH con la herramienta “Hydra”. La máquina atacante presenta la dirección IP 192.168.233.141 y la máquina víctima presenta la dirección IP 192.168.233.150.

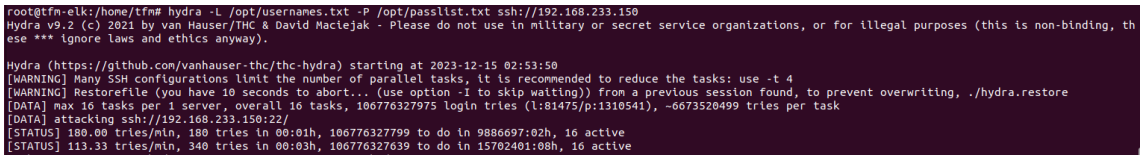


Figura 33: Detalle del ataque a SSH.

En la máquina “sonda” donde se encuentra instalado Suricata, es conveniente monitorizar a tiempo real lo que va sucediendo en “SYSLOG”. Esto se puede realizar mediante el comando “tail -f /var/log/SYSLOG”. Como se puede observar en la siguiente captura, Suricata ha detectado el ataque de fuerza bruta a SSH satisfactoriamente.

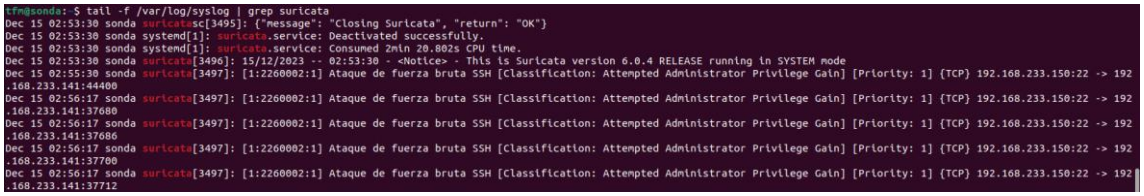


Figura 34: Detalle del SYSLOG.

En la siguiente captura de Kibana se muestran los logs de Suricata de la detección del ataque de fuerza bruta a SSH.

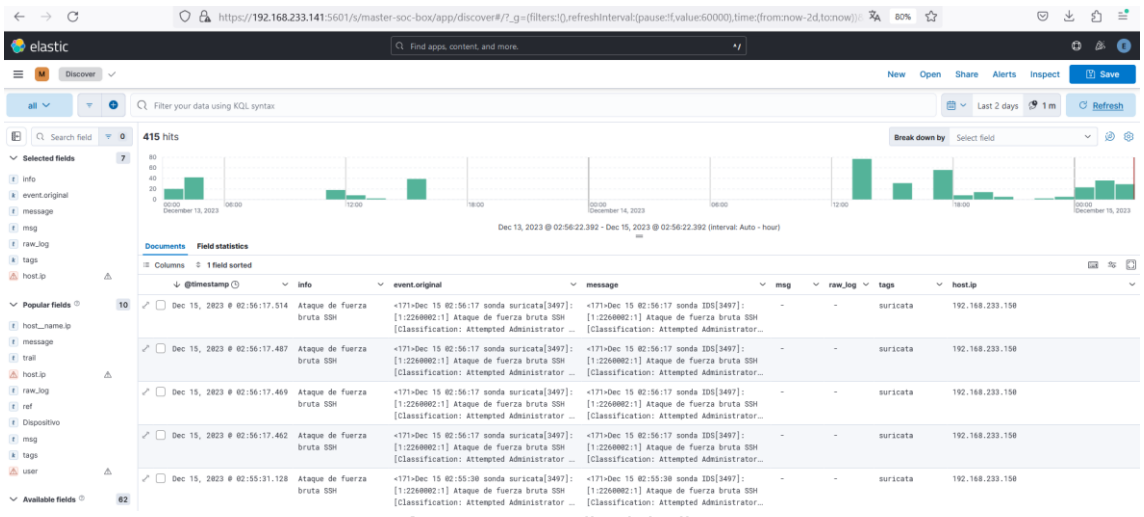


Figura 35: Detalle del Kibana.

De manera paralela, se realiza la ejecución de “ElastAlert2”, que detecta un patrón coincidente en su regla “sshbruteforce.yaml” y emite una alerta por correo electrónico.

```
root@tfm-elk:/home/tfm/elastalert2# python -m elastalert.elastalert --verbose --rule custom_rules/sshbruteforce.yaml --config config.yaml
INFO:elastalert:1 rules loaded
INFO:elastalert:Starting up
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.99993 seconds
INFO:elastalert:Queried rule Brute force rule from 2023-12-15 02:47 CET to 2023-12-15 02:58 CET: 7 / 7 hits
INFO:elastalert:Sent email to ['info@jaymonsecurity.com']
INFO:elastalert:Ignoring match for silenced rule Brute force rule
INFO:elastalert:Ignoring match for silenced rule Brute force rule
INFO:elastalert:Ignoring match for silenced rule Brute force rule
INFO:elastalert:Ignoring match for silenced rule Brute force rule
INFO:elastalert:Ignoring match for silenced rule Brute force rule
INFO:elastalert:Ignoring match for silenced rule Brute force rule
INFO:elastalert:Ran Brute force rule from 2023-12-15 02:47 CET to 2023-12-15 02:58 CET: 7 query hits (0 already seen), 7 matches, 1 alerts sent
INFO:elastalert:Brute force rule range 617
```

Figura 36: Detalle de la ejecución de ElastAlert2.

A continuación, se muestra el correo electrónico de la alerta que ElastAlert2 ha enviado con los detalles correspondientes.

MasterSocOnBOX- Alert detected

S support@jaymonsecurity.com
Para info@jaymonsecurity.com

Responder | Responder a todos | Reenviar | ...

vi. 15/12/2023 3:01

Se ha detectado ataque de fuerza bruta ...

At least 1 events occurred between 2023-12-14 02:58 CET and 2023-12-15 02:58 CET

@timestamp: 2023-12-15T01:58:07.138430Z
@version: 1
_id: DKwxa4wBcEbW9YCA_O-q
_index: tfm-2023.12.15
dst_ip: 192.168.233.141
dst_port: 60964
event: {
"original": "<171>Dec 15 02:58:06 sonda suricata[3497]: [1:2260002:1] Ataque de fuerza bruta SSH [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 54.38.122.217:26 -> 192.168.233.141:60964"
}
host: {
"ip": "192.168.233.150"
}
info: Ataque de fuerza bruta SSH
message: <171>Dec 15 02:58:06 sonda IDS[3497]: [1:2260002:1] Ataque de fuerza bruta SSH [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 54.38.122.217:26 -> 192.168.233.141:60964
num_hits: 1
num_matches: 1
protocol: TCP
ref: IDS
severity: high
src_ip: 54.38.122.217
src_port: 26

Figura 37: Detalle del email enviado por ElastAlert2.

3.1.2.3 Detección y alerta de inicio de sesión fallido en una máquina Windows.

Para llevar a cabo la detección de intentos de inicio de sesión fallidos en una máquina Windows, donde se encuentra instalado Wazuh, únicamente habrá que provocarlos y crear la alerta en ElastAlert, ya que el propio agente de Wazuh se encargará de reportarlo automáticamente al SIEM por los cauces correspondientes.

Así pues, en la siguiente captura se muestra cómo el usuario intenta realizar una escalada de privilegios mediante el comando “runas” en la máquina con dirección IP 192.168.233.221, fallando el inicio de sesión que le devolvería una Shell de comandos con privilegios de administrador.

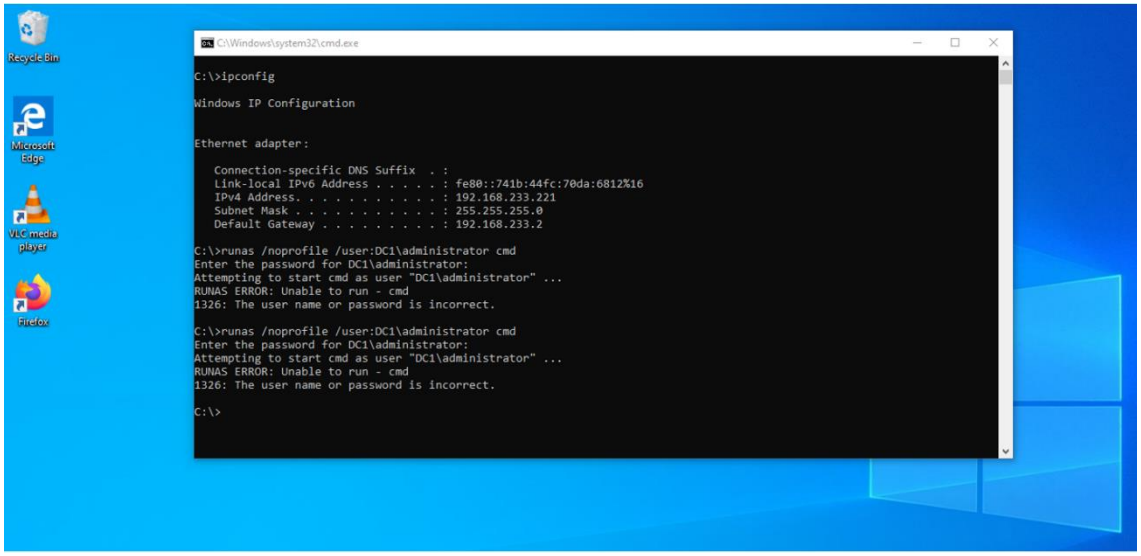


Figura 38: Detalle de los inicios de sesión fallidos con “runas”.

En la siguiente captura de Kibana se muestran los logs de Wazuh de la detección del intento de inicio de sesión fallido.

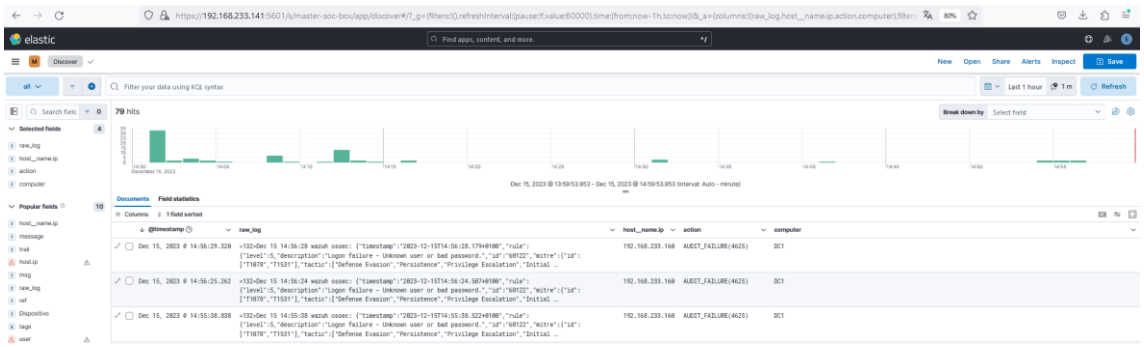


Figura 39: Detalle del Kibana.

De manera paralela, se realiza la ejecución de ElastAlert2, que detecta un patrón coincidente en su regla “logonfailure.yaml” y emite una alerta por correo electrónico.

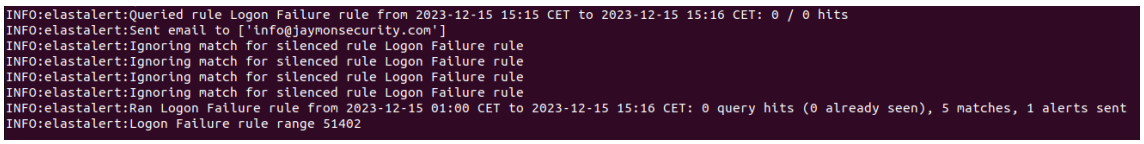


Figura 40: Detalle de la ejecución de ElastAlert2.

A continuación, se muestra el correo electrónico de la alerta que ElastAlert2 ha enviado con los detalles correspondientes.

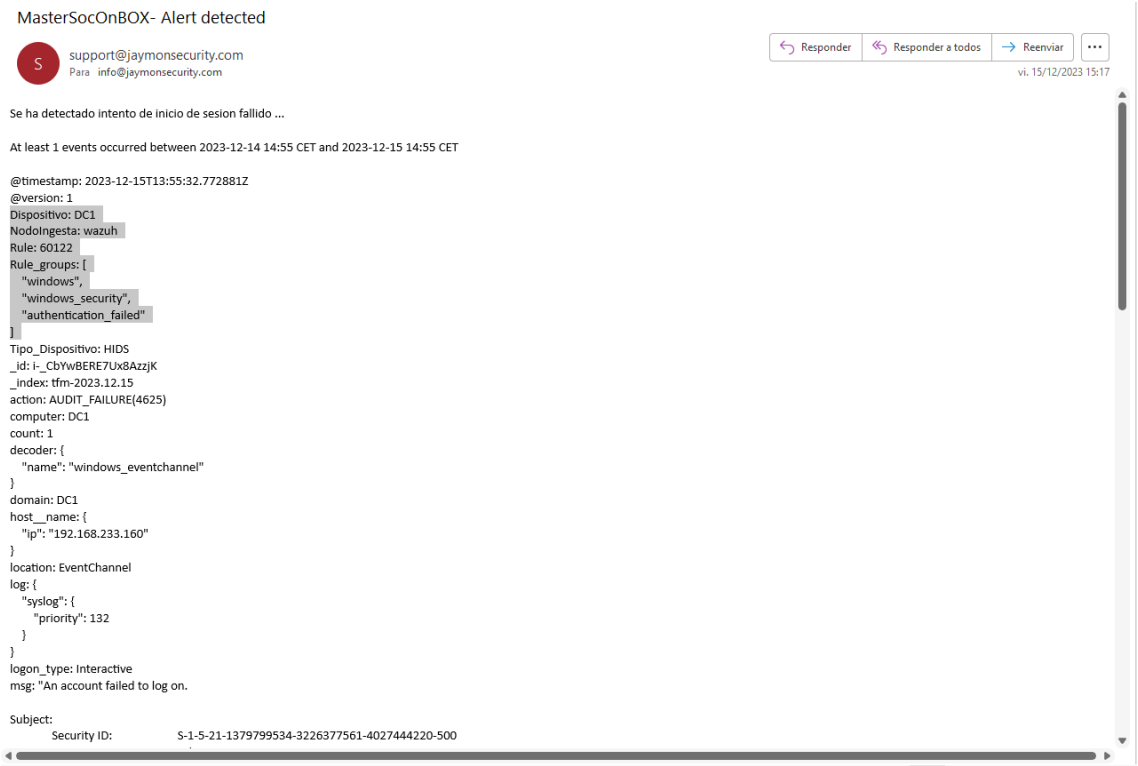


Figura 41: Detalle del email enviado por ElastAlert2.

3.1.2.4 Detección y alerta de inyección SQL en aplicación Web.

Para llevar a cabo esta prueba, se empleará la aplicación Web que se ha montado conforme a las instrucciones del anexo “H. Montaje de Web vulnerable a SQLi para pruebas del SOC”. Es relevante mencionar que no es indispensable que la aplicación sea vulnerable a inyecciones SQL (SQLi) para ejecutar esta prueba de concepto (PoC). Sin embargo, con el propósito de enriquecer futuras investigaciones sobre la correlación de alertas derivadas de secuencias de ataque (chainattacks) que sugieran una posible vulneración de la seguridad de la aplicación, se ha diseñado deliberadamente esta aplicación con vulnerabilidades.

Para llevar a cabo la detección de inyecciones SQL en aplicaciones Web, se deberá crear la siguiente regla en Suricata.

```
#SQL Injection
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains singlequote)"; flow:established,to_server; content:"'"; nocase; http_uri; sid:1;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains UNION)"; flow:established,to_server; content:"union"; nocase; http_uri; sid:2;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains SELECT)"; flow:established,to_server; content:"select"; nocase; http_uri; sid:3;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains singlequote POST DATA)"; flow:established,to_server; content:"'"; nocase; http_client_body; sid:4;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains UNION POST DATA)"; flow:established,to_server; content:"union"; nocase; http_client_body; sid:5;)
alert http any any -> any any (msg: "Possible SQL Injection attack (Contains SELECT POST DATA)"; flow:established,to_server; content:"select"; nocase; http_client_body; sid:6;)
```

Figura 42: Detalle de la regla de Suricata.

Una vez creada la regla anterior, se deberá ejecutar el comando “suricata-update” para verificar que la regla ha sido cargada satisfactoriamente y sin errores. En caso de no haber ocurrido errores en el comando anterior, se deberá reiniciar el servicio de Suricata con el comando “systemctl restart suricata”.

Llegados a este punto, se procede a realizar el intento de inyección SQL en la aplicación Web que se encuentra en la máquina Windows con dirección IP 192.168.233.1. Para este caso en concreto se ha optado por realizar el intento de SQLi de manera manual, como se puede observar en el parámetro “id” sobre la URL, donde se ha añadido una comilla simple que provocará el error que desencadene la alerta.

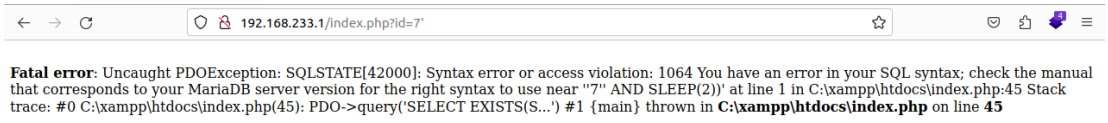


Figura 43: Detalle del error provocado por el ataque SQLi.

En la máquina “sonda” donde se encuentra instalado Suricata, es conveniente monitorizar a tiempo real lo que va sucediendo en “SYSLOG”. Esto se puede realizar mediante el comando “tail -f /var/log/SYSLOG”. Como se puede observar en la siguiente captura, Suricata ha detectado el intento de inyección SQL (SQLi) satisfactoriamente.

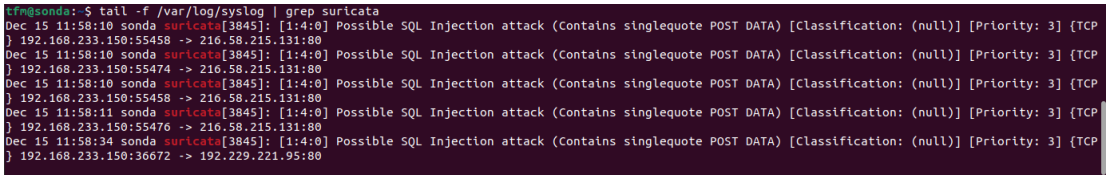


Figura 44: Detalle del SYSLOG.

En la siguiente captura de Kibana se muestran los logs de Suricata de la detección de la inyección SQL en la aplicación Web.

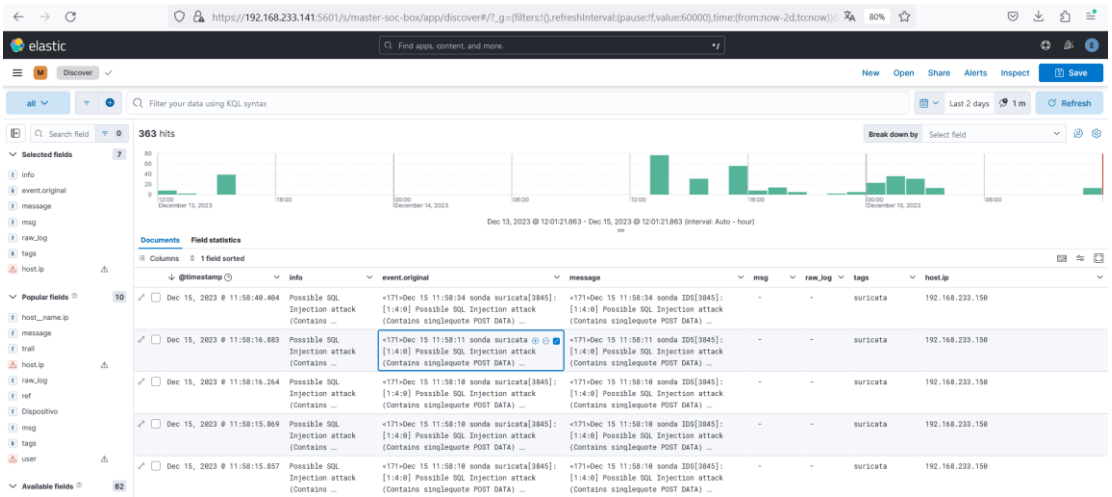


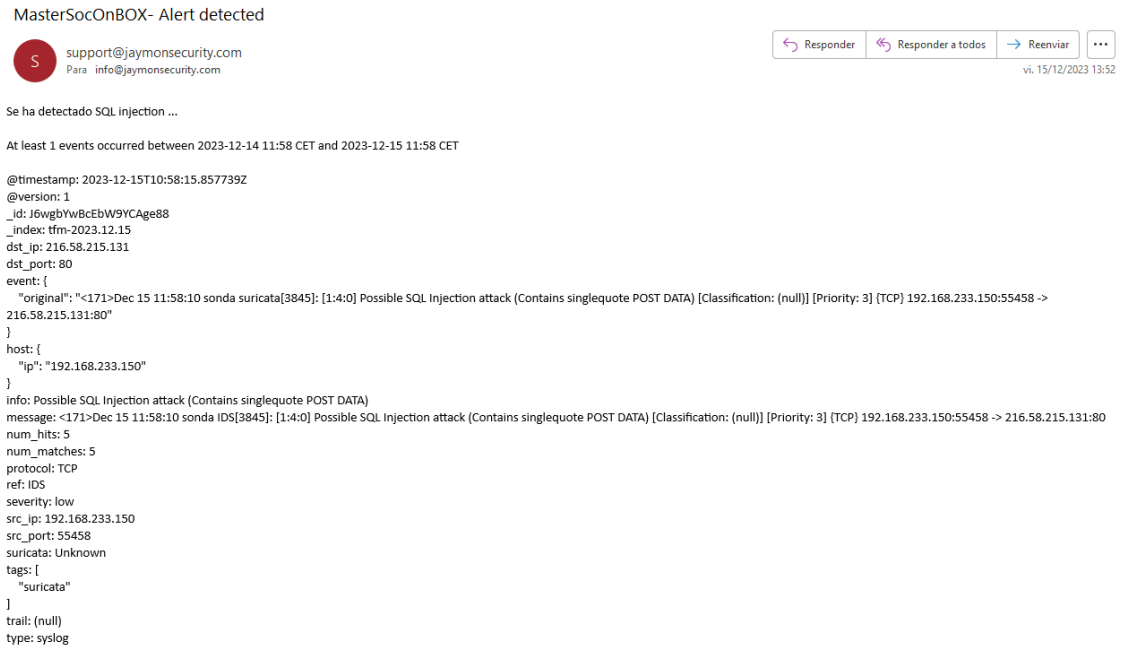
Figura 45: Detalle del Kibana.

De manera paralela, se realiza la ejecución de ElastAlert2, que detecta un patrón coincidente en su regla “sqli.yaml” y emite una alerta por correo electrónico.

```
INFO:elastalert:Queried rule SQLi rule from 2023-12-15 13:45 CET to 2023-12-15 13:51 CET: 0 / 0 hits
INFO:elastalert:Sent email to ['info@jaymonsecurity.com']
INFO:elastalert:Ignoring match for silenced rule SQLi rule
INFO:elastalert:Ignoring match for silenced rule SQLi rule
INFO:elastalert:Ignoring match for silenced rule SQLi rule
INFO:elastalert:Ignoring match for silenced rule SQLi rule
INFO:elastalert:Ran SQLi rule from 2023-12-15 01:00 CET to 2023-12-15 13:51 CET: 0 query hits (0 already seen), 5 matches, 1 alerts sent
INFO:elastalert:SQLi rule range 46296
```

Figura 46: Detalle de la ejecución de ElastAlert2.

A continuación, se muestra el correo electrónico de la alerta que ElastAlert2 ha enviado con los detalles correspondientes.



MasterSocOnBOX- Alert detected

S support@jaymonsecurity.com
Para info@jaymonsecurity.com

Responder | Responder a todos | Reenviar | ...
vi, 15/12/2023 13:52

Se ha detectado SQL injection ...

At least 1 events occurred between 2023-12-14 11:58 CET and 2023-12-15 11:58 CET

@timestamp: 2023-12-15T10:58:15.857739Z
@version: 1
_id: J6wgbYwBcEbW9YCAge88
_index: tfm-2023.12.15
dst_ip: 216.58.215.131
dst_port: 80
event: {
"original": "<171>Dec 15 11:58:10 sonda suricata[3845]: [1:4:0] Possible SQL Injection attack (Contains singlequote POST DATA) [Classification: (null)] [Priority: 3] {TCP} 192.168.233.150:55458 -> 216.58.215.131:80"
}
host: {
"ip": "192.168.233.150"
}
info: Possible SQL Injection attack (Contains singlequote POST DATA)
message: <171>Dec 15 11:58:10 sonda IDS[3845]: [1:4:0] Possible SQL Injection attack (Contains singlequote POST DATA) [Classification: (null)] [Priority: 3] {TCP} 192.168.233.150:55458 -> 216.58.215.131:80
num_hits: 5
num_matches: 5
protocol: TCP
ref: IDS
severity: low
src_ip: 192.168.233.150
src_port: 55458
suricata: Unknown
tags: [
"suricata"
]
trail: (null)
type: syslog

Figura 47: Detalle del email enviado por ElastAlert2.

3.1.2.5 Detección y alerta de la solución Sophos (XDR).

A continuación, se van a llevar a cabo distintas pruebas que verificarán la correcta implantación y funcionamiento de la solución Sophos en el Master SOC on Box.

3.1.2.5.1 Detección y alerta de ejecución de Exploit.

Para realizar esta prueba, se descarga un programa ejecutable de Internet que, una vez ejecutado, despliega una serie de exploits, cuyas características específicas, como la ejecución de movimientos laterales o la explotación de otras funcionalidades del sistema objetivo, no se detallarán aquí.

Como se ilustra en la captura de pantalla siguiente, se ha seleccionado para la descarga el ransomware “Cryptowall”. Este malware, al igual que muchos otros de su tipo, incluye en su código distintos exploits diseñados para realizar movimientos laterales, permitiéndole así escalar privilegios y propagarse por el sistema víctima.

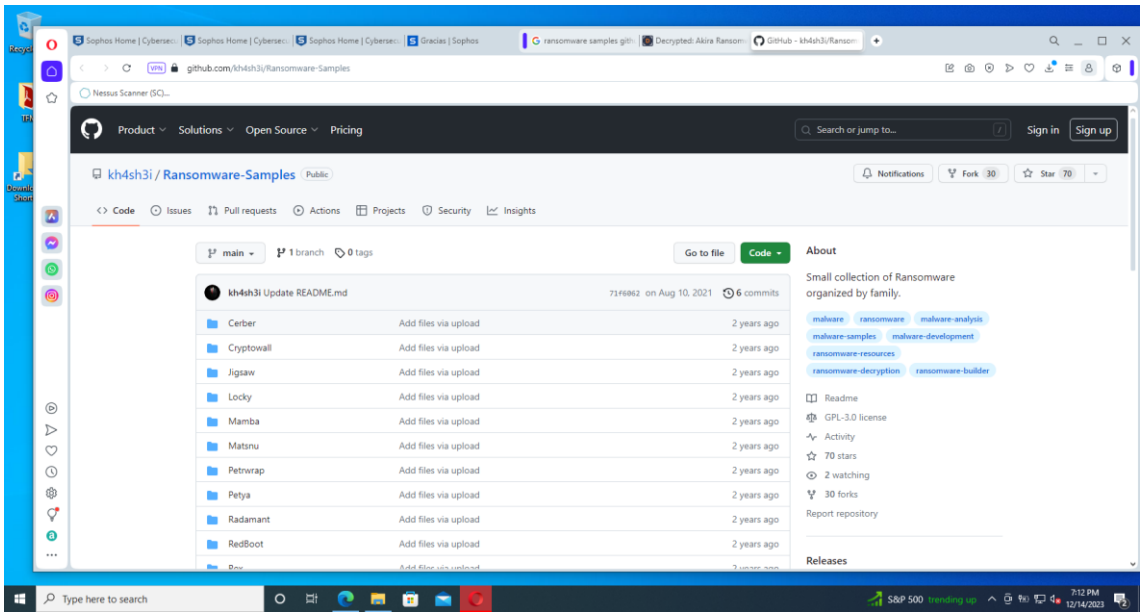


Figura 48: Repositorio GitHub de descarga del malware.

Se procede a extraerlo en disco como se muestra a continuación.

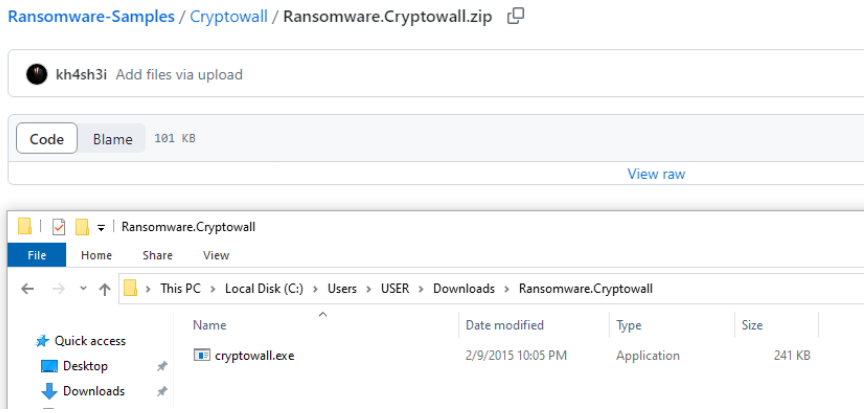


Figura 49: Detalle de la introducción de malware en el sistema víctima.

Una vez se ejecuta, se observa cómo Sophos lo marca como “exploit”, paralizando su ejecución y procediendo a su eliminación.

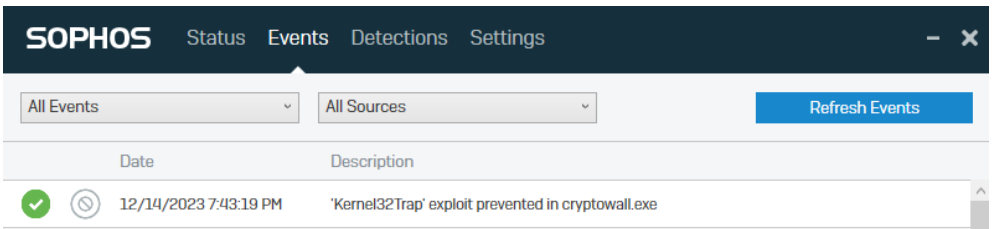


Figura 50: Detalle de la detección del ransomware por Sophos.

Tras ser detectado por Sophos, este envía los logs al cloud de Sophos, y el cloud de Sophos los envía al SIEM. No obstante, este proceso no es inmediato, ya que

se debe esperar a que el cron ejecute el script “siem.py”, el cual se encarga de pasar los logs que guarda en el archivo “result.txt”, al SIEM. Este proceso se describe en el anexo “F. Instalación, configuración e integración en SOC de solución Sophos”.

En la siguiente captura de Kibana se muestran los logs de Sophos de la detección del “exploit”.

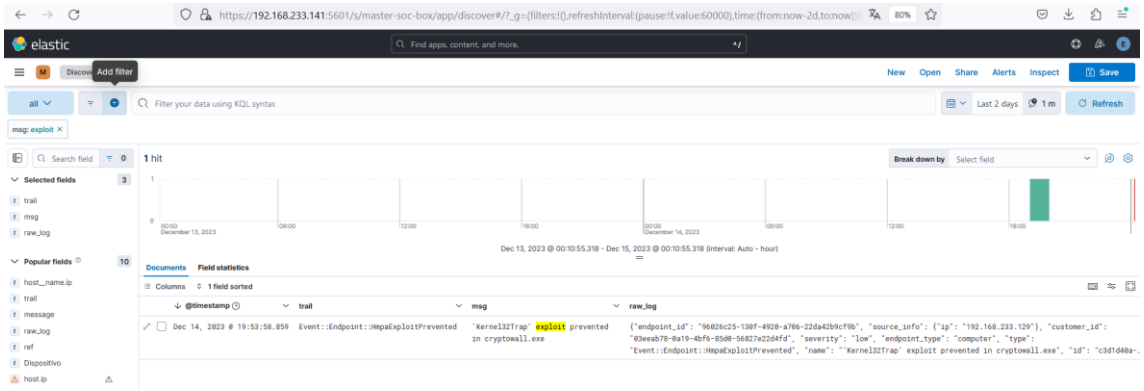


Figura 51: Detalle del Kibana.

De manera paralela, se realiza la ejecución de ElastAlert2, que detecta un patrón coincidente en su regla “exploit.yaml” y emite una alerta por correo electrónico.

```
root@tfm-elk:/home/tfm/elastalert2# python -m elastalert.elastalert --verbose --rule custom_rules/exploit.yaml --config config.yaml --start 2023-12-12
INFO:elastalert:1 rules loaded
INFO:elastalert:Starting up
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.99973 seconds
INFO:elastalert:Queried rule Exploit rule from 2023-12-12 01:00 CET to 2023-12-12 01:15 CET: 0 / 0 hits
INFO:elastalert:Queried rule Exploit rule from 2023-12-12 01:15 CET to 2023-12-12 01:30 CET: 0 / 0 hits
INFO:elastalert:Queried rule Exploit rule from 2023-12-15 00:00 CET to 2023-12-15 00:12 CET: 0 / 0 hits
INFO:elastalert:Sent email to ['info@jaymonsecurity.com']
INFO:elastalert:Ran Exploit rule from 2023-12-12 01:00 CET to 2023-12-15 00:12 CET: 0 query hits (0 already seen), 1 matches, 1 alerts sent
INFO:elastalert:Exploit rule range 256343
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.999201 seconds
INFO:elastalert:Background configuration change check run at 2023-12-15 00:13 CET
INFO:elastalert:Background alerts thread 0 pending alerts sent at 2023-12-15 00:13 CET
^CINFO:elastalert:SIGINT received, stopping ElastAlert...
root@tfm-elk:/home/tfm/elastalert2#
```

Figura 52: Detalle de la ejecución de ElastAlert2.

A continuación, se muestra el correo electrónico de la alerta que ElastAlert2 ha enviado con los detalles correspondientes.

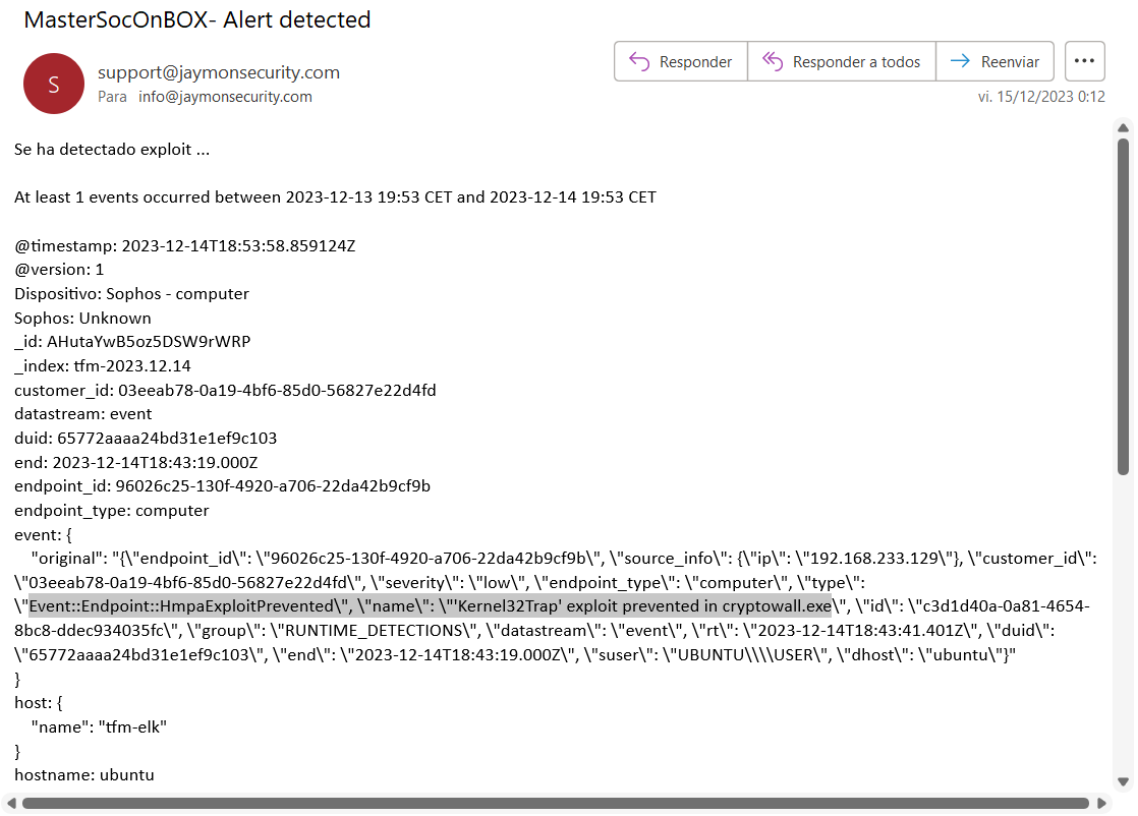


Figura 53: Detalle del email enviado por ElastAlert2.

3.1.2.5.2 Detección y alerta de Ransomware.

Para realizar esta prueba, se ha optado por el ransomware WannaCry. Este ransomware ganó notoriedad mundial tras un ataque masivo en mayo de 2017, en el que se propagó aprovechando una vulnerabilidad en los sistemas operativos Windows, conocida como EternalBlue, la cual había sido desarrollada inicialmente por la Agencia de Seguridad Nacional de Estados Unidos (NSA) y luego filtrada por el grupo de hackers "The Shadow Brokers".

Sin más preámbulos se procede con la prueba de concepto. En la siguiente captura se muestra el ransomware descargado y extraído en el disco de la máquina víctima.

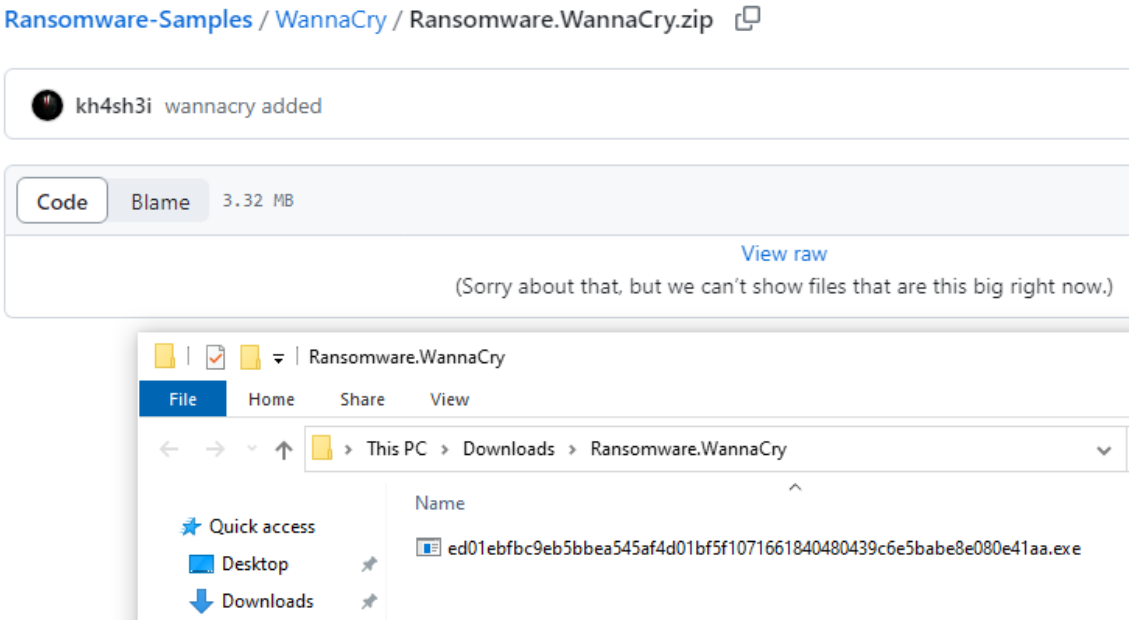


Figura 54: Detalle de la introducción del ransomware en el sistema víctima.

Tras su ejecución se muestra como Sophos lo detecta satisfactoriamente, parando su ejecución y eliminándolo.

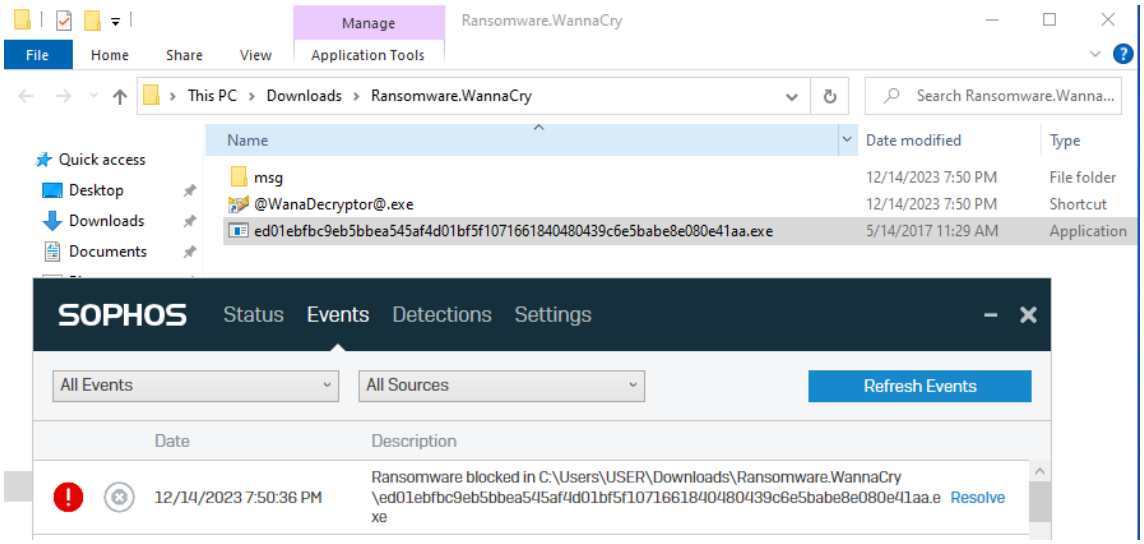


Figura 55: Detalle de la detección del ransomware por Sophos.

Estas acciones también pueden verse en el panel del cloud de Sophos.

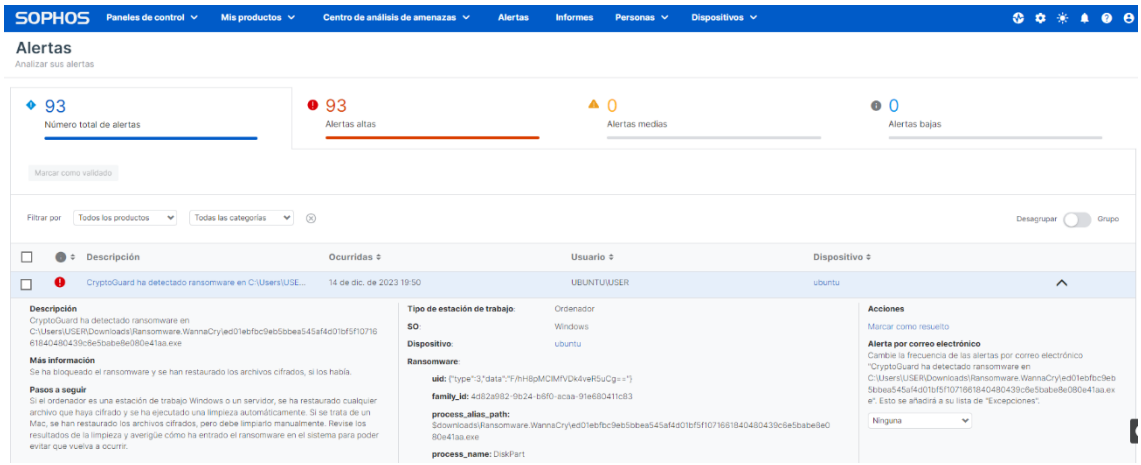


Figura 56: Detalle del panel de control de Sophos Cloud.

Tras ser detectado por Sophos, este envía los logs al cloud de Sophos, y el cloud de Sophos los envía al SIEM, siguiendo un proceso ya comentado en puntos anteriores.

En la siguiente captura de Kibana se muestran los logs de Sophos de la detección del ransomware.

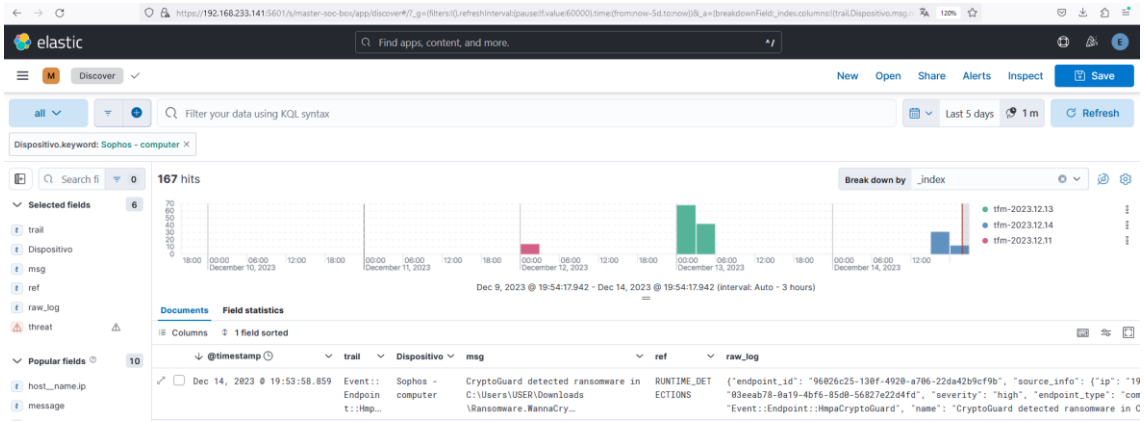


Figura 57: Detalle del Kibana.

De manera paralela, se realiza la ejecución de ElastAlert2, que detecta un patrón coincidente en su regla “ransomrules.yaml” y emite una alerta por correo electrónico.

```
root@tfm-elk:/home/tfm/elastalert2# python -m elastalert.elastalert --verbose --rule custom_rules/ransomrules.yaml --config config.yaml --start 2023-12-14
INFO:elastalert:1 rules loaded
INFO:elastalert:Starting up
INFO:elastalert:Disabled rules are: []
INFO:elastalert:Sleeping for 59.999885 seconds
INFO:elastalert:Queried rule Ransomware rule from 2023-12-14 01:00 CET to 2023-12-14 01:15 CET: 0 / 0 hits
INFO:elastalert:Queried rule Ransomware rule from 2023-12-14 01:15 CET to 2023-12-14 01:30 CET: 0 / 0 hits
INFO:elastalert:Queried rule Ransomware rule from 2023-12-14 01:30 CET to 2023-12-14 01:45 CET: 0 / 0 hits
INFO:elastalert:Queried rule Ransomware rule from 2023-12-14 01:45 CET to 2023-12-14 02:00 CET: 0 / 0 hits
INFO:elastalert:Queried rule Ransomware rule from 2023-12-14 02:00 CET to 2023-12-14 02:15 CET: 0 / 0 hits
INFO:elastalert:Sent email to ['info@jaymonsecurity.com']
INFO:elastalert:Ran Ransomware rule from 2023-12-14 01:00 CET to 2023-12-14 23:40 CET: 0 query hits (0 already seen), 1 matches, 1 alerts sent
INFO:elastalert:Ransomware rule range 81633
^CINFO:elastalert:SIGINT received, stopping ElastAlert...
root@tfm-elk:/home/tfm/elastalert2#
```

Figura 58: Detalle de la ejecución de ElastAlert2.

A continuación, se muestra el correo electrónico de la alerta que ElastAlert2 ha enviado con los detalles correspondientes.

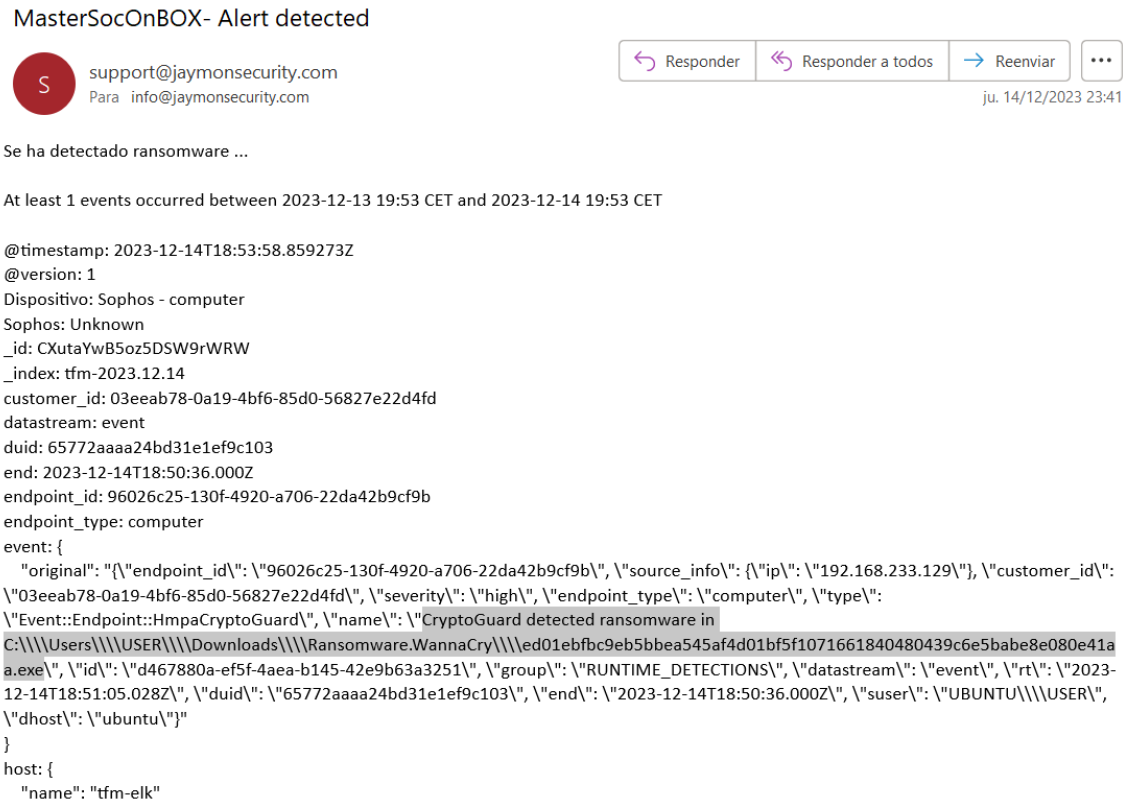


Figura 59: Detalle del email enviado por ElastAlert2.

3.1.2.5.3 Detección y alerta de Malware.

A continuación, se muestra cómo se detecta malware tras introducir en la máquina de Windows distintos tipos de malware, como son un archivo PDF infectado y dos aplicaciones HTA maliciosas

En la siguiente captura se observa cómo se introduce el malware en la máquina Windows con la solución Sophos instalada, a través de una carpeta compartida con otro equipo Windows que se encuentra bajo la misma Red de Área Local (LAN).

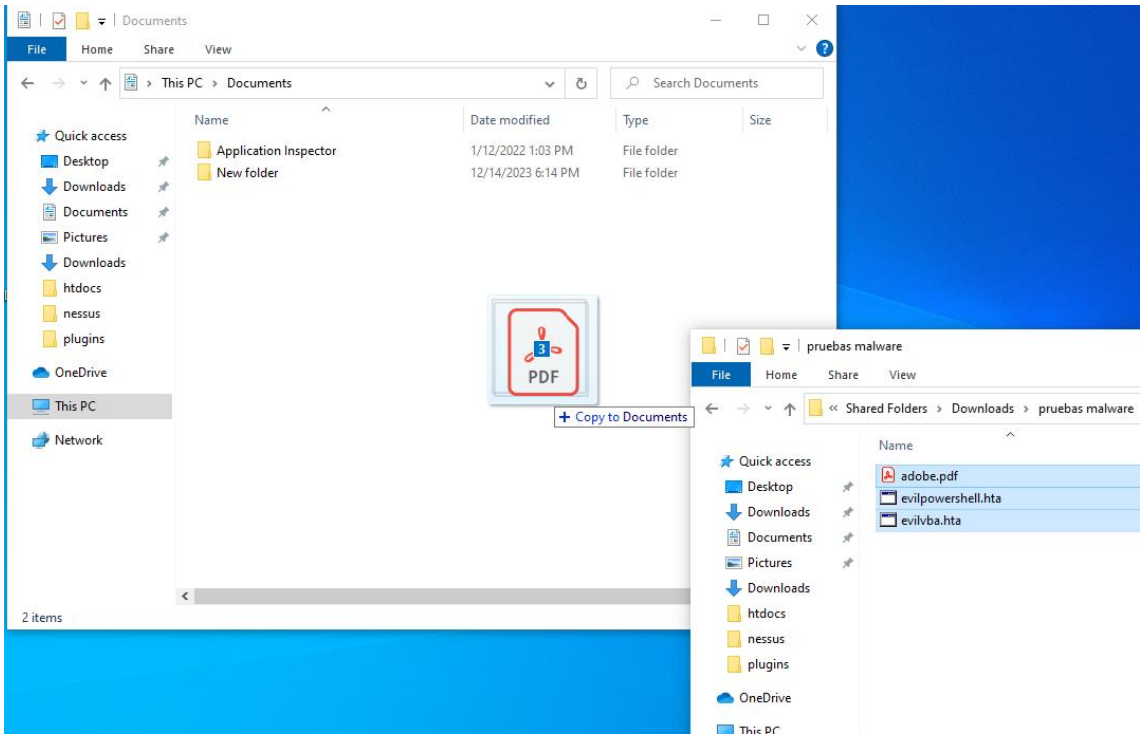


Figura 60: Detalle de la introducción de malware en el sistema víctima.

Tras ser detectados por Sophos, este envía los logs al cloud de Sophos, y el cloud de Sophos los envía al SIEM, pudiéndose observar el resultado en el Kibana.

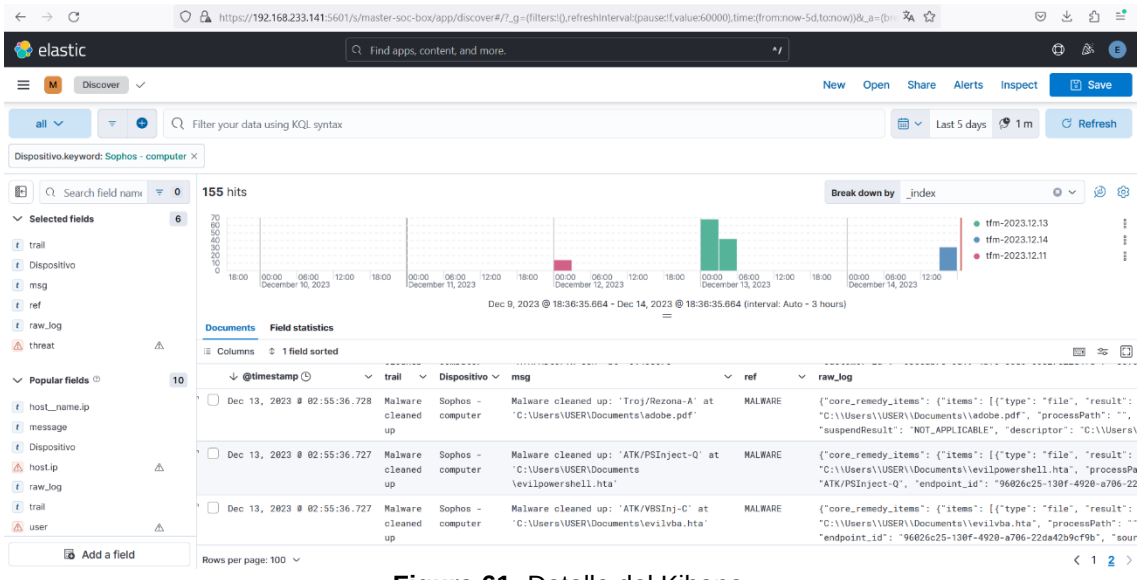


Figura 61: Detalle del Kibana.

De manera paralela, se realiza la ejecución de ElastAlert2, que detecta un patrón coincidente en su regla “malwareinjection.yaml” y emite una alerta por correo electrónico.

```
INFO:elastalert:Sent email to ['info@jaymonsecurity.com']
INFO:elastalert:Ignoring match for silenced rule Malware rule
INFO:elastalert:Ignoring match for silenced rule Malware rule
INFO:elastalert:Ignoring match for silenced rule Malware rule
INFO:elastalert:Ignoring match for silenced rule Malware rule
INFO:elastalert:Ignoring match for silenced rule Malware rule
INFO:elastalert:Ran Malware rule from 2023-12-11 01:00 CET to 2023-12-12 17:41 CET: 0 query hits (0 already seen), 6 matches, 1 alerts sent
INFO:elastalert:Malware rule range 405709
```

Figura 62: Detalle de la ejecución de ElastAlert2.

En la siguiente captura se muestra el correo electrónico emitido por “ElastAlert2” con los detalles de la alerta generada.

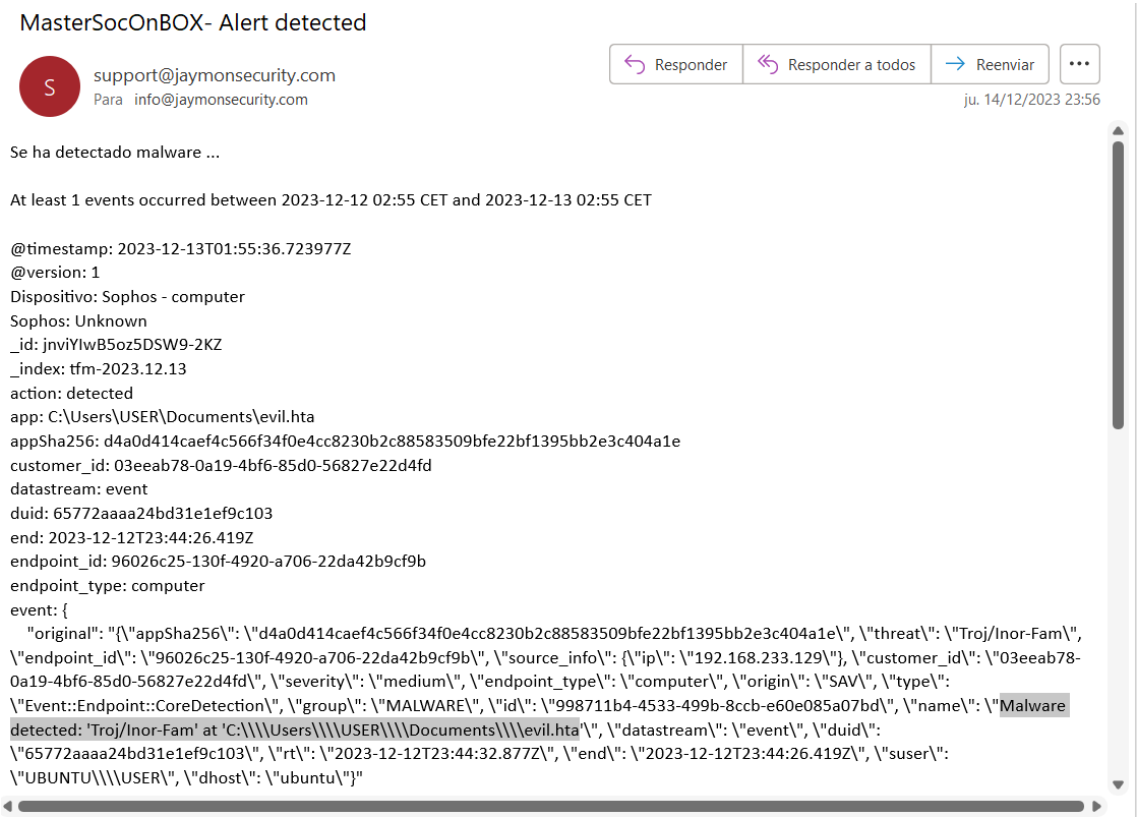
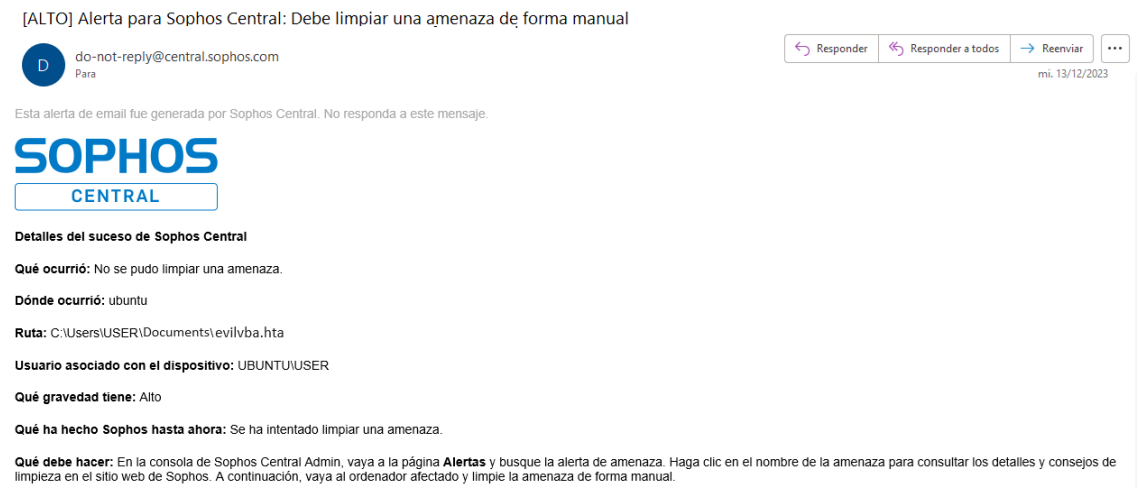


Figura 63: Detalle del email enviado por ElastAlert2.

De la misma manera, cabe destacar que la propia solución Sophos también tiene la capacidad de emitir ciertas alertas vía correo electrónico, aunque no tiene la capacidad de ser tan flexible como “ElastAlert2”, donde se pueden crear todas las alertas que se requieran a conveniencia.



[ALTO] Alerta para Sophos Central: Debe limpiar una amenaza de forma manual

do-not-reply@central.sophos.com
Para

Responder | Responder a todos | Reenviar | ...
mi. 13/12/2023

Esta alerta de email fue generada por Sophos Central. No responda a este mensaje.

SOPHOS CENTRAL

Detalles del suceso de Sophos Central

Qué ocurrió: No se pudo limpiar una amenaza.

Dónde ocurrió: ubuntu

Ruta: C:\Users\USER\Documents\evilvba.hta

Usuario asociado con el dispositivo: UBUNTU\USER

Qué gravedad tiene: Alto

Qué ha hecho Sophos hasta ahora: Se ha intentado limpiar una amenaza.

Qué debe hacer: En la consola de Sophos Central Admin, vaya a la página **Alertas** y busque la alerta de amenaza. Haga clic en el nombre de la amenaza para consultar los detalles y consejos de limpieza en el sitio web de Sophos. A continuación, vaya al ordenador afectado y limpie la amenaza de forma manual.

Figura 64: Detalle del email enviado por Sophos.

3.1.2.5.4 Detección y alerta de navegación segura.

Para llevar a cabo esta prueba se ha hecho uso de los distintos módulos de la herramienta AMTSO.

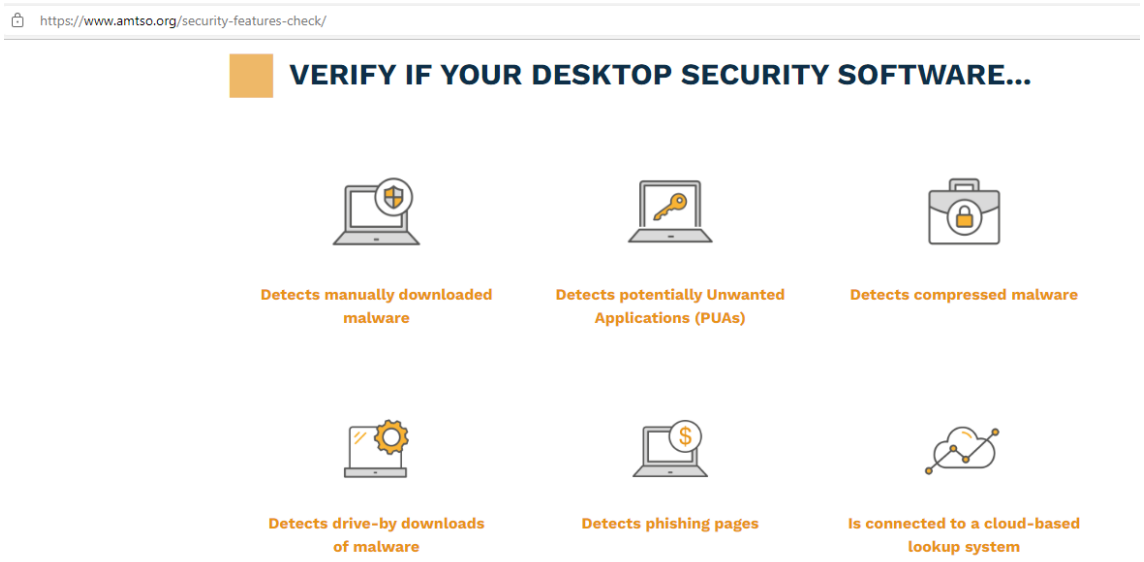


Figura 65: Detalle de las pruebas AMTSO.

Tras ser detectados por Sophos, este envía los logs al cloud de Sophos, y el cloud de Sophos los envía al SIEM, pudiéndose observar el resultado en Kibana.

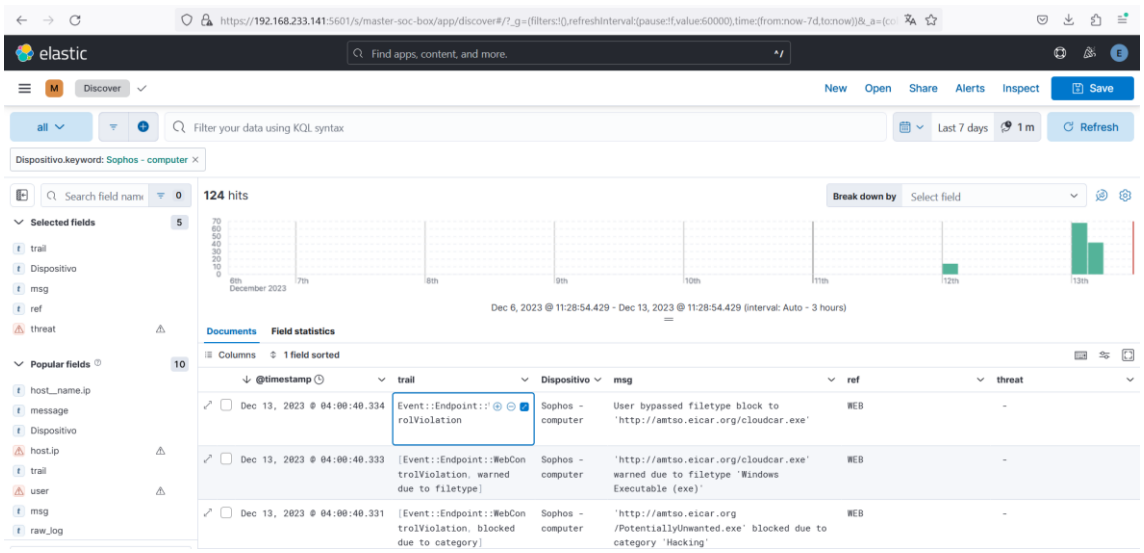


Figura 66: Detalle del Kibana.

De manera paralela, se realiza la ejecución de “ElastAlert2”, que detecta un patrón coincidente en su regla “webcontrolviolation.yaml” y emite una alerta por correo electrónico.

```
INFO:elastalert:Sent email to ['info@jaymonsecurity.com']
INFO:elastalert:Ignoring match for silenced rule WebControlViolation rule
INFO:elastalert:Ignoring match for silenced rule WebControlViolation rule
INFO:elastalert:Ran WebControlViolation rule from 2023-12-11 01:00 CET to 2023-12-12 17:48 CET: 0 query hits (0 already seen), 3 matches, 1 alerts sent
INFO:elastalert:WebControlViolation rule range 406115
```

Figura 67: Detalle de la ejecución de ElastAlert2.

A continuación, se muestra el correo electrónico de la alerta que ElastAlert2 ha enviado con los detalles correspondientes.

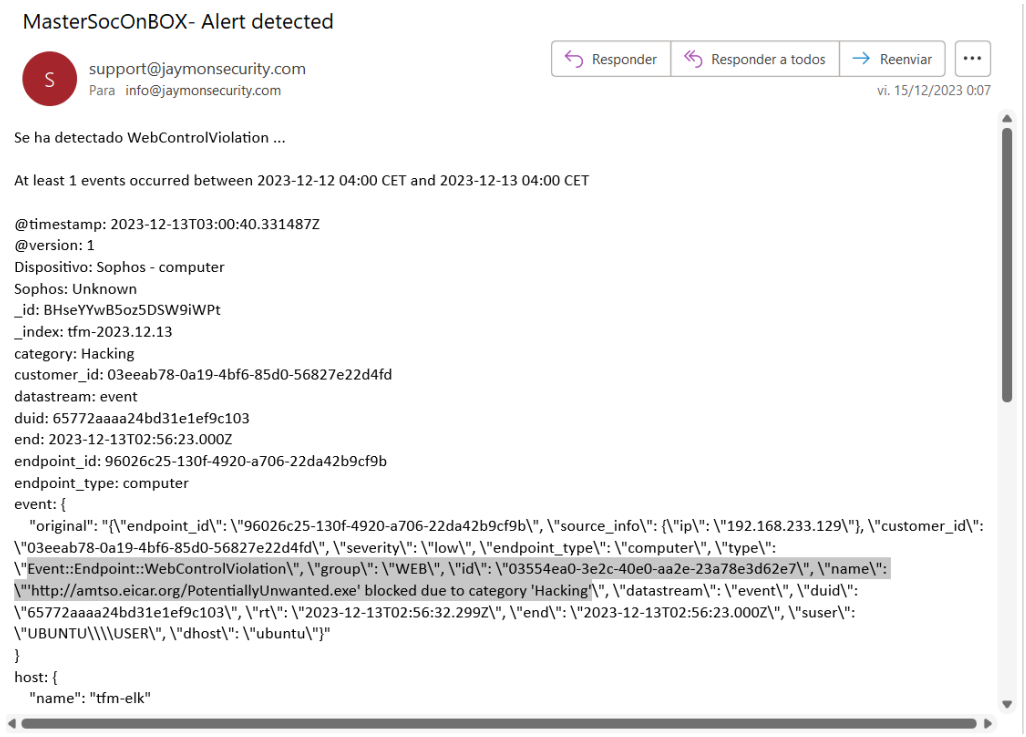


Figura 68: Detalle del email enviado por ElastAlert2.

4. Conclusiones y trabajos futuros.

Al inicio de este proyecto, el autor tenía un conocimiento básico y una percepción particular de cada herramienta incluida en el Master SOC on BOX. Esta visión estaba centrada principalmente en las funciones y capacidades específicas de cada componente por separado. Sin embargo, a lo largo del desarrollo de este trabajo, el autor ha adquirido una comprensión más amplia y detallada. Este proceso ha permitido al autor ver cómo cada herramienta se integra y contribuye al funcionamiento general del sistema, y ha revelado la sinergia entre las diferentes herramientas y cómo su interacción conduce a una mayor eficacia en la detección, análisis y respuesta a incidentes de seguridad.

Esta perspectiva integral es fundamental para entender el “Master SOC on BOX” como un sistema cohesivo y dinámico, capaz de adaptarse y responder de manera efectiva a los desafíos de seguridad en constante evolución. Con esta visión global, el autor ahora puede apreciar cómo las estrategias y decisiones tomadas en un área pueden impactar y mejorar las operaciones en otra, resultando en un enfoque de seguridad más robusto y eficiente.

A continuación, se detallan las conclusiones de este trabajo en cuanto a:

- **Efectividad del "Master SOC on Box"**.
  - Los resultados obtenidos tras implementar el "Master SOC on Box" indican una mejora notable en la capacidad de detección y respuesta a incidentes de seguridad. Se ha observado una integración fluida de diversas herramientas de seguridad, lo que ha mejorado significativamente la visión general y el control sobre las amenazas de seguridad.
  - La combinación de tecnologías como IDS (Suricata), HIDS (Wazuh), Firewall (FortiGate), XDR (Sophos) y el uso del Stack ELK para SIEM ha proporcionado una plataforma robusta y eficiente para la monitorización de seguridad, análisis de datos y respuesta a incidentes.

- **Expectativas y resultados sorprendentes**.
  - Aunque se esperaba una mejora en la seguridad general, los resultados han sido sorprendentemente positivos. La eficiencia en la detección de amenazas y la respuesta rápida a incidentes han superado las expectativas iniciales.
  - Lo sorprendente radica en cómo la integración y automatización de procesos no solo mejoró la seguridad, sino que también optimizó la gestión del tiempo y los recursos. La capacidad de alertas que “ElastAlert2” puede proporcionar, combinada con la monitorización proactiva de Wazuh, Suricata, FortiGate y Sophos, ha contribuido a una disminución significativa en el tiempo de respuesta a incidentes.

- La escalabilidad y adaptabilidad del sistema han sido mayores de lo esperado, permitiendo al ayuntamiento ajustarse rápidamente a las cambiantes necesidades de seguridad y a nuevos desafíos.

De todo lo anterior, se deduce que el "Master SOC on Box" ha demostrado ser una solución integral y eficaz para las necesidades de seguridad de un ayuntamiento, superando las expectativas iniciales en varios aspectos fundamentales. Su diseño y la implementación de diversas tecnologías han facilitado una operación de seguridad más cohesiva, ágil y eficiente. Además, la capacidad de adaptación del sistema asegura su relevancia y efectividad a largo plazo frente a un panorama de amenazas en constante evolución. Así pues, la combinación de tecnologías y la implementación de prácticas ágiles han resultado en un SOC funcional, innovador y proactivo en su enfoque de la seguridad cibernética.

Como reflexión crítica sobre la consecución de los objetivos inicialmente planteados en el proyecto del "Master SOC on Box", se detallan los siguientes puntos.

1. **Alcance de los objetivos establecidos**.
   - Los objetivos propuestos de mejora en la detección de amenazas, eficiencia operativa y respuesta rápida a incidentes se han cumplido correctamente. Todos los resultados han sido positivos, y cabe destacar que cada objetivo de manera individual también ha tenido un grado de cumplimiento satisfactorio.

2. **Evaluación de la implementación tecnológica**.
   - Con la integración de diversas tecnologías (como IDS, HIDS, SIEM), se han cumplido con las expectativas y necesidades del ayuntamiento. Así pues, han funcionado las herramientas de manera sinérgica, optimizando los recursos y minimizando los riesgos de seguridad.

3. **Adaptabilidad y escalabilidad**.
   - El sistema ha demostrado ser adaptable y escalable, especialmente frente a los desafíos de seguridad cambiantes y las necesidades en evolución del ayuntamiento.

4. **Capacitación y habilidades del personal**.
   - La falta de experiencia del personal de IT del ayuntamiento en ciertas tecnologías avanzadas constituye un desafío significativo. Por ello se propuso el modelo de SOC híbrido, solucionando de esta manera la falta de formación del personal mencionado.

5. **Gestión de alertas y falsos positivos**.
   - La gestión de un alto volumen de alertas, incluyendo la reducción de falsos positivos, fue un desafío operativo considerable, lo que en ocasiones llevó a ciertas sobrecargas. Así pues, se ajustaron y refinaron las reglas de alerta y se integraron soluciones para mejorar la precisión. Este proceso puso de manifiesto la necesidad

de una gestión dinámica de alertas y la adaptación constante de los umbrales de detección.

Al reflexionar críticamente, se debe reconocer que, aunque el "Master SOC on Box" ha alcanzado todos los objetivos iniciales planteados en este TFM, como cualquier proyecto complejo, es probable que haya áreas que requieran ajustes y mejoras continuas. Esta evaluación crítica no solo valida el éxito del proyecto hasta la fecha, sino que también proporciona una base para el crecimiento y la mejora continuos, asegurando que el SOC siga siendo efectivo y relevante en el dinámico campo de la ciberseguridad.

En cuanto a lo que concierne al seguimiento de la planificación y metodología del TFM, realizar un análisis crítico de este implica una evaluación detallada de cómo se han aplicado estas estrategias a lo largo del desarrollo del proyecto. Así pues, se detallan los siguientes puntos.

1. **Cumplimiento de los plazos establecidos**.
    - En el desarrollo del proyecto "Master SOC on Box", se logró un cumplimiento notable de todos los plazos establecidos para cada fase. Esta eficiencia en el manejo del tiempo evidencia una planificación y ejecución excepcionales del proyecto. La puntualidad en alcanzar cada hito demuestra una gestión de tiempo efectiva, y una excelente capacidad para mantenerse en el cronograma, a pesar de los desafíos inherentes a proyectos de esta envergadura, lo que refleja una combinación exitosa de anticipación proactiva y adaptabilidad dinámica. Sin duda este logro es un indicador de buenas prácticas en la gestión de proyectos.

2. **Gestión de recursos.**
    - Se observó que, en algunos casos, los recursos tecnológicos podrían haberse optimizado mejor, evitando redundancias y maximizando el uso de las herramientas existentes.
    - La revisión de la asignación de recursos en diferentes fases del proyecto sugiere que una planificación más flexible y una evaluación continua podrían haber conducido a una utilización más eficiente de los recursos.

3. **Eficacia de la metodología elegida.**
    - La metodología elegida ha sido fundamental para alcanzar los objetivos de manera eficiente, particularmente en términos de estructura y claridad en el proceso de implementación.
    - Sin embargo, se identificó que, aunque la metodología facilitó la solución de problemas, hubo margen para mayor innovación. En futuros proyectos, incorporar enfoques que fomenten la creatividad podría mejorar aún más los resultados.

4. **Integración de herramientas y procesos.**

- La metodología proporcionó una guía clara para la integración de diferentes componentes del SOC, lo que resultó en un sistema cohesivo y funcional.
- Sin embargo, hubo desafíos en la integración de ciertas herramientas avanzadas, lo que sugiere que una metodología con mayor énfasis en la adaptabilidad tecnológica podría haber sido beneficiosa.

5. **Adaptabilidad y flexibilidad.**
    - La metodología permitió ajustes durante el proyecto, lo que fue fundamental para abordar desafíos inesperados y cambios en el entorno de seguridad.
    - Sin embargo, futuras metodologías podrían beneficiarse de una mayor flexibilidad incorporada, permitiendo una adaptación más rápida y fluida a las circunstancias cambiantes sin afectar los resultados del proyecto.

Mientras que la gestión de recursos, la eficacia de la metodología, la integración de herramientas y la flexibilidad han sido en general efectivas en el proyecto "Master SOC on Box", la revisión crítica ha revelado áreas de mejora. Estas lecciones aprendidas son valiosas para la mejora continua y la planificación de futuros proyectos similares.

En cuanto a lo que concierne a la evaluación de impactos descritos en el punto “1.4. Impacto en sostenibilidad, ético-social y de diversidad”, se concluye lo siguiente:

- **Sostenibilidad.**
    - **Impactos positivos logrados**: La implementación del SOC con ELK Stack en ayuntamientos ha contribuido a una mayor eficiencia y resiliencia en la Administración Pública. Esto ha llevado a una reducción potencial de los costos asociados con incidentes de seguridad, logrando una asignación más sostenible de recursos financieros.
    - **Impactos negativos mitigados**: Aunque la implementación inicial supuso un aumento en el gasto y en el consumo energético, se han tomado medidas para optimizar la eficiencia energética de los centros de datos y servidores. Además, el ahorro a largo plazo en costos de gestión y respuesta a incidentes compensa este gasto inicial.

- **Ético-social.**
    - **Impactos positivos logrados**: La robustez en la ciberseguridad ha reforzado la protección de los datos personales, respetando el deber legal y ético de proteger la privacidad e integridad de la información ciudadana. Esto ha generado una mayor confianza en la Administración Pública y ha fortalecido su compromiso con el bienestar social.

  - **Impactos negativos mitigados**: Se han establecido estrictas políticas y controles para asegurar que las soluciones de monitorización y seguridad no se utilicen de manera no ética. Esto incluye la implementación de salvaguardas para prevenir la vigilancia invasiva y la violación de derechos fundamentales.

- **Diversidad.**
  - **Impactos positivos logrados**: El proyecto ha garantizado que todos los ciudadanos, sin importar su origen, género, edad o capacidad, tengan acceso equitativo a servicios públicos digitales seguros. Esto ha fomentado la inclusión y asegurado la no discriminación en el acceso a la información y protección de datos.
  - **Impactos negativos mitigados**: Se ha puesto especial atención en el diseño de interfaces y protocolos accesibles para atender a las diversas necesidades y capacidades de los usuarios. Esto ha ayudado a evitar la creación de barreras tecnológicas y ha garantizado el cumplimiento de las normativas de diversidad.

El "Master SOC on Box" ha logrado impactos notablemente positivos en términos de sostenibilidad, ética social y diversidad. Los impactos negativos han sido efectivamente identificados y mitigados a través de estrategias conscientes y proactivas. De este modo, el proyecto no solo ha mejorado la seguridad cibernética, sino que también ha contribuido al bienestar y la equidad en la sociedad, alineándose con los valores éticos y principios de sostenibilidad.

Para finalizar, siempre es de gran importancia identificar áreas y líneas de trabajo futuro que no se abordaron durante el proyecto, y que ofrecen oportunidades para exploraciones y mejoras adicionales. A continuación, se detallan estas áreas, así como las líneas de trabajo futuro identificadas.

1. **Integración con tecnologías emergentes**.
   - Explorar la integración del SOC con tecnologías emergentes como la inteligencia artificial (IA) y el aprendizaje automático para mejorar aún más la detección de amenazas y la respuesta automatizada a incidentes.
   - Investigar el potencial de las tecnologías blockchain para mejorar la seguridad y trazabilidad de las transacciones y operaciones dentro de la red del ayuntamiento.

2. **Expansión de capacidades de análisis predictivo**.
   - Desarrollar capacidades de análisis predictivo para anticipar y prevenir amenazas antes de que se materialicen.
   - Implementar modelos de análisis de comportamiento para identificar actividades sospechosas de manera más eficiente.
   - Desarrollar y entrenar modelos de “Machine Learning” (ML) para detectar comportamientos anómalos de manera más inteligente. Esto podría basarse en una red neuronal que se retroalimente continuamente con información de ciberataques realizados a dispositivos tipo “honeypots”, y otras fuentes de datos.

3. **Mejora en la gestión de alertas y respuestas**.
    - Implementar sistemas de correlación de alertas que, al detectar la repetición de un mismo tipo de alerta dentro de un período específico, generen una alerta de nivel superior que requiera una respuesta inmediata del equipo de SOC. Por ejemplo, si un tipo de alerta ocurre tres veces en una hora, se activaría una alerta prioritaria.
    - Crear un módulo de orquestación que permita ejecutar acciones automatizadas basadas en diversos casos de uso y correlaciones de eventos. Esto podría incluir la capacidad de poner en cuarentena o en listas negras direcciones IP maliciosas o sospechosas de forma automática, entre otras acciones.

4. **Expansión de casos de uso y aplicación de la matriz MITRE ATT&CK**.
    - Llevar a cabo la implementación de todos los casos de uso presentados en el anexo J. Estos son esenciales para identificar operaciones de un adversario en diferentes etapas y para reconocer eventos aparentemente insignificantes que podrían ser indicativos de un ataque más amplio.
    - La relevancia de contar con una amplia variedad de casos de uso (reglas que generan alertas) y sus procedimientos asociados (instrucciones sobre cómo responder a ellos para analizar y mitigar) se centra en que, al implementarlos adecuadamente, se dificulta bastante la capacidad de un atacante para pasar desapercibido por el Centro de Operaciones de Seguridad (SOC) que los haya activado.
    - Alinear y asociar la detección y respuesta de seguridad con las etapas de la Matriz MITRE ATT&CK. Esto ayudará en la identificación y mitigación de amenazas, así como en la atribución a grupos APT específicos.

5. **Desarrollo de estrategias de respuesta a incidentes a largo plazo**.
    - Formular y probar planes de respuesta a incidentes a largo plazo, incluyendo la recuperación ante desastres y la continuidad del negocio.
    - Crear simulacros de seguridad más complejos y realistas para evaluar y mejorar estas estrategias.

6. **Mejoras en la gestión de la diversidad y la inclusión**.
    - Investigar y desarrollar estrategias para mejorar la accesibilidad y la inclusión en todos los aspectos del SOC, asegurando que las soluciones sean accesibles para una gama más amplia de usuarios.

7. **Estudio del impacto ambiental y sostenibilidad**.
    - Realizar un estudio más profundo sobre el impacto ambiental de los centros de datos y servidores utilizados en el SOC.

- Desarrollar estrategias para mejorar la sostenibilidad, como la optimización del uso de energía y la adopción de soluciones más ecológicas.

8. **Colaboración y conformidad regulatoria**.
   - Fortalecer la colaboración con otras entidades gubernamentales y organizaciones para compartir conocimientos y recursos, como bases de datos de indicadores de compromiso (IOC), entre otros de interés.
   - Mantenerse al día y adaptarse a las cambiantes regulaciones y normativas en materia de ciberseguridad y protección de datos.

9. **Ampliación de la cobertura de seguridad**.
   - Expandir la cobertura del SOC para incluir más áreas de la infraestructura tecnológica del ayuntamiento.
   - Explorar la posibilidad de ofrecer servicios de SOC a otras entidades locales o regionales como parte de un esfuerzo colaborativo.

Con estos trabajos futuros se ampliará notablemente la capacidad del "Master SOC on Box" para responder a las amenazas actuales y emergentes, y además lo posicionarán como una solución de seguridad cibernética avanzada y adaptable, capaz de enfrentar los desafíos venideros.

5. Glosario.

- **Administración Electrónica (e-Government):** Aplicación de tecnologías digitales para proporcionar servicios gubernamentales y mejorar la interacción con la ciudadanía y empresas.
- **AMTSO:** La Organización de Estándares de Pruebas Anti-Malware (Anti-Malware Testing Standards Organization) es un grupo internacional que desarrolla estándares para la evaluación de productos de seguridad informática, específicamente aquellos diseñados para detectar y prevenir malware.
- **Antivirus:** Programa que busca, previene y elimina software malicioso de los dispositivos.
- **Ataque de Fuerza Bruta:** Es un método de prueba y error utilizado para obtener información como una contraseña o PIN. En este ataque, un atacante intenta muchas combinaciones de contraseñas o claves con la esperanza de eventualmente adivinar correctamente.
- **Auditorías de seguridad:** Revisiones meticulosas de las prácticas de seguridad de una organización.
- **Balanceadores de carga:** Tecnologías que reparten el tráfico de red entre servidores para equilibrar la carga.
- **Bastionado del servidor:** Proceso de fortalecimiento de la seguridad de un servidor para proteger contra ataques.
- **Chain Attack:** Un ataque en cadena o "chain attack" se refiere a un tipo de ataque cibernético en el cual el atacante utiliza múltiples vulnerabilidades en una secuencia para penetrar y comprometer un sistema o red.
- **Ciberataques:** Acciones malintencionadas que buscan dañar o acceder sin autorización a sistemas y redes informáticos.
- **Ciberinteligencia de amenazas:** Recopilación y análisis de datos sobre amenazas potenciales para prevenir ataques cibernéticos.
- **Cifrado de datos:** Proceso de codificar datos para proteger su confidencialidad e integridad.
- **Cumplimientos normativos:** Alineación con leyes y reglamentos aplicables a una industria o sector específico.
- **Dashboard:** Interfaz que muestra métricas clave y estadísticas relevantes de forma resumida.
- **Desarrollo sostenible:** Desarrollo que cumple con las necesidades actuales sin comprometer recursos futuros.
- **EDR (Endpoint Detection and Response):** Es una tecnología de seguridad que se centra en la detección, investigación y mitigación de actividades sospechosas en los endpoints o dispositivos finales.
- **Elastic Stack (ELK Stack):** Un conjunto de aplicaciones de código abierto para la búsqueda, análisis y visualización de datos en tiempo real. Incluye Elasticsearch, Logstash y Kibana.
- **Elasticsearch:** Motor de búsqueda y análisis que proporciona búsqueda en texto completo y capacidades de análisis distribuido.
- **ElastAlert2:** Herramienta para crear alertas en base a patrones en datos dentro de Elasticsearch.

- **Escala:** Capacidad de un sistema para aumentar su capacidad en respuesta a la demanda.
- **Escaneo de Puertos:** Es una técnica utilizada para identificar puertos abiertos en una computadora o servidor. Se usa tanto en la administración de redes como en actividades maliciosas para encontrar servicios accesibles o vulnerabilidades.
- **Esquema Nacional de Seguridad (ENS):** Conjunto de normas en España para proteger la información en el uso de medios electrónicos.
- **EternalBlue:** Es el nombre de una vulnerabilidad de seguridad en las versiones antiguas de Windows que fue explotada por varios ataques de ransomware, incluyendo WannaCry.
- **Exploit:** Un "exploit" en el contexto de la seguridad informática se refiere a una pieza de software, un fragmento de datos, o una secuencia de comandos que aprovecha una vulnerabilidad o fallo en el software para causar comportamientos no previstos en el sistema informático, generalmente con el fin de obtener algún tipo de control sobre el sistema.
- **Firewall:** Dispositivo que filtra el tráfico de red según reglas de seguridad establecidas.
- **Firewall FortiGate:** Dispositivo de seguridad de red que ofrece protección contra amenazas externas, controlando y filtrando el tráfico de entrada y salida en redes informáticas.
- **Firewall pfSense:** Solución de firewall de código abierto y gratuita que también actúa como enrutador de red. Ofrece funciones avanzadas de seguridad, como filtrado de paquetes, NAT, VPN, y control de tráfico. Es altamente personalizable y se adapta tanto a entornos domésticos como empresariales.
- **HIDS:** Sistema de detección de intrusos que opera en un servidor o estación de trabajo individual, controlando el tráfico de datos y las actividades del sistema.
- **Hydra:** Es una herramienta popular de cracking de contraseñas que realiza ataques de fuerza bruta o diccionario para descifrar credenciales de inicio de sesión.
- **IDS:** Sistemas que vigilan redes y sistemas en busca de actividades anómalas que puedan ser indicios de una intrusión.
- **Inyección SQL:** Es una técnica de inyección de código que explota una vulnerabilidad de seguridad en una aplicación que interactúa con una base de datos, permitiendo al atacante ejecutar comandos SQL maliciosos.
- **IOC:** Un Indicador de Compromiso (IOC, del inglés) comprende información crucial que caracteriza incidentes de ciberseguridad, actividades y artefactos maliciosos, identificándolos a través del análisis de sus patrones de comportamiento.
- **Kibana:** Aplicación de visualización de datos para Elasticsearch. Permite la creación de dashboards para visualizar datos de Elasticsearch.
- **Logstash:** Herramienta de procesamiento de datos que ingesta datos de múltiples fuentes, los transforma y los envía a un "stash" como Elasticsearch.
- **Malware:** Software diseñado para dañar o realizar acciones no autorizadas en sistemas informáticos.

- **MITRE ATT&CK:** Es un marco de conocimiento globalmente reconocido que se utiliza para describir y clasificar las tácticas, técnicas y procedimientos (TTP) utilizados por los ciberdelincuentes y actores de amenazas. La sigla ATT&CK significa "Adversarial Tactics, Techniques, and Common Knowledge" (Tácticas, Técnicas y Conocimiento Común de Adversarios).
- **Monitorización de alertas:** Supervisión y análisis de notificaciones automáticas sobre eventos significativos que puedan afectar la seguridad de sistemas o redes.
- **Monitorización de sistemas y redes:** Inspección constante de la infraestructura informática para asegurar su funcionamiento óptimo y seguro.
- **On-premise:** Infraestructura de tecnología de información que se localiza físicamente en las instalaciones de la empresa, en contraste con la nube.
- **Protección de endpoint:** Medidas de seguridad enfocadas en dispositivos terminales conectados a una red.
- **Prueba de concepto (PoC):** Demostración para probar la viabilidad de una idea o método, especialmente en ciberseguridad para mostrar cómo se puede explotar una vulnerabilidad.
- **Ransomware:** Tipo de malware que encripta archivos y exige un rescate para su desbloqueo.
- **Reglamento General de Protección de Datos (RGPD):** Ley de la UE que regula la privacidad y protección de datos personales.
- **SaaS (Software como Servicio):** Software disponible a través de internet provisto por un tercero.
- **SIEM:** Un Sistema de Información de Eventos y Gestión de Seguridad (SIEM, por sus siglas en inglés) es una solución tecnológica en el campo de la seguridad informática. Su función principal es proporcionar una visión integral y en tiempo real de la seguridad de la información dentro de una organización. Un SIEM recopila y analiza datos de seguridad de una variedad de fuentes dentro de una red, incluyendo dispositivos de seguridad, sistemas de red, servidores, bases de datos, aplicaciones y otros sistemas.
- **SOC (Security Operations Center):** Centro que gestiona la seguridad informática en tiempo real, enfocado en identificar, analizar y responder a incidentes cibernéticos.
- **Sophos:** Empresa de ciberseguridad que ofrece productos y servicios para proteger sistemas informáticos.
- **SOAR:** Plataforma que automatiza la recolección y respuesta a incidentes de seguridad.
- **SSH (Secure Shell):** Es un protocolo que proporciona una forma segura de acceder a un sistema remoto. Se utiliza comúnmente para administrar sistemas y aplicaciones de forma remota, y para transferir archivos.
- **Syslog**: Es un estándar para el envío de mensajes de registro en una red IP para el monitoreo y diagnóstico de sistemas. Se utiliza ampliamente para la gestión de registros en sistemas Unix y Linux.
- **TCP (Transmission Control Protocol):** Protocolo de control de transmisión, es un estándar que define cómo se establecen y mantienen

las conexiones de red para que las aplicaciones puedan intercambiar datos.

- **Transparencia:** Apertura y accesibilidad de la información gubernamental para el conocimiento público.
- **UDP (User Datagram Protocol):** Es un protocolo de comunicaciones de la capa de transporte que se utiliza para enviar mensajes cortos llamados datagramas. Es conocido por ser un protocolo sin conexión y proporciona una comunicación rápida, pero sin garantías de entrega.
- **VLAN:** Red de Área Local Virtual, representa una técnica utilizada para formar redes lógicas independientes dentro de una misma infraestructura de red física.
- **WannaCry:** Ransomware conocido por su ataque global en 2017, cifrando archivos y exigiendo rescate en Bitcoin.
- **Wazuh:** Plataforma para la detección de amenazas, monitorización de seguridad y cumplimiento normativo.
- **XDR (Extended Detection and Response):** Es una solución de seguridad que extiende la detección y respuesta más allá de los endpoints tradicionales para incluir redes, cloud, y cargas de trabajo de servidores.

6. Bibliografía.

- Alcober Fuertes, Gabriel. (2020, mayo). "*Arquitectura ELK como herramienta de datos abiertos para Aragón Open Data*" [artículo en línea]. Deloitte [Fecha de consulta: 4 de octubre de 2023]. <https://www2.deloitte.com/es/es/pages/technology/articles/arquitectura-elk-datos-abiertos-aragon-open-data.html>

- Gobierno de España. (2021, enero). "*Plan de Digitalización de las Administraciones Públicas 2021 - 2025*" [artículo en línea]. Gobierno de España [Fecha de consulta: 4 de octubre de 2023]. <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficherof/210127_plan_digitalizacion_administraciones_publicas.pdf>

- Gobierno de España. (2021, diciembre). "*Estudio sobre digitalización de la Administración*" [artículo en línea]. Gobierno de España [Fecha de consulta: 5 de octubre de 2023]. <https://www.ontsi.es/sites/ontsi/files/2021-12/informedigitalizacionAAPPdic21.pdf>

- Salvador, Y. & Llanes, M. & Suárez, M. (2020, septiembre). "*Transformación digital en la Administración Pública: ejes y factores esenciales*" [artículo en línea]. AMELICA [Fecha de consulta: 6 de octubre de 2023]. <http://portal.amelica.org/ameli/jatsRepo/145/1451943011/index.html>

- Cotino, Lorenzo (2023, octubre). "*La digitalización en las Administraciones Públicas en España*" [artículo en línea]. Fundación alternativas [Fecha de consulta: 31 de octubre de 2023]. <https://fundacionalternativas.org/wp-content/uploads/2023/10/DIGITALIZACION_ADMIN_PUBLICAS.pdf>

- Candau, Javier (2021, septiembre). "*Ciberseguridad. Evolución y tendencias*" [artículo en línea]. Instituto Español de Estudios Estratégicos [Fecha de consulta: 31 de octubre de 2023]. < <https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM11_2022_JAVCAND_Ciberseguridad.pdf>

- Álvarez, Manel (2020, septiembre). "*La evolución del SOC ante el nuevo modelo de amenazas.*" [artículo en línea]. UST INSIGHTS [Fecha de consulta: 31 de octubre de 2023]. <https://www.ust.com/es/insights/la-evolucion-del-soc-ante-el-nuevo-modelo-de-amenazas>

- Pérez Arbesú, Lizzette B. (2017, agosto). "*Ocho consideraciones para adoptar un SOC híbrido*" [artículo en línea]. COMPUTERWEEKLY [Fecha de consulta: 16 de noviembre de 2023]. <https://www.computerweekly.com/es/consejo/Ocho-consideraciones-para-adoptar-un-SOC-hibrido>

- Ayuntamiento Madrid (2023, junio). "*Áreas de gobierno y áreas delegadas.*" [artículo en línea]. Ayuntamiento Madrid [Fecha de consulta: 02 de noviembre de 2023]. <https://www.madrid.es/portales/munimadrid/es/Inicio/El-Ayuntamiento/Organizacion-municipal/Areas-de-gobierno-y-areas-delegadas/>

- Glass, E. & Camisso, J. (2022, abril). "*How To Install Elasticsearch, Logstash, and Kibana (Elastic Stack) on Ubuntu 22.04*." [artículo en línea]. DIGITAL OCEAN [Fecha de consulta: 03 de noviembre de 2023]. <https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-22-04>

- Ducre, K. (2018, agosto). "*How to Install Elastic Stack on Ubuntu 22.04 LTS.*" [artículo en línea]. DEVOPS [Fecha de consulta: 03 de noviembre de 2023]. <https://blog.devops.dev/how-to-install-elastic-stack-on-ubuntu-22-04-lts-18c3d9120494>

- El Bazi, Zakaria (2020, noviembre). "*wazuh-elk-searchguard*." [artículo en línea]. GITHUB [Fecha de consulta: 05 de noviembre de 2023]. <https://GitHub.com/Z4ck404/wazuh-elk-searchguard>

- Informatica (2019, mayo). "*Configurar Elasticsearch.*" [artículo en línea]. Informatica [Fecha de consulta: 06 de noviembre de 2023]. <https://docs.informatica.com/es_es/master-data-management/multidomain-mdm/10-3/actualizar-desde--version-9-5-1/actualizacion-de-la-configuracion-de-busqueda/paso-1--configurar-elasticsearch.html>

- De Luz, Sergio (2023, mayo). "*Configura pfSense para proteger tu hogar o empresa con este firewall.*" [artículo en línea]. Redeszone [Fecha de consulta: 06 de noviembre de 2023]. <https://www.redeszone.net/tutoriales/seguridad/pfsense-firewall-profesional-configuracion/>

- Marquardt, Alex (2020, febrero). "*Cómo crear pipelines de Logstash que se puedan mantener y volver a usar.*" [artículo en línea]. Elastic [Fecha de consulta: 07 de noviembre de 2023]. < https://www.elastic.co/es/blog/how-to-create-maintainable-and-reusable-logstash-pipelines

- García, Sergio (2020, mayo). "*¿Qué es Logstash? + Ejemplo práctico de uso.*" [artículo en línea]. Davinciti [Fecha de consulta: 08 de noviembre de 2023]. <https://davinciti.com/que-es-logstash-ejemplo-practico-de-uso/>

- El-brujo (2021, marzo). "*Suricata - IDS/IPS - Instalación, configuración básica reglas.*" [artículo en línea]. ELHACKER.NET [Fecha de consulta: 09 de noviembre de 2023]. <https://blog.elhacker.net/2021/03/suricata-ids-ips-instalacion-configuracion-reglas-.html>

- Solvetic (2022, septiembre). "*Cómo instalar y Configurar Suricata en*

Ubuntu" [artículo en línea]. Solvetic [Fecha de consulta: 09 de noviembre de 2023]. <https://www.solvetic.com/tutoriales/article/12180-como-instalar-y-configurar-suricata-en-ubuntu/>

- Elastic (s.f.). *"pfSense"* [artículo en línea]. Elastic [Fecha de consulta: 11 de noviembre de 2023]. <https://docs.elastic.co/en/integrations/pfsens>

- GITHUB (s.f.). "*pfSense/OPNsense + Elastic Stack*" [artículo en línea]. GITHUB [Fecha de consulta: 12 de noviembre de 2023]. <https://GitHub.com/pfelk/pfelk>

- Elastic (s.f.). "*Install Elasticsearch with Debian Package*" [artículo en línea]. Elastic [Fecha de consulta: 14 de noviembre de 2023]. <https://www.elastic.co/guide/en/elasticsearch/reference/8.11/deb.html>

- Elastic (s.f.). "*Install Kibana with Debian package*" [artículo en línea]. Elastic [Fecha de consulta: 15 de noviembre de 2023]. <https://www.elastic.co/guide/en/kibana/current/deb.html#deb-key>

- Wazuh (s.f.). "*Wazuh server*" [artículo en línea]. Wazuh [Fecha de consulta: 15 de noviembre de 2023]. <https://documentation.wazuh.com/current/installation-guide/wazuh-server/index.html>

- Malinkin, Sergey (s.f.). "*ElastAlert 2 - Automated rule-based alerting for Elasticsearch*" [artículo en línea]. Readthedocs [Fecha de consulta: 17 de noviembre de 2023]. <https://elastalert2.readthedocs.io/en/latest/elastalert.html>

- Uranga, Maitane (2021, septiembre). "*SPLUNK: The Ultimate SIEM for Control*" [artículo en línea]. JAYMON SECURITY [Fecha de consulta: 27 de noviembre de 2023]. <https://jaymonsecurity.com/splunk-un-siem-para-controlarlos-a-todos/>

- Shulkhan, M (2020, noviembre). "*Detection Attack using Suricata-2*" [artículo en línea]. Medium [Fecha de consulta: 08 de diciembre de 2023]. <https://medium.com/@mshulkhan/detection-attack-using-suricata-2-d93d423a435>

- Gonzales Jurado, Jose Antonio (2020, octubre). "*Detección de Intrusos utilizando Suricata IDS/IPS & ELK*" [artículo en línea]. Linkedin [Fecha de consulta: 09 de diciembre de 2023]. < https://www.linkedin.com/pulse/detección-de-intrusos-utilizando-suricata-idsips-elk-gonzales-jurado/>

- Suricata (s.f.). "*Suricata Rules*" [artículo en línea]. Suricata [Fecha de consulta: 10 de diciembre de 2023]. <https://docs.suricata.io/en/suricata-6.0.0/rules/ssh-keywords.html>

- Edwards, Daniel (2015, agosto). "*Blue Teaming with Wazuh Part 2:*

Attacks & Alerts" [artículo en línea]. Systemweakness [Fecha de consulta: 11 de diciembre de 2023]. <https://systemweakness.com/introduction-to-wazuh-part-2-attacks-defenses-e8a7be995480>

- SerializingMe (2015, agosto). "*SSH Brute Force and Suricata*" [artículo en línea]. SerializingMe [Fecha de consulta: 11 de diciembre de 2023]. <https://www.serializing.me/2015/08/12/ssh-brute-force-and-suricata/>

- Hackertarget (2011, mayo). "*Brute Forcing Passwords with ncrack, hydra and medusa*" [artículo en línea]. Hackertarget [Fecha de consulta: 12 de diciembre de 2023]. <https://hackertarget.com/brute-forcing-passwords-with-ncrack-hydra-and-medusa/>

- Buzdar, Karim (2023, mayo). "*How to Install Hydra on Ubuntu 22.04*" [artículo en línea]. Linuxgenie [Fecha de consulta: 12 de diciembre de 2023]. < https://linuxgenie.net/how-to-install-hydra-on-ubuntu-22-04/>

- Rosa Mondragón, Juan Miguel (2021, septiembre). "*Remote Desktop Attacks – Ransomware Entry*" [artículo en línea]. JAYMON SECURITY [Fecha de consulta: 13 de diciembre de 2023]. <https://jaymonsecurity.com/ransomware-escritorio-remoto-rdp/>

- Rosa Mondragón, Juan Miguel (2021, septiembre). "*How to Create a Script for SQL Injection Testing*" [artículo en línea]. JAYMON SECURITY [Fecha de consulta: 13 de diciembre de 2023]. <https://jaymonsecurity.com/script-sql-injection/>

- ATTACK MITRE (s.f.). "*Resources*" [recursos en línea]. ATTACK MITRE [Fecha de consulta: 07 de enero de 2024]. <https://attack.mitre.org/resources/>

7. Anexos.

A. Instalación Ubuntu Server 22.04 LTS en servidor físico.

Los procedimientos para configurar Ubuntu Server LTS son:

1. Se obtiene la versión más reciente de Ubuntu Server desde el sitio oficial: <https://ubuntu.com/download/server>. En el caso que de este TFM se ha obtenido el archivo iso “ubuntu-22.04.3-live-server-amd64.iso”.
2. Se realiza la instalación como se indica en la página web oficial, en la URL <https://ubuntu.com/tutorials/install-ubuntu-server>.
    - Durante su instalación se deberá tener en cuenta las siguientes configuraciones:
        - Idioma de la interfaz: español.
        - Disposición del teclado: español (España).
        - Conexión de red: asignación de 'eth0' con los siguientes parámetros:
            - Subred: 192.168.233.1/24.
        - Dirección IP: asignación específica dependiendo del propósito del servidor:
            - Para servidor 1 ELK Stack: 192.168.233.141.
            - Para servidor 2 Wazuh: 192.168.233.151.
            - Para servidor 3 Surikata: 192.168.233.152.
            - Para servidor 4 PfSense: 192.168.233.130.
        - Puerta de enlace: 192.168.233.2
        - Servidores de nombres: 192.168.233.2
        - Dominios de búsqueda: [dominio específico].
        - Dirección del espejo de Ubuntu: http://archive.ubuntu.com/ubuntu.
        - Configuración de disco: uso completo del disco seleccionado, manteniendo la partición predeterminada.
        - Información del equipo:
            - Nombre del usuario: MasterSOC
            - Nombre del servidor: definido por el propósito de este.
            - Contraseña: definida y confirmada por el usuario.
        - Configuración adicional:
            - Instalación del servidor SSH: marcado.
            - Identidad SSH para importar: No.
            - Snap adicionales: ninguno seleccionado.

    Tras completar la instalación, se procede con la actualización de paquetes mediante el comando “sudo apt-get update && sudo apt-get upgrade”.

B. Instalación ELK Stack en Ubuntu Server 22.04 LTS en servidor físico.

B.1. Requisitos de instalación del ELK Stack.

Para continuar con la guía de implementación, el servidor debe cumplir con las siguientes especificaciones:

- **Recursos del sistema**: Mínimo de 4 GB de memoria RAM y 2 núcleos de CPU. Estas son las especificaciones básicas recomendadas para el correcto funcionamiento de Elasticsearch.
- **Privilegios de usuario**: Un usuario con permisos “sudo” que no sea el usuario “root”.
- **Java Development Kit**: “OpenJDK 11” debe estar instalado en el sistema, ya que es un requisito previo para Elasticsearch.

B.2. Instalación de Elasticsearch.

Para implementar Elasticsearch en Ubuntu, es necesario añadir manualmente el repositorio de Elasticsearch ya que no está incluido en los repositorios por defecto de Ubuntu. El siguiente conjunto de comandos ilustra cómo llevar a cabo esta tarea:

1. Añadir la clave GPG de Elasticsearch para validar la autenticidad de los paquetes:
    - *wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg*
2. Registrar el repositorio de Elasticsearch para la versión 8.x en el sistema APT:
    - *echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list*
3. Refrescar la lista de paquetes disponibles:
    - *sudo apt update*
4. Instalar Elasticsearch utilizando APT:
    - *sudo apt install elasticsearch*

Tras instalar Elasticsearch se observará en el terminal la contraseña de acceso del “superuser”, la cual se ha generado de manera aleatoria durante el proceso de instalación. Como es obvio, estas credenciales son muy importantes por lo que habrá que guardarlas en lugar seguro.

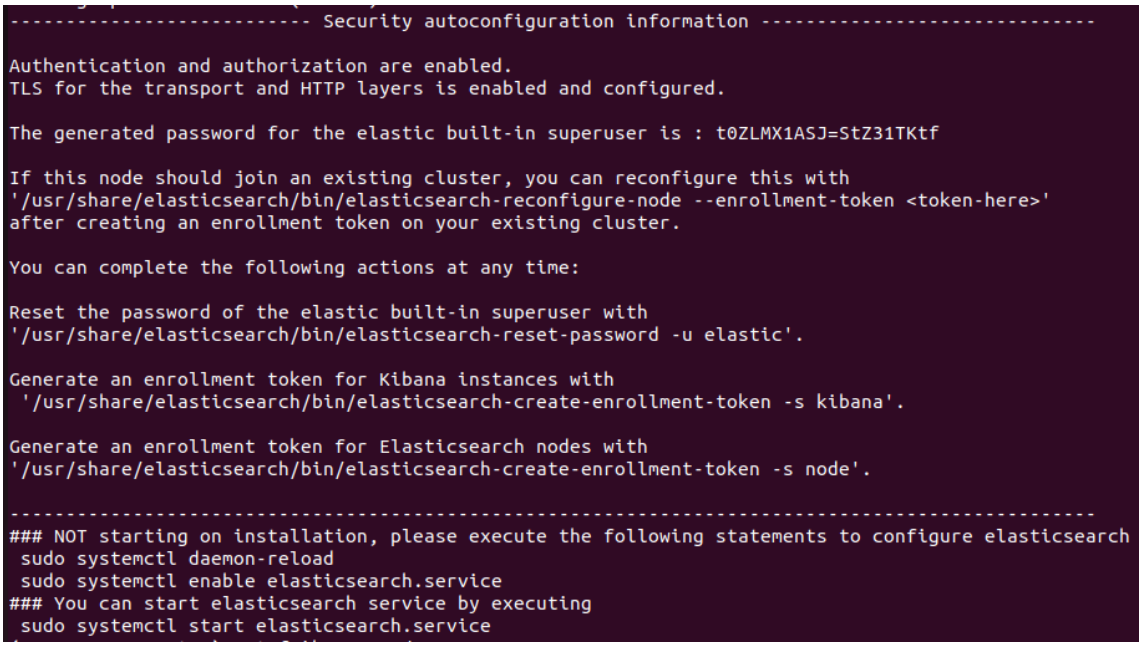


Figura 69: Detalle contraseña del usuario “Elastic”.

5. Configurar Elasticsearch editando su archivo de configuración principal, “/etc/elasticsearch/elasticsearch.yml”. Aquí, especificaremos la interfaz de red para escuchar:

    - *network.host: 192.168.233.141*

6. Activar el servicio de Elasticsearch para que se inicie automáticamente con el sistema:

    - *sudo systemctl enable elasticsearch*

7. Iniciar el servicio de Elasticsearch:

    - *sudo systemctl start elasticsearch*

8. Para verificar el correcto funcionamiento de Elasticsearch, se puede hacer a través de la línea de comandos, tal como se muestra en la siguiente figura, o accediendo desde un navegador web a la dirección y puerto predeterminados de Elasticsearch, es decir, “localhost:9200”. Es importante destacar que Elasticsearch utiliza cifrado de forma predeterminada, por lo que es necesario el uso de HTTPS.

```
sh-5.1# sudo curl --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic https://127.0.0.1:9200
Enter host password for user 'elastic':
{
  "name" : "eshd-1",
  "cluster_uuid" : "kib6ZHUzRfG8l_q-ukABfA",
  "version" : {
    "number" : "8.3.3",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "801fed82df74dbe537f89b71b098ccaff88d2c56",
    "build_snapshot" : false,
    "lucene_version" : "9.2.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Figura 70: Detalle correcto funcionamiento de Elasticsearch.

La salida esperada indica que Elasticsearch se está ejecutando adecuadamente y se encuentra listo para recibir y procesar datos.

B.3. Instalación y configuración de Kibana.

Para instalar Kibana y conectarla con Elasticsearch, se deben seguir una serie de pasos muy similares a los utilizados para la instalación de Elasticsearch, ya que Kibana también se encuentra en el mismo repositorio de paquetes. El siguiente conjunto de comandos ilustra cómo llevar a cabo esta tarea:

1. Instalar Kibana utilizando el gestor de paquetes APT:
    - *sudo apt install kibana*
2. Habilitar el servicio de Kibana para que se inicie automáticamente con el sistema:
    - *sudo systemctl enable kibana*
3. Iniciar el servicio de Kibana:
    - *sudo systemctl start kibana*
4. Confirmar que Kibana está operativa y escuchando en su puerto predeterminado, 5601:
    - *netstat -tulpn | grep 5601*

La salida esperada indica que Kibana está activa y escuchando solicitudes en el puerto 5601, normalmente a través de un proceso llamado “node”.

Con estos pasos, Kibana estará operativa y podrá ser utilizada para crear visualizaciones y dashboards que ayudan a interpretar los datos almacenados en Elasticsearch. Por defecto, Kibana se conectará a Elasticsearch en la misma

máquina en la que está instalada, a menos que se modifique la configuración para apuntar a un clúster de Elasticsearch diferente.

Así pues, tras la instalación de Kibana, se debe crear un token como se muestra en la siguiente figura. Este token debe ser introducido en el formulario que aparece al ingresar a Kibana a través de un navegador, utilizando la dirección y puertos predeterminados, “localhost:5601”, por medio de HTTP. Posteriormente, es necesario generar un código de verificación siguiendo las instrucciones proporcionadas en la interfaz web de Kibana y luego ingresarlo en el navegador.

```
sh-5.1#  /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
eyJ2ZXIiOiI4LjMuMyIsImFkciI6WyIxNzIuMzEuMjUyLjIwOjkyMDAiXSwiZmdyIjoiOGRlODQyNTI4ZjcyZTBhNTY5NmU0ODEwZjEwMDIzMDQzMGM1NzQyNWIzNTZkNGRjYTY4MjVhZjc5YjgyYjE1NCIsImtleSI6IlZU0UJ4WXNCT09JeGJYZkVXTEJVOnhpbjZ1ZXRPU2xTZ01PbVdjN1lxR3cifQ==
```

Figura 71: Detalle de la generación del token de Kibana.

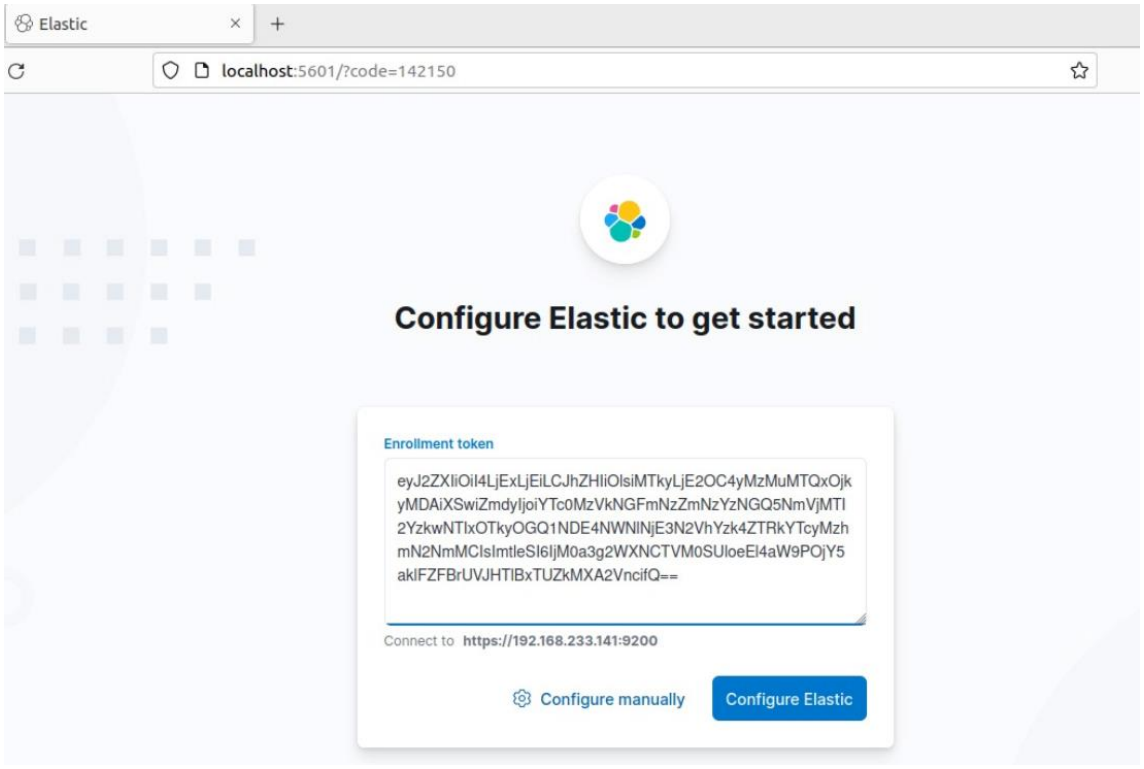


Figura 72: Detalle ingreso del token Kibana en Elasticsearch.

Una vez completado el proceso de verificación, se obtiene acceso a Elasticsearch mediante Kibana, utilizando el nombre de usuario "elastic" y la contraseña generada durante la instalación de Elasticsearch que se muestra en el anexo B.2. Finalmente, es esencial modificar la dirección IP de escucha de Elasticsearch en el archivo de configuración “/etc/elasticsearch/elasticsearch.yml” cambiando el valor predeterminado de “localhost” por la dirección de la interfaz de red de la red NAT compartida con el servidor Logstash.

A continuación, se muestra captura del correcto funcionamiento de Kibana.

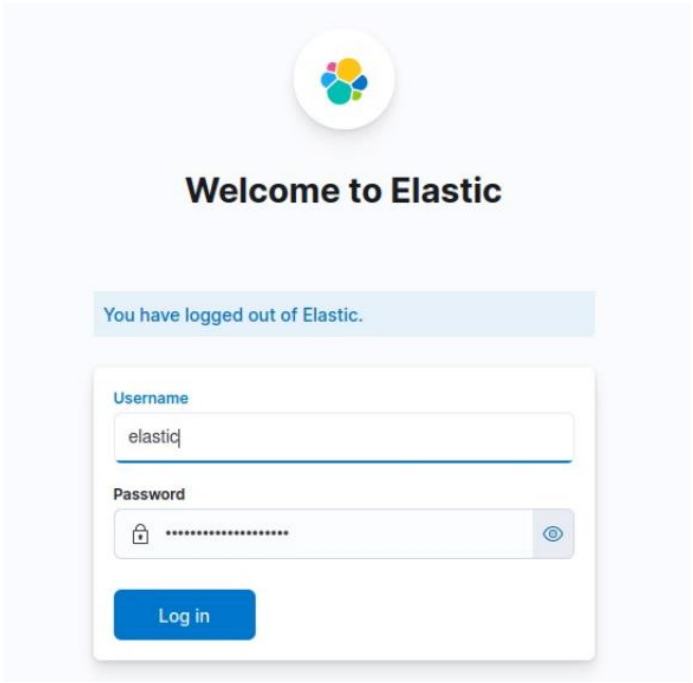


Figura 73: Detalle del ingreso vía web a Kibana.

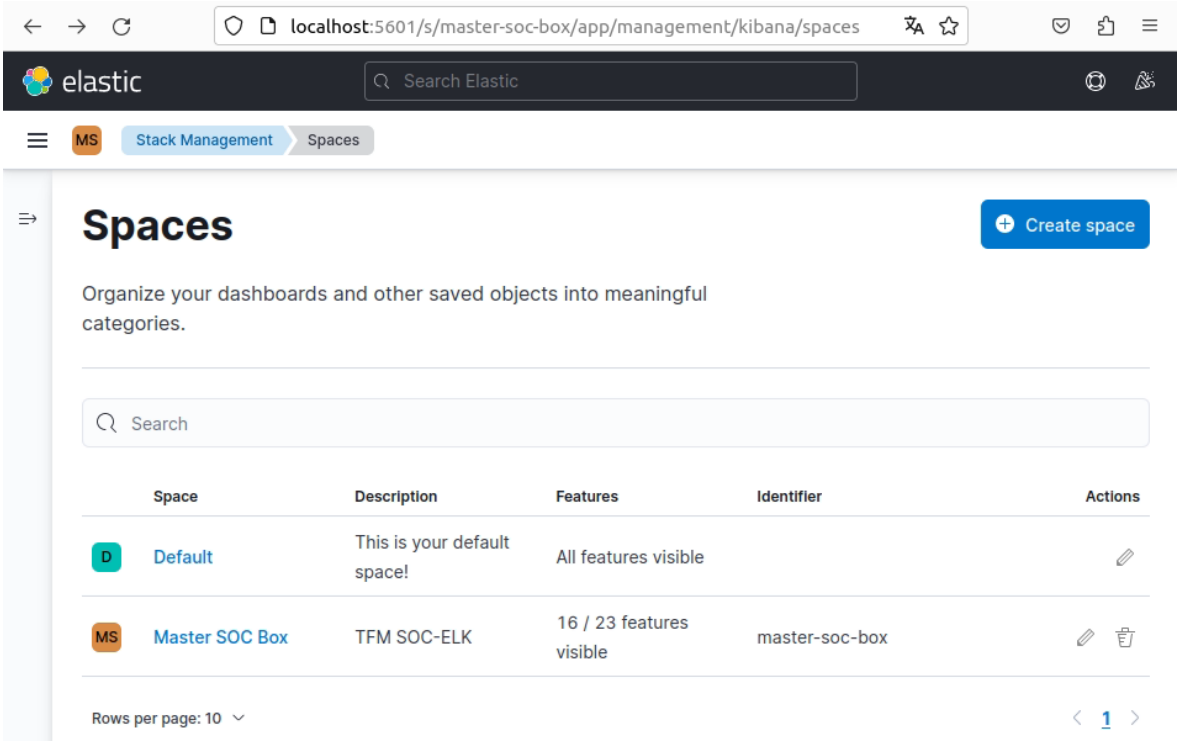


Figura 74: Detalle del correcto acceso vía web a Kibana.

```
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
#cluster.name: my-application
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: master
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
# ----------------------------------- Paths ------------------------------------
#
# Path to directory where to store the data (separate multiple locations by comma):
#
path.data: /var/lib/elasticsearch
#
# Path to log files:
#
path.logs: /var/log/elasticsearch
#
# ----------------------------------- Memory -----------------------------------
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 192.168.233.141
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
```

Figura 75: Detalle del contenido del archivo “Elasticsearch.yml”.

B.4. Instalación y configuración de Logstash.

Para establecer Logstash en el servidor y configurarlo para procesar y transmitir datos, se deben seguir los siguientes pasos:

1. **Instalación de Logstash:**

   - *sudo apt install logstash*

   Esta acción instala Logstash pero no lo inicia inmediatamente, ya que primero se necesita definir cómo procesará los datos.

2. **Configuración de Logstash:** Logstash utiliza "pipelines" configurados a través de archivos para definir cómo se deben procesar los datos. Para crear un archivo de configuración básico:

   - *sudo nano /etc/logstash/conf.d/basic.conf*

   Dentro de este archivo, puede estructurar su configuración inicial de la siguiente manera:

- *input { file { path => "/var/log/*.log" start_position => "beginning" } } filter { grok { match => { "message" => "%{COMBINEDAPACHELOG}" } } } output { elasticsearch { hosts => ["http://localhost:9200"] } stdout { codec => rubydebug } }*

Este esquema básico instruye a Logstash para leer archivos de log, procesarlos con un filtro "grok" para estructurar los datos no estructurados, y luego enviarlos a una instancia de Elasticsearch en el localhost. También se configura para mostrar la información procesada en la consola.

3. **Iniciar y habilitar el servicio de Logstash:** Con la configuración realizada, se da paso a iniciar Logstash y configurarlo para que se ejecute al iniciar el sistema.

   - *sudo systemctl enable logstash sudo systemctl start logstash*

   Con estos pasos, Logstash estará operativo y listo para procesar los datos según las especificaciones del archivo de configuración.

En cuanto a la configuración de PIPELINES, se muestra el contenido del archivo "/etc/logstash/conf.d/pipelines.conf" realizado para este Trabajo. Cabe destacar que en dicho archivo habrá que introducir todas las fuentes de ingesta que se quieran integrar.

El archivo "pipelines.conf" (o cualquier archivo ".conf" en el directorio "conf.d") define la configuración de un pipeline individual en Logstash. Esta configuración incluye las fases de entrada (input), filtrado (filter) y salida (output) de los datos.

Así pues, se puede resumir lo siguiente:

- **Entrada (input)**: Aquí se define cómo y de dónde Logstash recibe los datos. Por ejemplo, puede ser a través de archivos de registro, flujos de datos en tiempo real, bases de datos, etc.
- **Filtrado (filter)**: En esta sección se procesan y transforman los datos. Se pueden usar diversos filtros para modificar, enriquecer, eliminar o transformar los datos según sea necesario.
- **Salida (output)**: Esta fase especifica hacia dónde se enviarán los datos procesados, como Elasticsearch, un archivo, una base de datos, entre otros.

```
input
{
	udp
	{
		port => 5001
		workers => 8
		queue_size => 16384
		type => SYSLOG
		codec => plain { charset => "ISO8859-1" }
	}
filter
{
	mutate
	{
		add_field => [ "Cliente", "Unknown" ]
		add_field => [ "Tipo_Dispositivo", "Unknown" ]
		add_field => [ "Dispositivo", "Unknown" ]
	}
else if [host] == "192.168.233.130"
{
	mutate
	{
		replace => [ "Cliente", "Ayuntamiento" ]
		replace => [ "Tipo_Dispositivo", "PFSense" ]
		replace => [ "Dispositivo", "Pfsense" ]
	}
}
output {
		elasticsearch {
			hosts => ["https://192.168.233.151:9200"]
			action=> "create"
			user => "elastic"
			password => "wR=q=u6oQeLvHpERcLQA"
			index => "logstash-%{i.cliente}"
					cacert=>"/etc/logstash/certs/http_ca.crt"
					ssl => "true"
		}
}
```

Figura 76: Detalle del contenido del archivo “pipelines.conf”.

B.5. Securización de ELK Stack con X-Pack.

Establecer conexiones seguras entre los componentes de Elasticsearch implica implementar y gestionar adecuadamente los certificados y archivos mencionados, asegurando así la integridad y confidencialidad de las comunicaciones en cada nivel del sistema.

Tras la instalación de Elasticsearch se crean automáticamente sus propios certificados para realizar la comunicación entre nodos (transport.p12) y para que se comuniquen el resto de las aplicaciones (Kibana, Logstash) por protocolo HTTPS (http.p12). No obstante, a continuación se muestra cómo proceder a la creación de certificados propios autofirmados.

Para ello es importante saber que las comunicaciones seguras entre Elasticsearch y todos sus componentes se conforma de la siguiente manera:

- Comunicación entre nodos de Elasticsearch:
    - En el caso de un clúster con varios nodos, es esencial garantizar que la comunicación interna entre estos nodos sea segura y cifrada. En el contexto que atañe, esta seguridad se logra mediante el uso del certificado denominado “transport.p12”.
- Comunicación entre elasticsearch y otros componentes (como pueden ser Kibana y Logstash):
    - La comunicación entre Elasticsearch y otros componentes, como Kibana y Logstash, debe realizarse de manera cifrada, ya que se lleva a cabo a través del protocolo HTTPS. En el entorno que atañe, se emplean los archivos “http.p12” (para Elasticsearch) y “elasticsearch_ca.pem” (para Kibana y Logstash) para garantizar la seguridad de estas interacciones.
- Comunicación entre Kibana y el navegador:
    - Asimismo, es deseable que la comunicación entre Kibana y el navegador del usuario esté cifrada. En este caso, se utilizan los archivos “kibana-server.com.crt” y “kibana-server.com.key” para asegurar que esta conexión sea segura.

Así pues, en la siguiente captura se muestra la creación de la autoridad certificadora (CA), esencial para poder firmar nuevos certificados para las aplicaciones correspondientes de Elasticsearch, Logstash y Kibana.

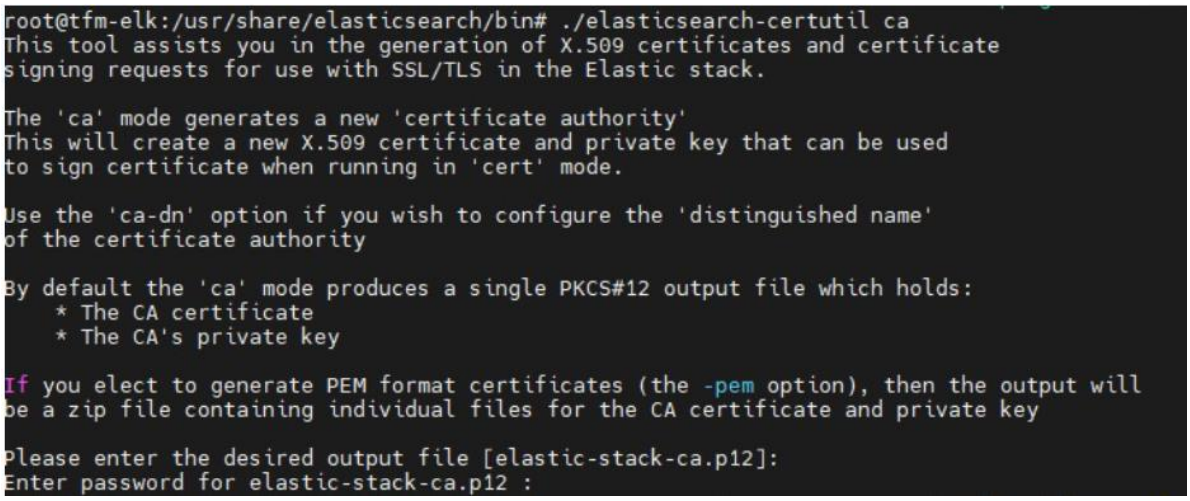


Figura 77: Detalle de creación de CA.

[Elasticsearch] A continuación se muestra la creación de certificados para conectar internamente nodos de Elasticsearch por SSL, lo cual es necesario para realizar conexiones seguras entre estos.

```
root@tfm-elk:/usr/share/elasticsearch# ./bin/elasticsearch-certutil cert --ca elastic-stack-ca.p12
This tool assists you in the generation of X.509 certificates and certificate
signing requests for use with SSL/TLS in the Elastic stack.

The 'cert' mode generates X.509 certificate and private keys.
    * By default, this generates a single certificate and key for use
      on a single instance.
    * The '-multiple' option will prompt you to enter details for multiple
      instances and will generate a certificate and key for each one
    * The '-in' option allows for the certificate generation to be automated by describing
      the details of each instance in a YAML file

    * An instance is any piece of the Elastic Stack that requires an SSL certificate.
      Depending on your configuration, Elasticsearch, Logstash, Kibana, and Beats
      may all require a certificate and private key.
    * The minimum required value for each instance is a name. This can simply be the
      hostname, which will be used as the Common Name of the certificate. A full
      distinguished name may also be used.
    * A filename value may be required for each instance. This is necessary when the
      name would result in an invalid file or directory name. The name provided here
      is used as the directory name (within the zip) and the prefix for the key and
      certificate files. The filename is required if you are prompted and the name
      is not displayed in the prompt.
    * IP addresses and DNS names are optional. Multiple values can be specified as a
      comma separated string. If no IP addresses or DNS names are provided, you may
      disable hostname verification in your SSL configuration.


    * All certificates generated by this tool will be signed by a certificate authority (CA)
      unless the --self-signed command line option is specified.
      The tool can automatically generate a new CA for you, or you can provide your own with
      the --ca or --ca-cert command line options.


By default the 'cert' mode produces a single PKCS#12 output file which holds:
    * The instance certificate
    * The private key for the instance certificate
    * The CA certificate

If you specify any of the following options:
    * -pem (PEM formatted output)
    * -multiple (generate multiple certificates)
    * -in (generate certificates from an input file)
then the output will be be a zip file containing individual certificate/key files

Enter password for CA (elastic-stack-ca.p12) :
Please enter the desired output file [elastic-certificates.p12]:
```

Figura 78: Detalle de creación de certificados.

A continuación, se muestra captura de la correcta creación del certificado “elastic-certificates.p12”.

```
root@tfm-elk:/usr/share/elasticsearch# ls
bin  csr-bundle.zip  elastic-certificates.p12  elastic-stack-ca.p12
```

Figura 79: Detalle de creación de certificados.

A continuación, se modifican los permisos y el propietario del certificado en cuestión, para que pueda ser empleado por la aplicación.

```
root@tfm-elk:/usr/share/elasticsearch# chown root:elasticsearch /etc/elasticsearch/certs_new/elastic-*
root@tfm-elk:/usr/share/elasticsearch# chmod 660 /etc/elasticsearch/certs_new/elastic-*
root@tfm-elk:/usr/share/elasticsearch# ls -lah /etc/elasticsearch/certs_new/
total 16K
drwxr-sr-x 2 root elasticsearch 4,0K dic  6 17:25 .
drwxr-s--- 5 root elasticsearch 4,0K dic  6 17:27 ..
-rw-rw---- 1 root elasticsearch 3,6K dic  6 17:24 elastic-certificates.p12
-rw-rw---- 1 root elasticsearch 2,7K dic  6 17:19 elastic-stack-ca.p12
```

Figura 80: Detalle de permisos de certificados.

A continuación, se ejecuta el comando para agregar una contraseña al keystore de transporte SSL (xpack.security.transport.ssl.keystore.secure_password) a través del keystore de Elasticsearch, así como el comando para agregar la contraseña al "truststore" de transporte SSL (xpack.security.transport.ssl.truststore.secure_password). El sistema responde que ya existen entradas anteriores para esa clave, debido a que durante la instalación inicial se crearon por defecto. Se procede a sobrescribir para continuar con los objetivos correspondientes.

```
root@tfm-elk:/usr/share/elasticsearch# ./bin/elasticsearch-keystore add xpack.security.transport.ssl.keystore.secure_password
Setting xpack.security.transport.ssl.keystore.secure_password already exists. Overwrite? [y/N]y
Enter value for xpack.security.transport.ssl.keystore.secure_password:
root@tfm-elk:/usr/share/elasticsearch# ./bin/elasticsearch-keystore add xpack.security.transport.ssl.truststore.secure_password
Setting xpack.security.transport.ssl.truststore.secure_password already exists. Overwrite? [y/N]y
Enter value for xpack.security.transport.ssl.truststore.secure_password:
```

Figura 81: Agregar credencial al keystore.

[kibana] A continuación, se muestra la creación de certificados para conectar por protocolo HTTPS la aplicación de Kibana y Elasticsearch.

```
root@tfm-elk:/usr/share/elasticsearch# ./bin/elasticsearch-certutil http

## Elasticsearch HTTP Certificate Utility

The 'http' command guides you through the process of generating certificates
for use on the HTTP (Rest) interface for Elasticsearch.

This tool will ask you a number of questions in order to generate the right
set of files for your needs.

## Do you wish to generate a Certificate Signing Request (CSR)?

A CSR is used when you want your certificate to be created by an existing
Certificate Authority (CA) that you do not control (that is, you don't have
access to the keys for that CA).

If you are in a corporate environment with a central security team, then you
may have an existing Corporate CA that can generate your certificate for you.
Infrastructure within your organisation may already be configured to trust this
CA, so it may be easier for clients to connect to Elasticsearch if you use a
CSR and send that request to the team that controls your CA.

If you choose not to generate a CSR, this tool will generate a new certificate
for you. That certificate will be signed by a CA under your control. This is a
quick and easy way to secure your cluster with TLS, but you will need to
configure all your clients to trust that custom CA.

Generate a CSR? [y/N]n

## Do you have an existing Certificate Authority (CA) key-pair that you wish to use to sign your certificate?

If you have an existing CA certificate and key, then you can use that CA to
sign your new http certificate. This allows you to use the same CA across
multiple Elasticsearch clusters which can make it easier to configure clients,
and may be easier for you to manage.

If you do not have an existing CA, one will be generated for you.

Use an existing CA? [y/N]y

## What is the path to your CA?

Please enter the full pathname to the Certificate Authority that you wish to
use for signing your new http certificate. This can be in PKCS#12 (.p12), JKS
(.jks) or PEM (.crt, .key, .pem) format.
CA Path: /etc/elasticsearch/certs_new/elastic-stack-ca.p12
Reading a PKCS12 keystore requires a password.
It is possible for the keystore's password to be blank,
in which case you can simply press <ENTER> at the prompt
Password for elastic-stack-ca.p12:
```

Figura 82: Detalle de creación de certificados.

A continuación, se muestra la captura de la correcta creación de los certificados "http.p12" y " elasticsearch-ca.pem".

```
root@tfm-elk:/etc/elasticsearch/certs_new# ls -lah elasticsearch
total 20K
drwxr-xr-x 2 root root          4,0K dic  6 17:48 .
drwxr-sr-x 4 root elasticsearch 4,0K dic  6 17:52 ..
-rw-r--r-- 1 root root          3,6K dic  6 17:48 http.p12
-rw-r--r-- 1 root root          1,4K dic  6 17:48 README.txt
-rw-r--r-- 1 root root           850 dic  6 17:48 sample-elasticsearch.yml
root@tfm-elk:/etc/elasticsearch/certs_new# ls -lah kibana/
total 20K
drwxr-xr-x 2 root root          4,0K dic  6 17:48 .
drwxr-sr-x 4 root elasticsearch 4,0K dic  6 17:52 ..
-rw-r--r-- 1 root root          1,2K dic  6 17:48 elasticsearch-ca.pem
-rw-r--r-- 1 root root          1,3K dic  6 17:48 README.txt
-rw-r--r-- 1 root root          1,1K dic  6 17:48 sample-kibana.yml
root@tfm-elk:/etc/elasticsearch/certs_new#
```

Figura 83: Detalle de creación de certificados.

Al igual que en el caso anterior, se procede a guardar en Keystore la clave del certificado “http” generado.

```
root@tfm-elk:/etc/elasticsearch/certs_new# /usr/share//elasticsearch/bin/elasticsearch-keystore add xpack.security.http.ssl.keystore.secure_password
Setting xpack.security.http.ssl.keystore.secure_password already exists. Overwrite? [y/N]y
Enter value for xpack.security.http.ssl.keystore.secure_password:
```

Figura 84: Agregar credencial al keystore.

Llegados a este punto, se procede a modificar el fichero de configuración “/etc/elasticsearch/elasticsearch.yml” para indicarle las rutas de los nuevos certificados. Cabe destacar que de esta manera quedarán securizados, como se puede leer en el propio archivo de configuración, las conexiones de clientes HTTP vía API de Kibana, Logstash y agentes (Filebeat).

```
# Enable security features
xpack.security.enabled: true

xpack.security.enrollment.enabled: true

# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
  enabled: true
  keystore.path: certs_new/http.p12

# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  keystore.path: certs_new/elastic-certificates.p12
  truststore.path: certs_new/elastic-certificates.p12
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
```

Figura 85: Detalle del fichero de configuración elasticsearch.yml.

Del mismo modo, se procede a modificar el fichero de configuración “/etc/kibana/kibana.yml” para indicarle la ruta del nuevo certificado.

```
# This section was automatically generated during setup.
elasticsearch.hosts: ['https://192.168.233.141:9200']
elasticsearch.serviceAccountToken: AAEAAWVsYXN0aWMva2liYW5hL2Vucm9sbC1wcm9jZXNzLXRva2VuLTE3MDA0MjQ4MDM2MDY6QlZMWFFOZGNRLXk0SVdBVmtIT1dfUQ
#elasticsearch.ssl.certificateAuthorities: [/var/lib/kibana/ca_1700424804451.crt]
elasticsearch.ssl.certificateAuthorities: [/etc/kibana/certs_new/elasticsearch-ca.pem]
#xpack.fleet.outputs: [{id: fleet-default-output, name: default, is_default: true, is_default_monitoring: true, type: elasticsearch, hosts
```

Figura 86: Detalle del fichero de configuración kibana.yml.

[Logstash] Para la configuración de Logstash se emplea el certificado anteriormente creado “elasticsearch-ca.pem”, por lo que únicamente se debe indicar su ruta en el archivo de configuración “pipeline.conf”, como se muestra en la siguiente captura.

```
  GNU nano 6.2                                          /etc/logstash/conf.d/pipeline.conf
output {
        elasticsearch {
        hosts => ["https://192.168.233.141:9200"]
        action => "create"
        index => "tfm-%{+YYYY.MM.dd}"
        user => "elastic"
        password => "IuPOh+JT*y34nAgZQHMu"
        ssl => true
        cacert => "/etc/logstash/certs_new/elasticsearch-ca.pem"
```

Figura 87: Detalle del fichero de configuración pipeline.conf.

Se reinicia el servicio Logstash y queda listo para su uso seguro.

[Comunicación con navegador web] A continuación, se muestra el comando a ejecutar para crear el certificado web firmado por la CA.

```
root@tfm-elk:/etc/kibana# /usr/share/elasticsearch/bin/elasticsearch-certutil cert --pem -ca /etc/elasticsearch/certs_new/elastic-stack-ca.p12 -name kibana-server
This tool assists you in the generation of X.509 certificates and certificate
signing requests for use with SSL/TLS in the Elastic stack.

The 'cert' mode generates X.509 certificate and private keys.
    * By default, this generates a single certificate and key for use
      on a single instance.
    * The '-multiple' option will prompt you to enter details for multiple
      instances and will generate a certificate and key for each one
    * The '-in' option allows for the certificate generation to be automated by describing
      the details of each instance in a YAML file

    * An instance is any piece of the Elastic Stack that requires an SSL certificate.
      Depending on your configuration, Elasticsearch, Logstash, Kibana, and Beats
      may all require a certificate and private key.
    * The minimum required value for each instance is a name. This can simply be the
      hostname, which will be used as the Common Name of the certificate. A full
      distinguished name may also be used.
    * A filename value may be required for each instance. This is necessary when the
      name would result in an invalid file or directory name. The name provided here
      is used as the directory name (within the zip) and the prefix for the key and
      certificate files. The filename is required if you are prompted and the name
      is not displayed in the prompt.
    * IP addresses and DNS names are optional. Multiple values can be specified as a
      comma separated string. If no IP addresses or DNS names are provided, you may
      disable hostname verification in your SSL configuration.


    * All certificates generated by this tool will be signed by a certificate authority (CA)
      unless the --self-signed command line option is specified.
      The tool can automatically generate a new CA for you, or you can provide your own with
      the --ca or --ca-cert command line options.
```

Figura 88: Detalle de creación de CA.

En la siguiente captura se muestra la correcta creación de los certificados “kibana-server.crt” y “kibana-server.key”.

```
root@tfm-elk:/etc/logstash/conf.d# ls -lah /etc/kibana/certs_new/
total 32K
drwxr-sr-x 3 root kibana 4,0K dic 10 15:07 .
drwxr-s--- 4 root kibana 4,0K dic 10 15:07 ..
-rw-rw---- 1 root kibana 1,2K dic  6 18:35 elasticsearch-ca.pem
-rw-rw---- 1 root kibana 1,2K dic  6 23:34 kibana-server.com.crt
-rw-rw---- 1 root kibana 1,7K dic  6 23:34 kibana-server.com.key
drwxr-sr-x 2 root kibana 4,0K dic 10 15:06 old
-rw-r--r-- 1 root kibana 1,3K dic  6 18:35 README.txt
-rw-r--r-- 1 root kibana 1,1K dic  6 18:35 sample-kibana.yml
```

Figura 89: Detalle de creación de certificados.

Una vez creado el certificado anterior, se procede a modificar el archivo de configuración “kibana.yml” para indicarle las rutas de los nuevos certificados.

```
GNU nano 6.2                                                    /etc/kibana/kibana.yml
# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# Defaults to `false`.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
server.name: "tfm-elk"

# ================== System: Kibana Server (Optional) ==================
# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
server.ssl.enabled: true
#server.ssl.certificate: /etc/kibana/certs_new/kibana-server.crt
#server.ssl.key: /etc/kibana/certs_new/kibana-server.key
server.ssl.certificate: /etc/kibana/certs_new/kibana-server.com.crt
server.ssl.key: /etc/kibana/certs_new/kibana-server.com.key
#server.ssl.certificate: /etc/kibana/kibana.crt
#server.ssl.key: /etc/kibana/kibana.key
# ================== System: Elasticsearch ==================
# The URLs of the Elasticsearch instances to use for all your queries.
# elasticsearch.hosts: ["https://192.168.233.141:9200"]
```

Figura 90: Detalle del fichero de configuración kibana.yml.

Llegados a este punto, solo se debe reiniciar Kibana y proceder a acceder a él a través del navegador.
A continuación, se muestra la información del certificado HTTPS correctamente configurado.

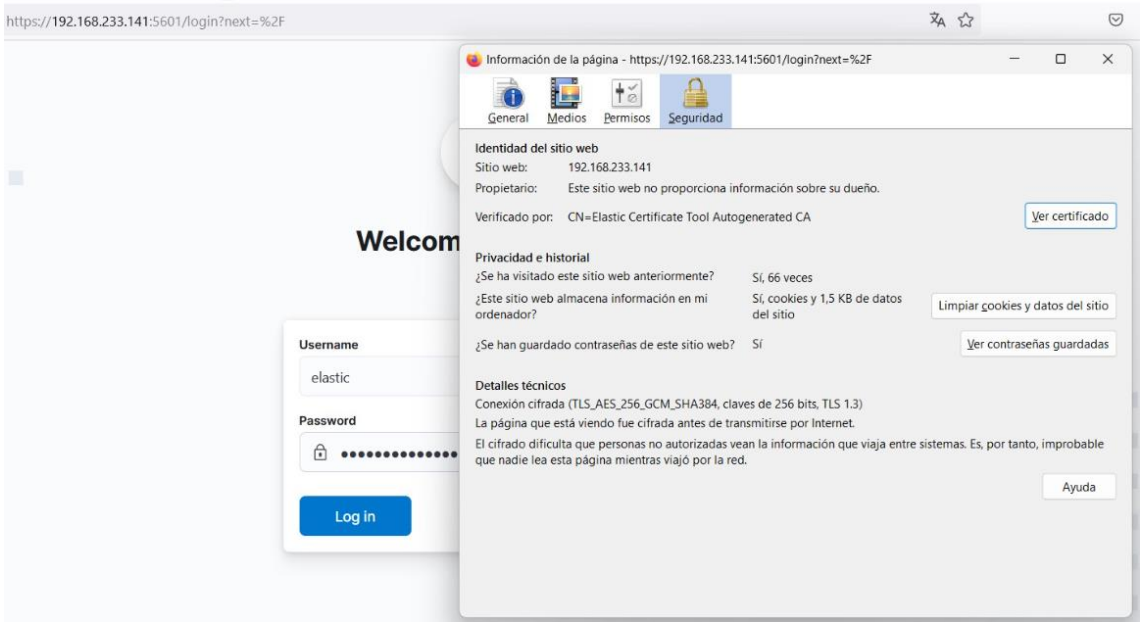


Figura 91: Detalle de la correcta implementación de los certificados HTTPS.

C. Instalación y configuración del sistema Wazuh.

C.1. Instalación y configuración de Wazuh Manager (Gestor Wazuh).

Antes de proceder con la instalación del Mánager de Wazuh, es necesario instalar algunos prerrequisitos para Elasticsearch, como se ha indicado en el anexo “B.1. Requisitos de instalación del ELK Stack”. Una vez instalados los paquetes referentes en el anexo (kit de desarrollo de Java, etc.), se procede a la instalación del Wazuh Manager como se indica a continuación.

1. **Agregar el repositorio de Wazuh**: Primero se debe agregar la clave GPG y luego el repositorio de Wazuh. Esto se realiza mediante la ejecución de los siguientes comandos en la terminal:

    - *wget -q -O - https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -*
    - *echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee -a /etc/apt/sources.list.d/wazuh.list*

2. **Actualizar la lista de paquetes**: Después de agregar el repositorio, se debe actualizar la lista de paquetes disponibles:

    - *sudo apt-get update*

3. **Instalar el gestor de Wazuh**: Ahora puedes instalar el gestor de Wazuh utilizando APT:

    - *sudo apt-get install wazuh-manager*

4. **Habilitar e iniciar el servicio de Wazuh**: Una vez instalado el gestor de Wazuh, debes habilitarlo y luego iniciar el servicio:

    - *sudo systemctl daemon-reload*
    - *sudo systemctl enable wazuh-manager*
    - *sudo systemctl start wazuh-manager*

Tras haber realizado los pasos anteriores, se procede a comprobar que el servicio funciona adecuadamente mediante el siguiente comando:

- *systemctl status wazuh-manager*

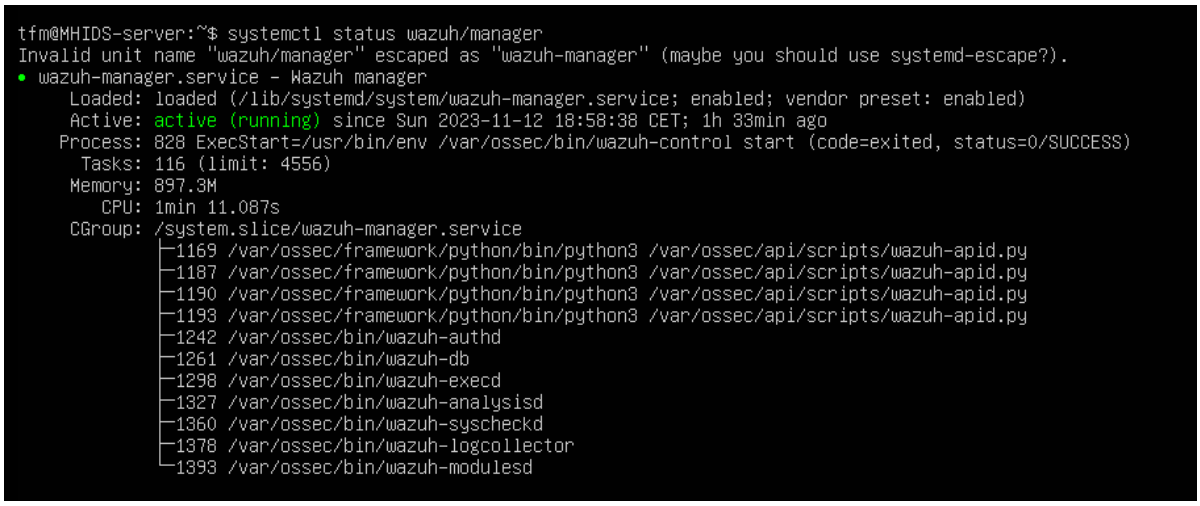


Figura 92: Detalle correcto funcionamiento del gestor Wazuh.

Como los eventos generados por Wazuh Manager se enviarán vía SYSLOG, se debe configurar en el archivo “ossec.conf” el parámetro “SYSLOG_output”, como se muestra en la siguiente captura.

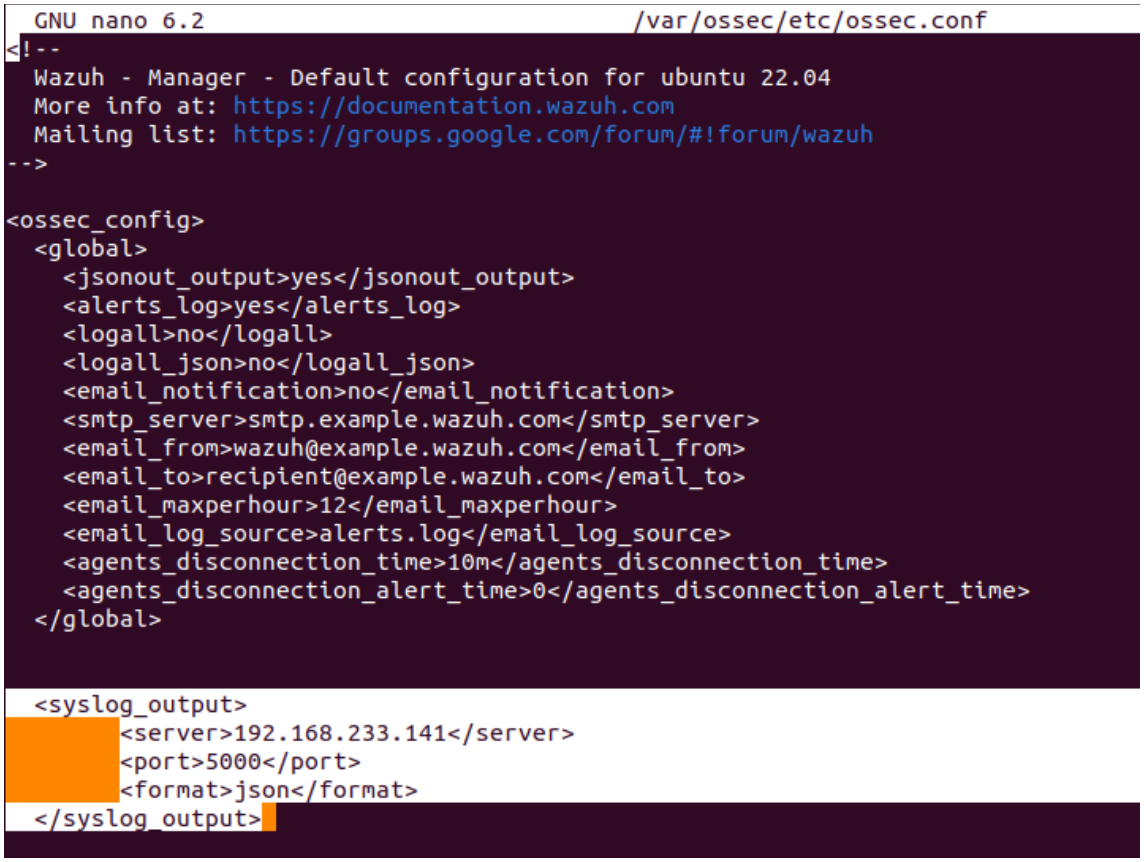


Figura 93: Detalle del fichero de configuración ossec.conf.

Para pasar al SIEM los eventos generados por Wazuh Manager por SYSLOG, se deberá especificar el puerto y protocolo en el fichero “pipeline.conf” de Logstash en su parámetro “input”, como se muestra en la siguiente captura.

```
root@tfm-elk: /etc/logstash/conf.d
  GNU nano 6.2                                              pipeline.conf *
input {
        udp{
        port => 5000
        queue_size => 16384
        type => syslog
        codec => plain { charset => "ISO8859-1"}
        tags => ["WAZUH"]
        }
```

Figura 94: Detalle del fichero de configuración pipeline.conf.

C.2. Instalación y configuración de Wazuh Agent (Agente Wazuh).

En el caso de este TFM, el sistema a monitorizar presentará un Sistema Operativo Windows, por lo que se procede a descargar el paquete de instalación desde la página oficial de Wazuh:

<https://packages.wazuh.com/4.x/windows/wazuh-agent-4.6.0-1.msi>.

1. **Instalar el Agente Wazuh**: Aparecerá un asistente y hay que dar a siguiente hasta finalizar la instalación, que aparecerá la siguiente ventana:

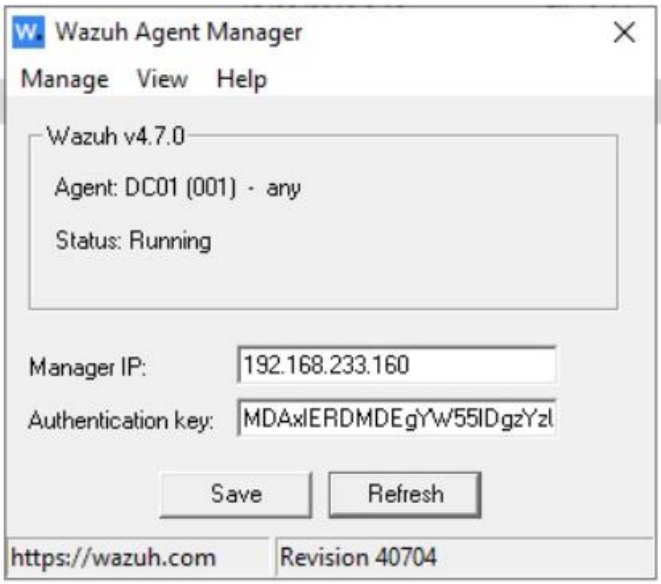


Figura 95: Detalle de instalación del agente Wazuh.

2. **Configurar la IP del gestor (Manager) en el archivo de configuración**: Editar el archivo de configuración del agente para configurar la IP del gestor:

    - *C:\Program Files (x86)\ossec-agent*

```
<ossec_config>

  <client>
    <server>
      <address>192.168.233.151</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>
```

Figura 96: Detalle de configuración del agente Wazuh.

3. **Registrar y configurar el agente**: Después de la instalación, el agente se registrará automáticamente en el manager:

    - *sudo /var/ossec/bin/agent_control -l*

```
root@sonda:/etc/filebeat# /var/ossec/bin/agent_control -l

Wazuh agent_control. List of available agents:
   ID: 000, Name: wazuh (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: DC01, IP: any, Active

List of agentless devices:
```

Figura 97: Detalle de la correcta integración del agente Wazuh con el gestor Wazuh.

Después de estos pasos, el agente Wazuh estará instalado, configurado y conectado correctamente con el gestor. Así pues, se podrá observar su estado correctamente en la interfaz de Kibana.

C.3. Instalación de Filebeat. Configuración de seguridad entre Wazuh y Elasticsearch mediante el agente Filebeat.

A continuación, se realiza la instalación y configuración de Filebeat.

```
root@wazuh:/home/tfm# apt-get -y install filebeat
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhtp2 libhyperscan5 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 oinkmaster python3-simplejson snort-rules-default suricata-update
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  filebeat
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 43 no actualizados.
Se necesita descargar 0 B/50,1 MB de archivos.
Se utilizarán 183 MB de espacio de disco adicional después de esta operación.
Seleccionando el paquete filebeat previamente no seleccionado.
(Leyendo la base de datos ... 215883 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../filebeat_8.11.2_amd64.deb ...
Desempaquetando filebeat (8.11.2) ...
Configurando filebeat (8.11.2) ...
root@wazuh:/home/tfm# curl -o /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.7/tpl/wazuh/filebeat/filebeat.yml
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   867  100   867    0     0    780      0  0:00:01  0:00:01 --:--:--   780
```

Figura 98: Detalle de la instalación de filebeat.

Para llevar a cabo la securización entre Wazuh y Elasticsearch mediante Filebeat se utilizará el certificado “elasticsearch-ca.pem” generado en puntos anteriores.

A continuación, se muestra captura del fichero de configuración “filebeat.yml”.

```
root@wazuh: /etc/filebeat
  GNU nano 6.2                                                  filebeat.yml *
# Wazuh - Filebeat configuration file
output.elasticsearch:
  hosts: ["192.168.233.141:9200"]
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    /etc/filebeat/certs_new/elasticsearch-ca.pem
  #ssl.certificate: "/etc/filebeat/certs/filebeat.pem"
  #ssl.key: "/etc/filebeat/certs/filebeat-key.pem"
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: true
```

Figura 99: Detalle del fichero de configuración filebeat.yml.

Una vez modificado el archivo de configuración se debe reiniciar el servicio de Filebeat. A continuación, se muestra captura que evidencia la correcta implementación de securización entre Wazuh y Elasticsearch mediante Filebeat.

```
root@wazuh:/etc/filebeat# filebeat test output
elasticsearch: https://192.168.233.141:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 192.168.233.141
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 8.11.1
```

Figura 100: Detalle del correcto funcionamiento seguro de Filebeat.

D. Instalación y configuración del sistema Surikata.

A continuación, se muestran los pasos para llevar a cabo la instalación y configuración de Surikata. Todos los comandos deben ejecutarse con privilegios de superusuario (**sudo**).

1. **Actualizar repositorios**: Para asegurarse obtener la última versión disponible:

    - *sudo apt-get update*

2. **Agregar repositorio e instalar Suricata**: Añadir el repositorio oficial de Suricata e instalar la herramienta:

    - *sudo add-apt-repository ppa:oisf/suricata-stable*
    - *sudo apt install suricata*

3. **Configuración del archivo "Suricata.yaml"**: Se debe abrir el archivo de configuración como sigue:

    - *sudo nano /etc/suricata/suricata.yaml*

    Dentro del archivo de configuración, se deben realizar las modificaciones que procedan en los siguientes campos:

    - **HOME_NET**: Define las redes consideradas internas.
    - **EXTERNAL_NET**: Define todas las direcciones distintas a **HOME_NET**.
    - Configurar la sección de "**eve-log"** para habilitar la salida y el formato de los logs.

    A continuación, se muestra captura del archivo de configuración en cuestión utilizado en este TFM.

```
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 6.0.11.
suricata-version: "6.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
```

Figura 101: Detalle del contenido del archivo “suricata.yaml”.

```
  GNU nano 5.6.1                                        /etc/suricata/suricata.yaml
# Configure the type of alert (and other) logging you would like.
outputs:
  # a line based alerts log similar to Snort's fast.log
  - fast:
      enabled: no
      filename: fast.log
      append: yes
      #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'

  # Extensible Event Format (nicknamed EVE) event log in JSON format
  - eve-log:
      enabled: no
      filetype: regular #regular|4syslog|unix_dgram|unix_stream|redis
      filename: eve.json
      # Enable for multi-threaded eve.json output; output files are amended with
      # with an identifier, e.g., eve.9.json
      #threaded: false
      #prefix: "@cee: " # prefix to prepend to each log entry
      # the following are valid when type: syslog above
      #identity: "suricata"
      #facility: local5
      #level: Info ## possible levels: Emergency, Alert, Critical,
                   ## Error, Warning, Notice, Info, Debug
```

Figura 102: Detalle del contenido del archivo “suricata.yaml”.

```
GNU nano 5.6.1                                  /etc/suricata/suricata.yaml

# a line based alerts log similar to fast.log into syslog
- syslog:
    enabled: yes
    # reported identity to syslog. If omitted the program name (usually
    # suricata) will be used.
    #identity: "suricata"
    facility: local5
    #level: Info ## possible levels: Emergency, Alert, Critical,
                 ## Error, Warning, Notice, Info, Debug
```

Figura 103: Detalle del contenido del archivo “suricata.yaml”.

4. **Configurar la herramienta “suricata-update”**: Viene instalada por defecto y se emplea para gestionar las reglas.

    - *suricata-update enable-source et/open*
    - *suricata-update list-enabled-sources*

5. **Crear y Configurar ficheros para “suricata-update”**: Se deben crear los siguientes tres archivos específicos para la gestión de reglas en Suricata. Estos archivos se utilizan para controlar el comportamiento de las reglas de Suricata de manera automatizada cuando se ejecute “suricata-update”. El propósito de cada uno es el siguiente:

    - **enable.conf**: En este archivo especificarás las reglas que quieres habilitar. Es decir, las reglas que estarán activas en Suricata para detectar patrones de tráfico específicos.
    - **disable.conf**: Aquí listarás las reglas que deseas desactivar. Estas reglas no se aplicarán, permitiendo que ignores ciertos patrones de tráfico que no consideres relevantes para tu entorno.
    - **drop.conf**: En este fichero indicarás las reglas cuya acción debe ser "drop". Esto significa que cualquier paquete de red que coincida con estas reglas será descartado automáticamente por Suricata, impidiendo su paso a través de la red.

    Para crear estos archivos, se pueden utilizar los siguientes comandos:

    - *touch /etc/suricata/enable.conf*
    - *touch /etc/suricata/disable.conf*
    - *touch* /etc/suricata/drop.conf

Una vez creados, se debe editar cada uno de ellos para añadir las reglas específicas según las necesidades operativas.

A continuación, se muestra detalle del archivo “disable.conf”, donde se deshabilitan reglas que no proceden según la operatividad que se quiera presentar en el SOC.

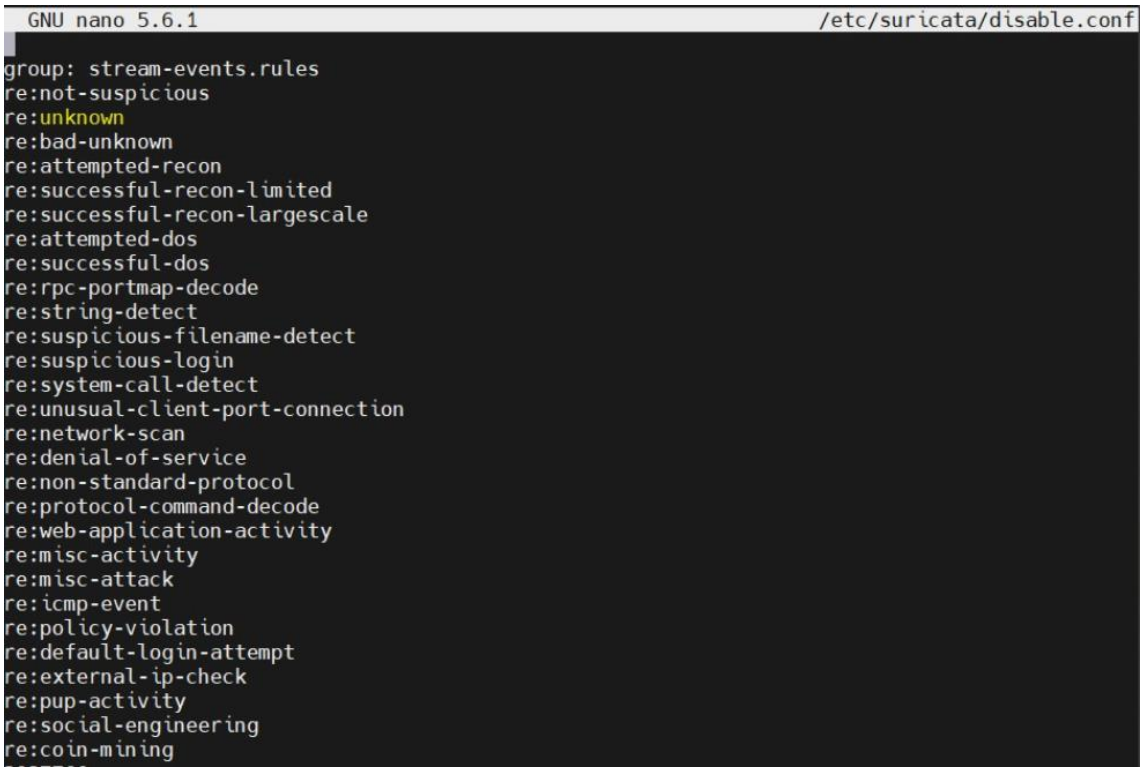


Figura 104: Detalle del contenido del archivo “disable.conf”.

6. **Descargar y actualizar reglas con “suricata-update”**: Se debe ejecutar el siguiente comando para actualizar las reglas.

    - *suricata-update*

7. **Configurar IPTables para encaminamiento y NAT**: Se deben establecer las reglas necesarias en IPTables para el encaminamiento y NAT. Estos comandos dependen de la configuración de red específica y pueden variar. A continuación, se muestran los comandos que han sido empleados en este Trabajo.

    - *sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE*
    - *sudo iptables -I INPUT -j NFQUEUE sudo iptables -I OUTPUT -j NFQUEUE*
    - *sudo iptables -A FORWARD -i ens33 -o ens34 -j ACCEPT*
    - *sudo iptables -A FORWARD -i ens34 -o ens33 -j ACCEPT*
    - *sudo iptables-save > /etc/iptables.rules*

8. **Permitir que Suricata intercepte paquetes**: Configurar IPTables para que los paquetes pasen a través de Suricata:

    - *sudo iptables -I INPUT -j NFQUEUE*
    - *sudo iptables -I OUTPUT -j NFQUEUE*

9. **Ejecutar Suricata**: Iniciar Suricata conforme al archivo de configuración.

- *suricata -c /etc/suricata/suricata.yaml -q 0*

10. **Automatizar actualización de reglas con Cron**: Añadir una tarea programada en “Crontab” para actualizar las reglas diariamente.

    - *(sudo crontab -l ; echo "0 0 * * * suricata-update") | sudo crontab -*

De esta manera se habrá instalado y configurado Suricata en Ubuntu, incluyendo la gestión de reglas y la configuración de IPTables para el correcto funcionamiento del sistema de detección de intrusos.

Como los eventos generados por Suricata se enviarán vía SYSLOG, se debe configurar en el archivo “rSYSLOG.conf” el siguiente parámetro, que indica nivel de log (5), dirección IP a la que enviar dichos logs y que corresponde a la dirección IP de la máquina que aloja Logstash, y el puerto por donde Logstash recibirá los datos.

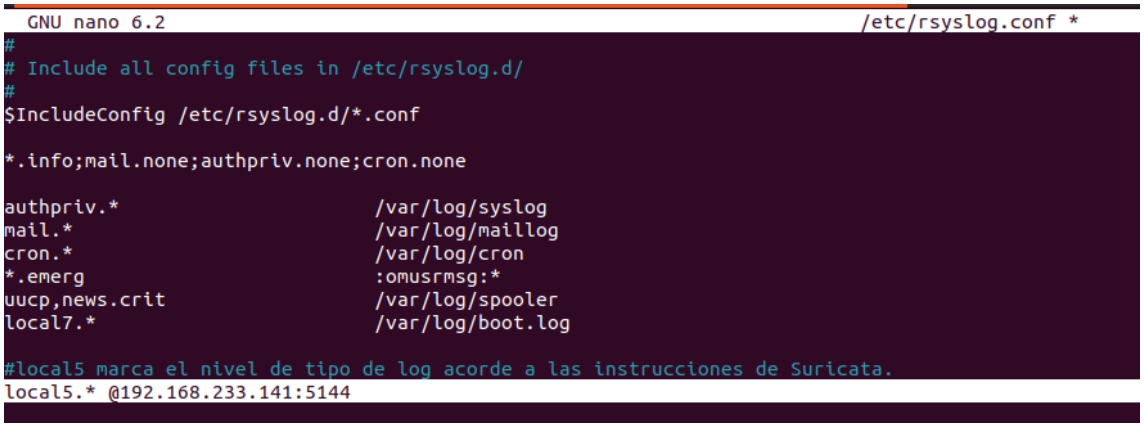


Figura 105: Detalle del fichero de configuración rSYSLOG.conf.

Para pasar al SIEM los eventos generados por Suricata por SYSLOG, se deberá especificar el puerto y protocolo en el fichero “pipeline.conf” de Logstash en su parámetro “input”, como se muestra en la siguiente captura.

Figura 106: Detalle del fichero de configuración pipeline.conf.

E. Instalación y configuración del Firewall.

E.1 Firewall PfSense.

Para instalar PfSense en un servidor, que es un sistema operativo basado en FreeBSD enfocado en funciones de firewall y enrutamiento, se aconseja seguir los siguientes pasos.

1. **Requisitos previos para la instalación.**
   - Verificar los requisitos mínimos de hardware para PfSense.
   - Preparar un dispositivo de almacenamiento (como una unidad USB) para el instalador de PfSense.

2. **Descargar la imagen ISO de PfSense de la arquitectura que proceda**.
   - Esto debe realizarse desde el sitio web oficial de PfSense: <https://www.pfsense.org/download/>.

3. **Crear el medio de instalación**:
   - Mediante una herramienta como “dd**”** en Linux o un programa como “Rufus” en Windows para crear un USB de arranque con la imagen ISO de PfSense.

4. **Configuración del BIOS/UEFI**:
   - Se debe configurar el orden de arranque en la configuración del BIOS/UEFI de la máquina donde se vaya a instalar, para iniciar desde el medio de instalación.

5. **Instalación de PfSense**:
   - Insertar el USB de arranque en el servidor y reiniciarlo.

- Seguir las instrucciones en pantalla para iniciar el proceso de instalación y elegir las opciones de instalación adecuadas para el entorno
- Configura las interfaces de red. PfSense requerirá al usuario configurar las interfaces LAN y WAN.

6. **Configuración inicial**:
   - Una vez completada la instalación, PfSense se reiniciará.
   - En este punto se deberá acceder a la interfaz de configuración web de PfSense (por HTTP) usando otra máquina en la misma red.
   - La primera vez que se acceda, se ejecutará un asistente de configuración que le guiará a través de los pasos básicos para configurar el firewall.
   - Se deberán configurar las reglas de firewall, NAT, VPN, entre otras, según las necesidades de la red.

E.2 Firewall FortiGate.

Una vez se haya adquirido el producto y la licencia de uso de FortiGate, se procede como sigue.

Para instalar el firewall de FortiGate en el Master SOC on BOX, se han ejecutado los siguientes comandos.

```
FortiGate-VM64 login: admin
Password:
Welcome!

FortiGate-VM64 # config system interface

FortiGate-VM64 (interface) # edit port1

FortiGate-VM64 (port1) # mode static
Unknown action 0

FortiGate-VM64 (port1) # set ip 192.168.233.100 255.255.255.0

FortiGate-VM64 (port1) # set allowaccess http https ping ssh

FortiGate-VM64 (port1) # end

FortiGate-VM64 # config router static

FortiGate-VM64 (static) # edit 1

FortiGate-VM64 (1) # set dst 0.0.0.0 0.0.0.0
```

Figura 107: Detalle de los comandos de configuración del firewall Fortinet.

Una vez la máquina del Firewall Fortinet queda configurada, se puede acceder a su configuración a través de su aplicación Web.

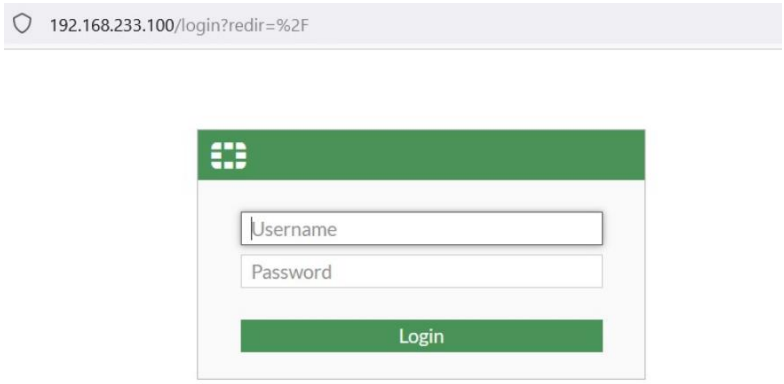


Figura 108: Detalle del acceso al portal Web del firewall FortiGate.

Nada más ingresar al panel de control se solicita introducir el archivo de licencia. Se procede como se muestra en la siguiente captura y al finalizar se reiniciará el sistema para llevar a cabo los nuevos cambios.

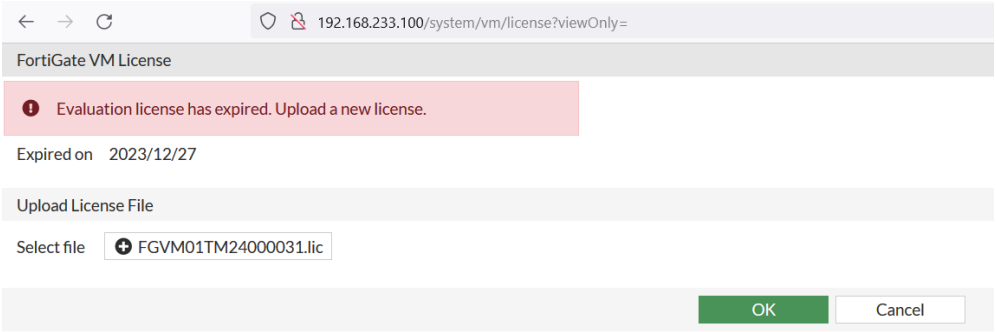


Figura 109: Detalle de instalación de licencia del firewall FortiGate.

Una vez se haya reiniciado el sistema, se podrá observar el siguiente panel donde se podrá llevar a cabo las distintas labores que sean necesarias para la protección de la infraestructura.

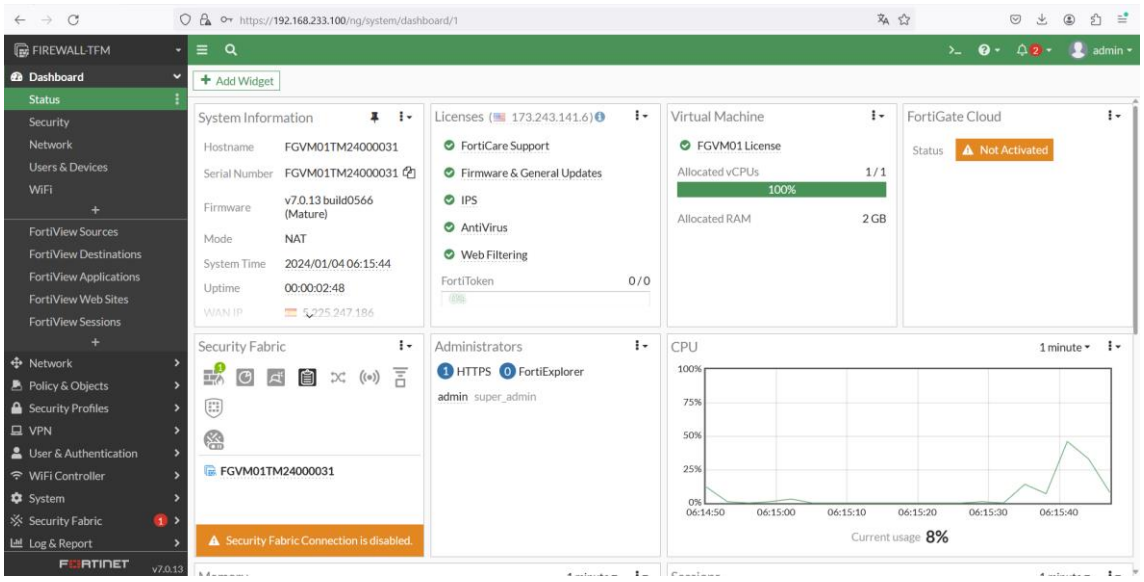


Figura 110: Panel de control del firewall FortiGate.

En la siguiente captura se muestran las opciones de configuración de “Log&Report”, las cuales deberán configurarse para que se envíen los logs obtenidos a Elasticsearch para su correcto procesado y análisis.

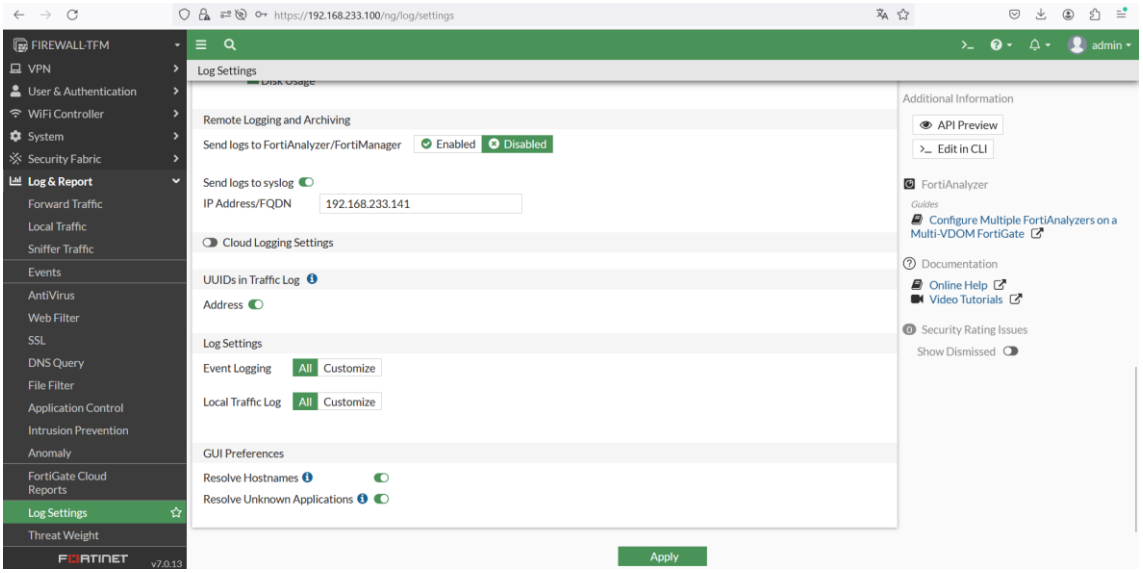


Figura 111: Panel de control de log&report del firewall FortiGate.

En la siguiente captura se muestra la política que habilita la captura de todos los datos que pasarán a través del Firewall.

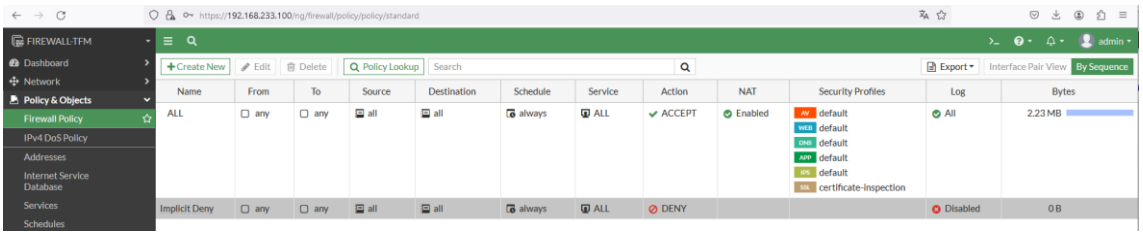


Figura 112.1: Panel de control de log&report del firewall FortiGate.

Para que el tráfico de las máquinas que conforman la LAN pase por el firewall, se deberá poner como puerta de enlace la dirección IP de este. A continuación, se muestran algunas capturas de configuraciones de las máquinas ELK y WAZUH, y de la comprobación de acceso a Internet.

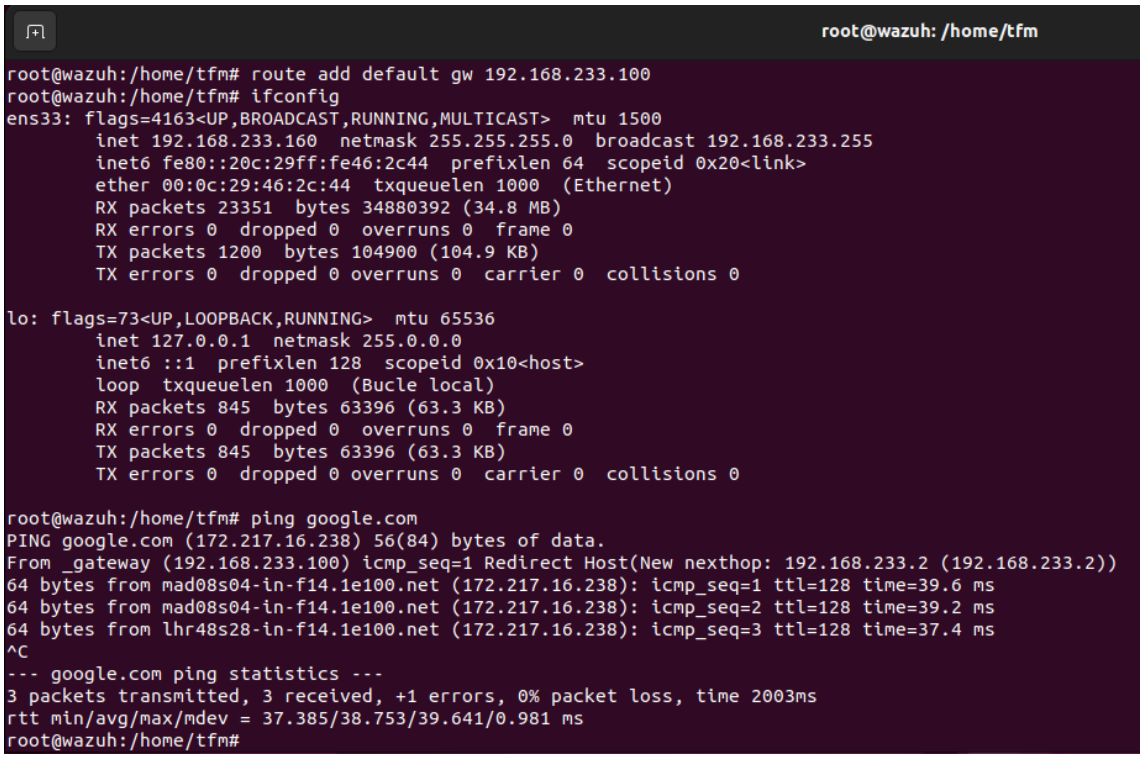


Figura 113: Detalle configuración gw FortiGate máquina Wazuh M.

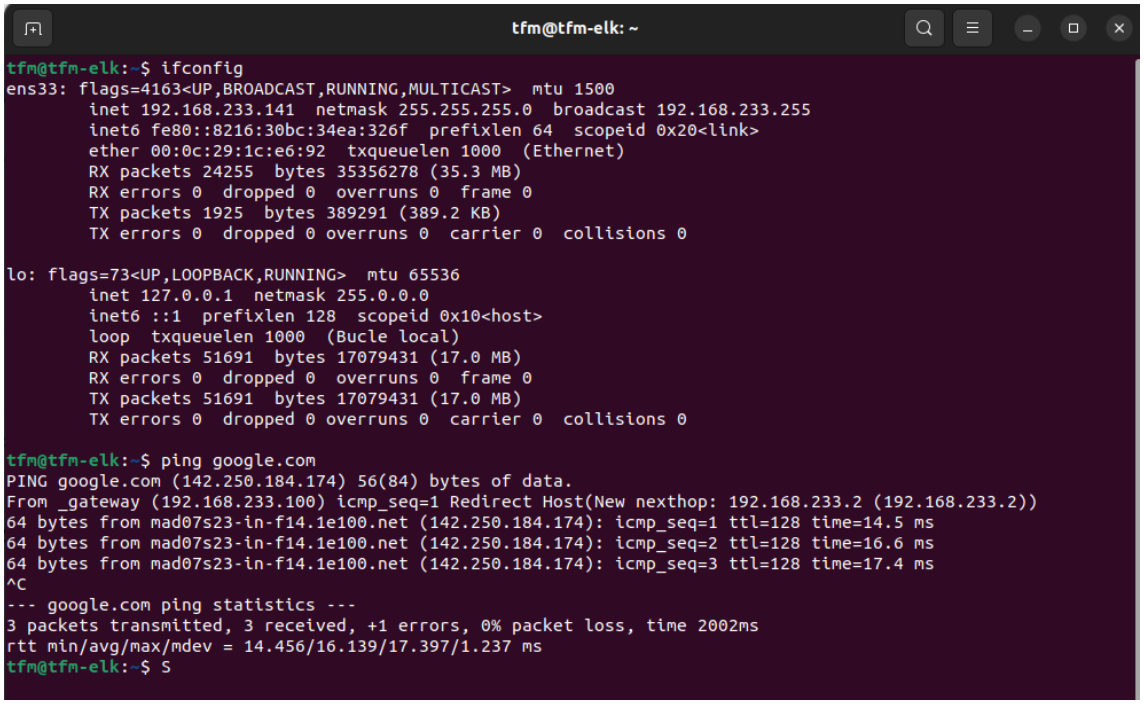


Figura 114: Detalle configuración gw FortiGate máquina ELK.

En conjunto con el equipo IT del ayuntamiento se deberán implementar las políticas que correspondan para la correcta configuración del firewall.

A continuación, se muestra cómo cambiarle el puerto de envío por SYSLOG, ya que por defecto es el puerto 514 por protocolo UDP, y este puerto puede encontrarse en uso y, por tanto, no entrar los logs del firewall en logstash.

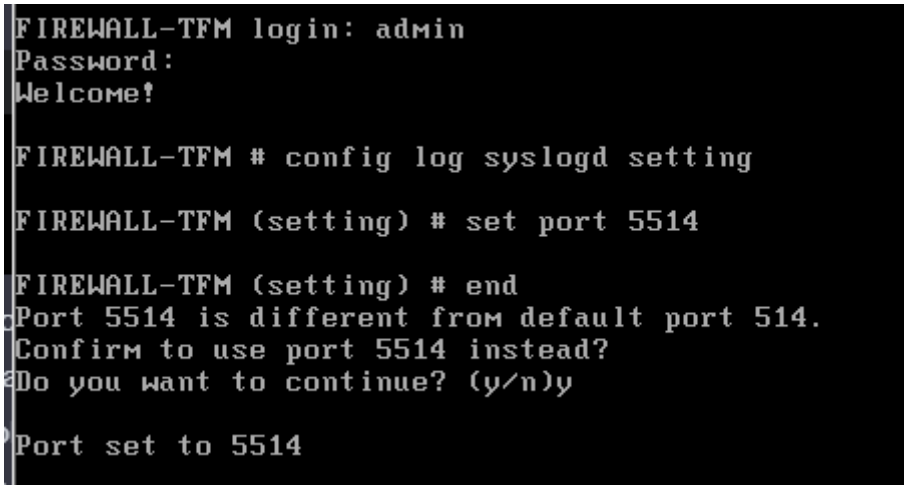


Figura 115.1: Detalle configuración puerto envío syslog FortiGate.

F. Instalación, configuración e integración en SOC de solución Sophos.

Tras contratar la solución Sophos e ingresar en el panel central, se deberá especificar que se requiere la solución “Endpoint Protection”, como se muestra en la siguiente captura.

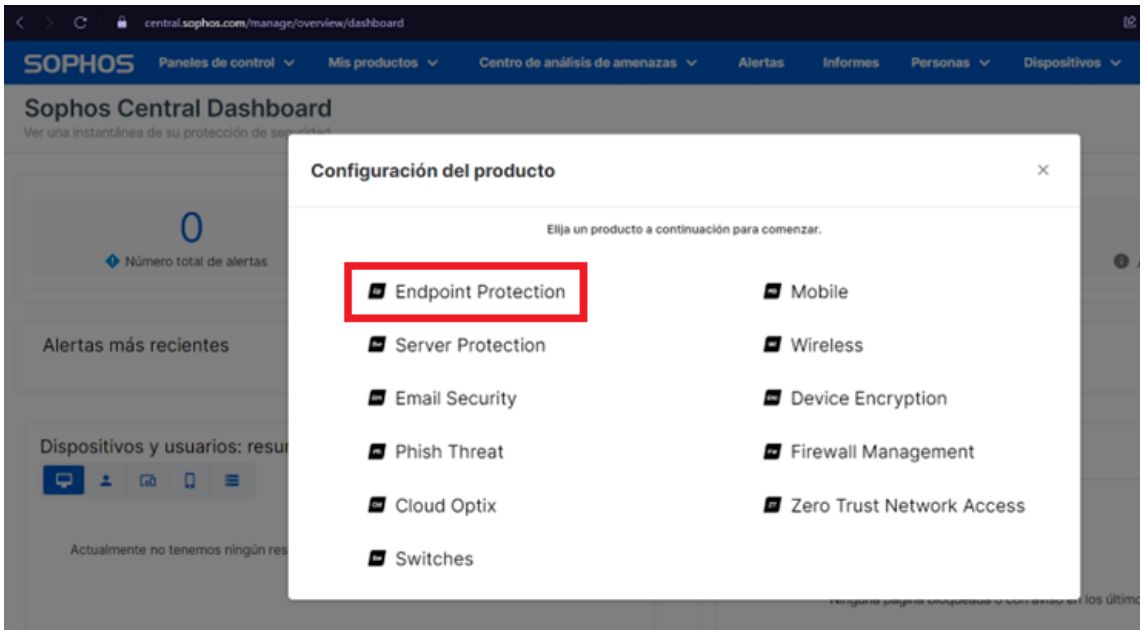


Figura 116: Detalle de la solución Sophos a descargar.

Posteriormente, se deberá descargar el correspondiente instalador.

Figura 117: Detalle del instalador de la solución Sophos a descargar.

Se procederá a la instalación de la solución en la máquina del Endpoint correspondiente. En este caso una máquina con S.O. “Windows 10 x64”.

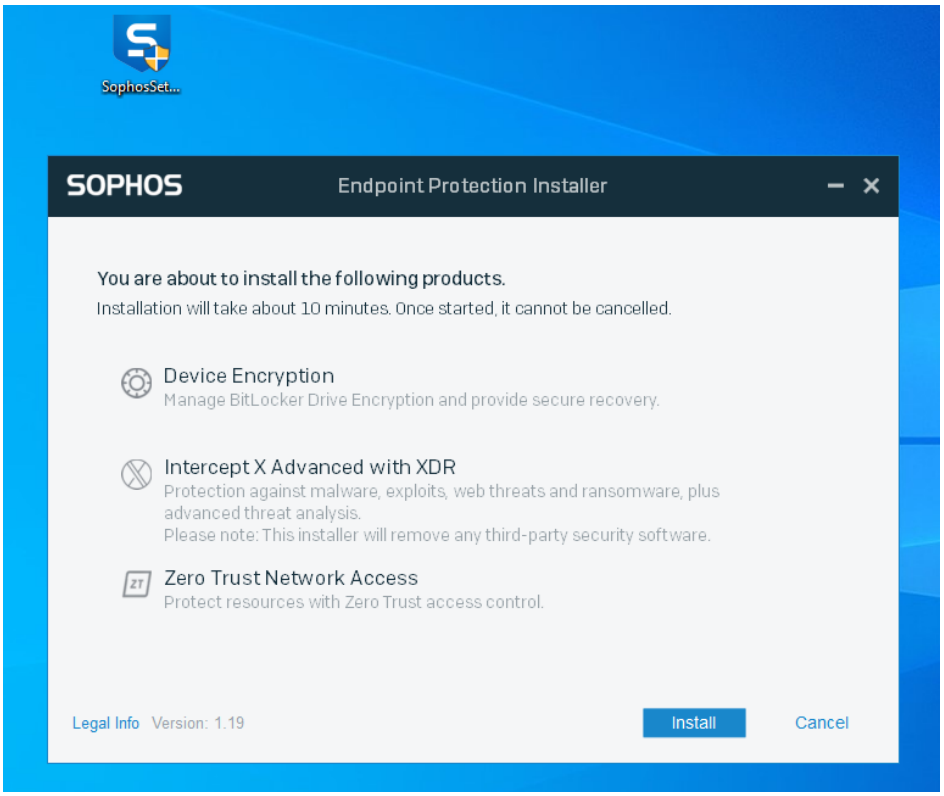


Figura 118: Detalle de la instalación de la solución Sophos.

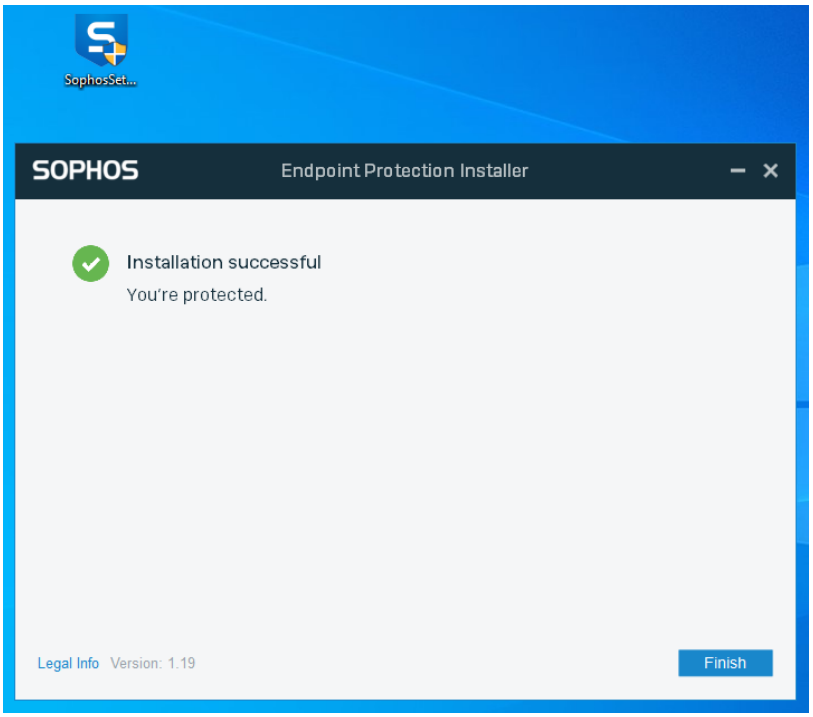


Figura 119: Detalle de la instalación de la solución Sophos.

Una vez finalizada la instalación, se procederá al panel de control de Sophos en la nube, vía Web. En dicho panel se observará que se encuentra registrada la máquina donde se ha instalado la solución.

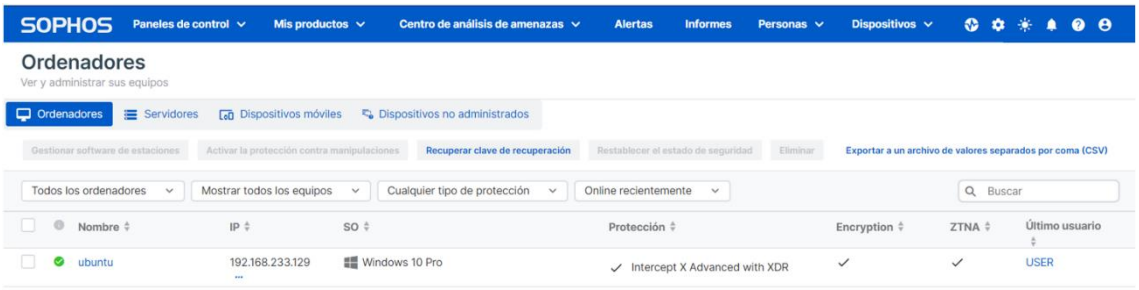


Figura 120: Detalle del panel cloud de la solución Sophos.

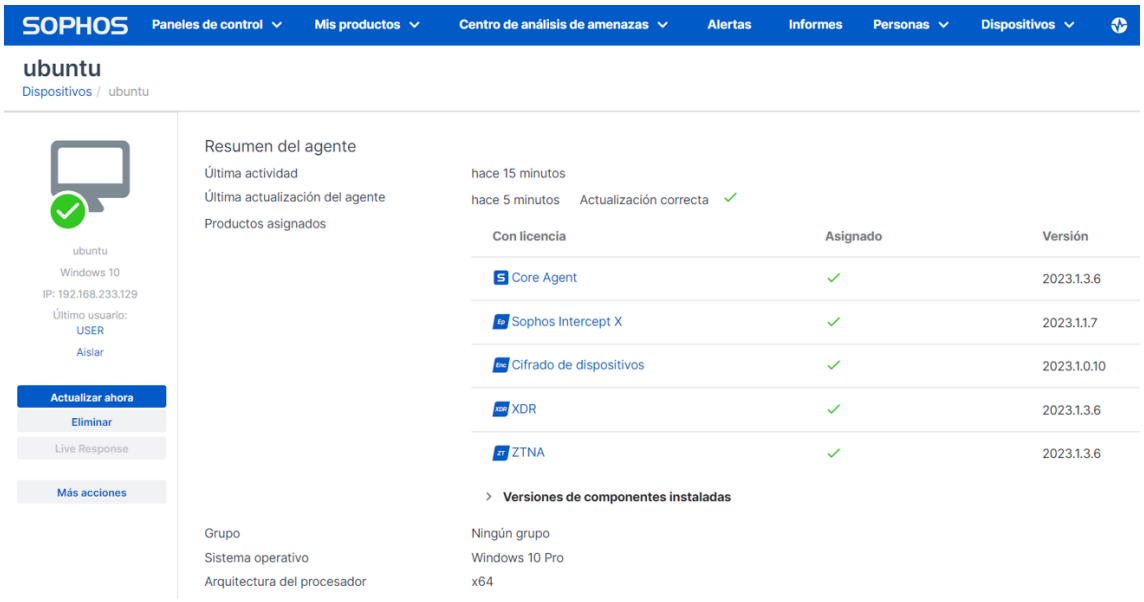


Figura 121: Detalle del endpoint en el panel cloud de la solución Sophos.

Para poder ingresar como administrador en el panel de la solución de escritorio instalada en el endpoint, y acceder a realizar cambios en las configuraciones de la herramienta, se debe obtener la credencial desde el panel de control Web, como se muestra a continuación.

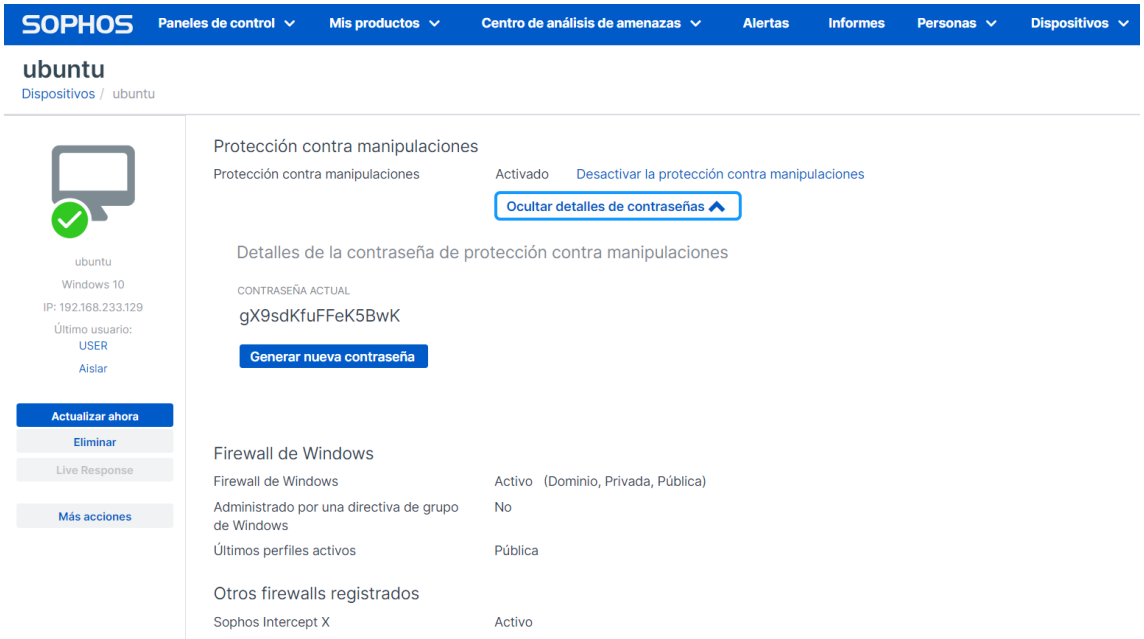


Figura 122: Detalle del endpoint en el panel cloud de la solución Sophos.

Una vez se tenga la credencial, basta con introducirla como se muestra en la siguiente captura.

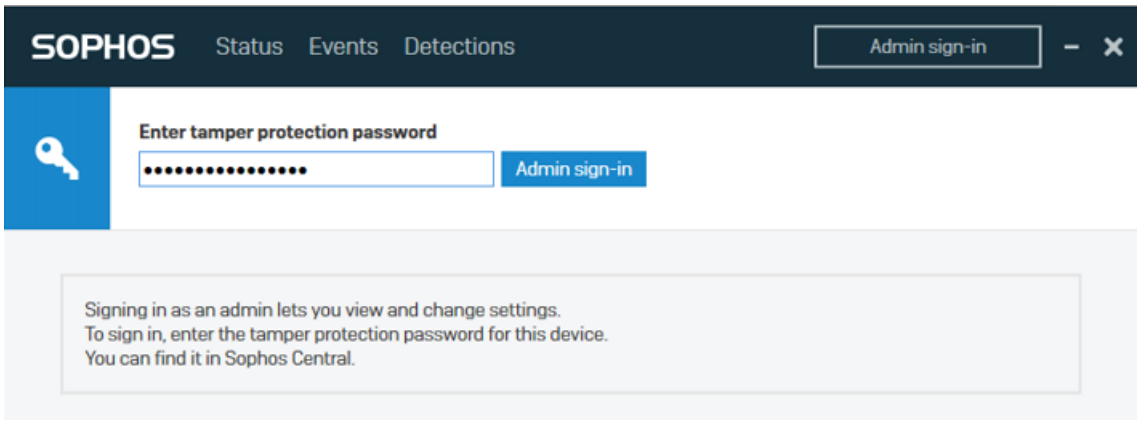


Figura 123: Detalle del logado en la aplicación de escritorio Sophos instalada en el endpoint.

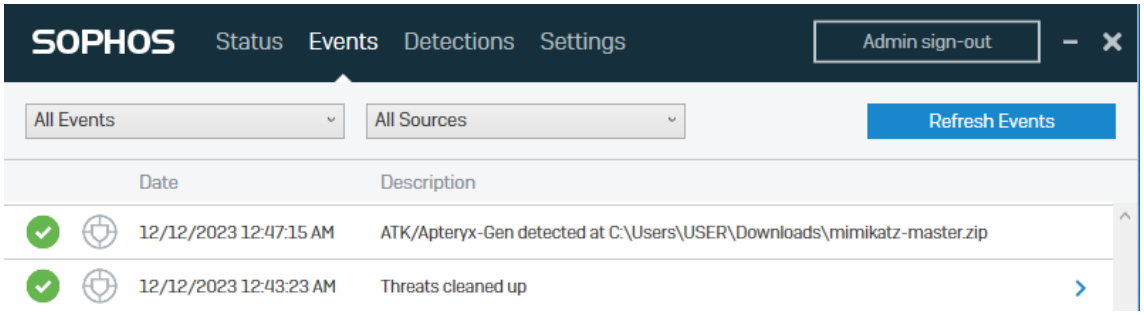


Figura 124: Detalle del logado en la aplicación de escritorio Sophos instalada en el endpoint.

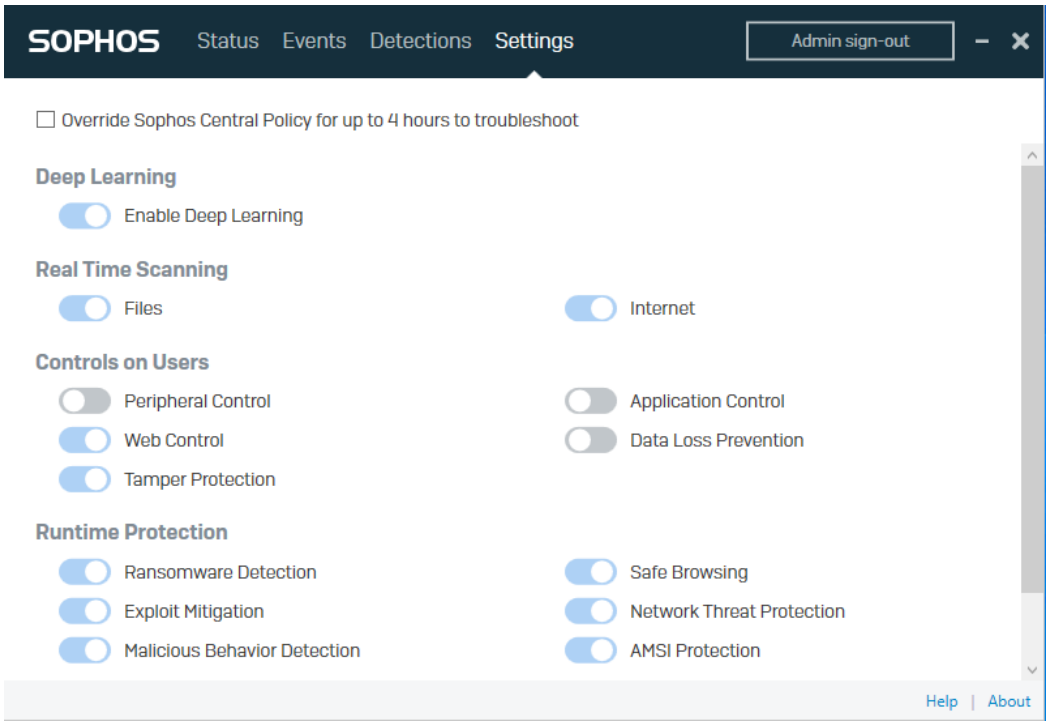


Figura 125: Detalle de las soluciones que presenta la aplicación Sophos instalada en el endpoint.

Para recoger los logs generados por la solución Sophos que se encuentran en la nube, se debe descargar la siguiente solución de su repositorio GitHub:

- <https://GitHub.com/sophos/Sophos-Central-SIEM-Integration/archive/v2.0.1.zip>

Una vez descargada, únicamente se debe configurar el archivo “config.ini” indicando los parámetros “client_id” y “client secret” como corresponda. Estos deben obtenerse del panel cloud de Sophos, en la parte correspondiente a la administración de credenciales de API, como se muestra en la siguiente captura.

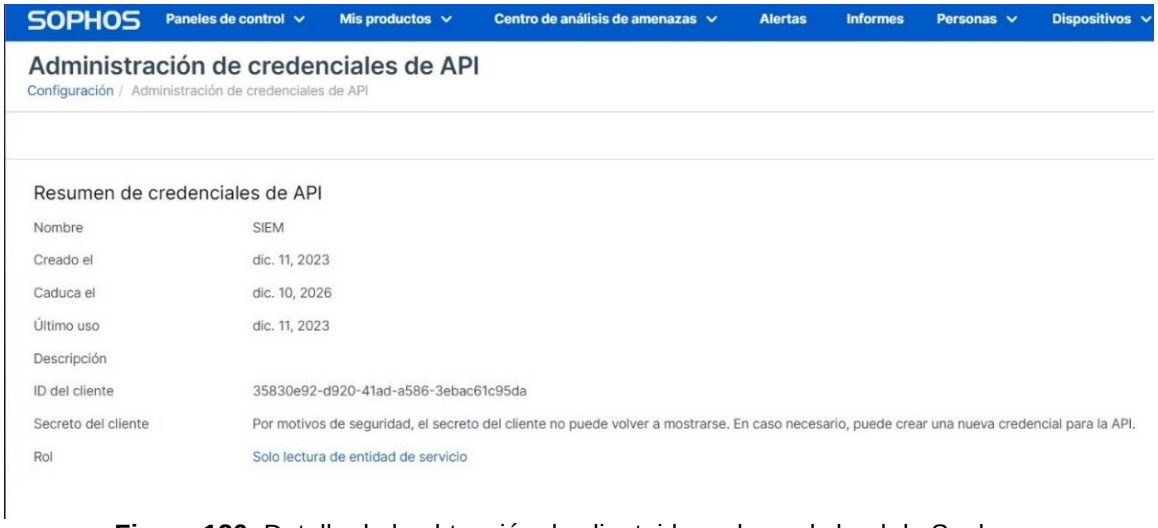


Figura 126: Detalle de la obtención de client_id en el panel cloud de Sophos.

```
[login]
# API Access URL + Headers
# API token setup steps: https://community.sophos.com/kb/en-us/125169
token_info = <Copy API Access URL + Headers block from Sophos Central
here>

# Client ID and Client Secret for Partners, Organizations and Tenants
# <Copy Client ID and Client Secret from Sophos Central here>
client_id = 35830e92-xxxx-41ad-xxxx-3ebac61c95da
client_secret =
a0f5b65c127d6d0868c9cxxxxxxxxxxxxxxcf40e4a93de3728c36ce7058a12
97babc8437fb9d80bbe0b68e8fa706155

# Customer tenant Id
tenant_id =

# Host URL for Oauth token
auth_url = https://id.sophos.com/api/v2/oauth2/token

# whoami API host url
api_host = api.central.sophos.com

# format can be json, cef or keyvalue
format = json

# filename can be SYSLOG, stdout, any custom filename
filename = result.txt

# endpoint can be event, alert or all
endpoint = event

# SYSLOG properties
# for remote address use <remoteServerIp>:<port>, for e.g. 192.1.2.3:514
# for linux local systems use /dev/log
# for MAC OSX use /var/run/SYSLOG
address = /var/run/SYSLOG
facility = daemon
socktype = udp

# cache file full or relative path (with a ".json" extension)
state_file_path = state/siem_sophos.json
```

Figura 127: Detalle del archivo config.ini.

Tras la ejecución de “siem.py”, descarga los eventos generados (logs) por la solución Sophos instalada en los Endpoints, en un archivo con nombre “result.txt”, como vemos a continuación.

Figura x: Detalle de la ejecución de siem.py.

Figura 128: Detalle del archivo result.txt.

Para pasar al SIEM los datos recogidos en el archivo “result.txt”, se deberá especificar la ruta de este en el fichero “pipeline.conf” de Logstash en su parámetro “input”, como se muestra en la siguiente captura.

Figura 129: Detalle del fichero de configuración pipeline.conf.

Finalmente, para que el script “siem.py” descargue del cloud de Sophos los logs generados por esta solución cada 3 minutos, se deberá introducir en el crontab la siguiente línea.

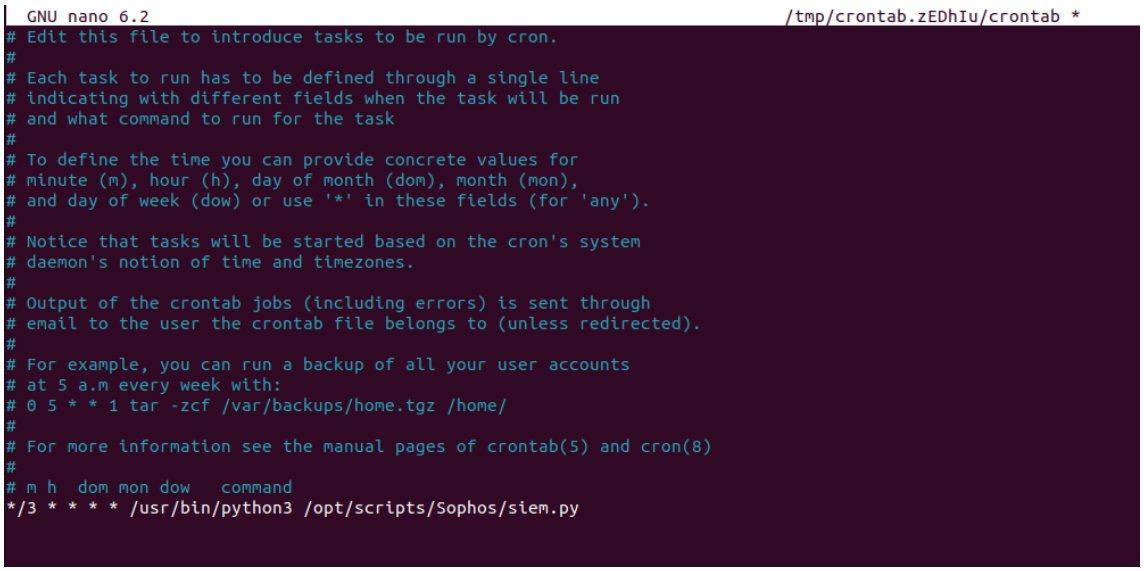


Figura 130: Detalle del crontab para la ejecución del script de descarga de logs de Sophos.

De este modo quedará implementada la solución Sophos correctamente.

G. Instalación, configuración, creación de reglas y ejecución de ElastAlert2.

G.1. Instalación, configuración y ejecución de ElastAlert2.

En la siguiente captura se muestra la instalación de la herramienta ElastAlert2. En el caso que nos atañe se ha realizado la instalación mediante python3.11.

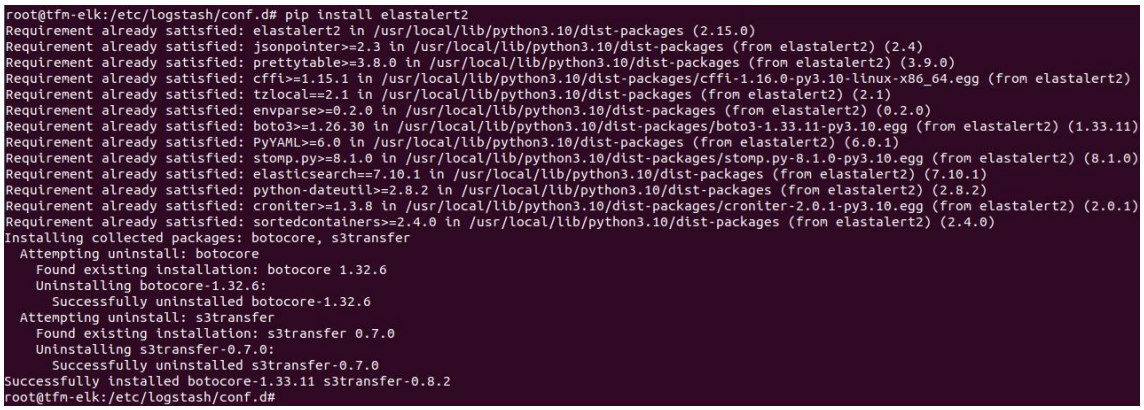


Figura 131: Detalle de la instalación de ElastAlert2.

En el caso de presentar error de módulos no instalados, se deberán instalar los requerimientos presentes en el repositorio de GitHub, como se muestra a continuación.

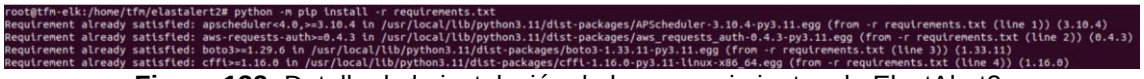


Figura 132: Detalle de la instalación de los requerimientos de ElastAlert2.

A continuación, se muestra el archivo de configuración “elastalert2/config.yaml”.

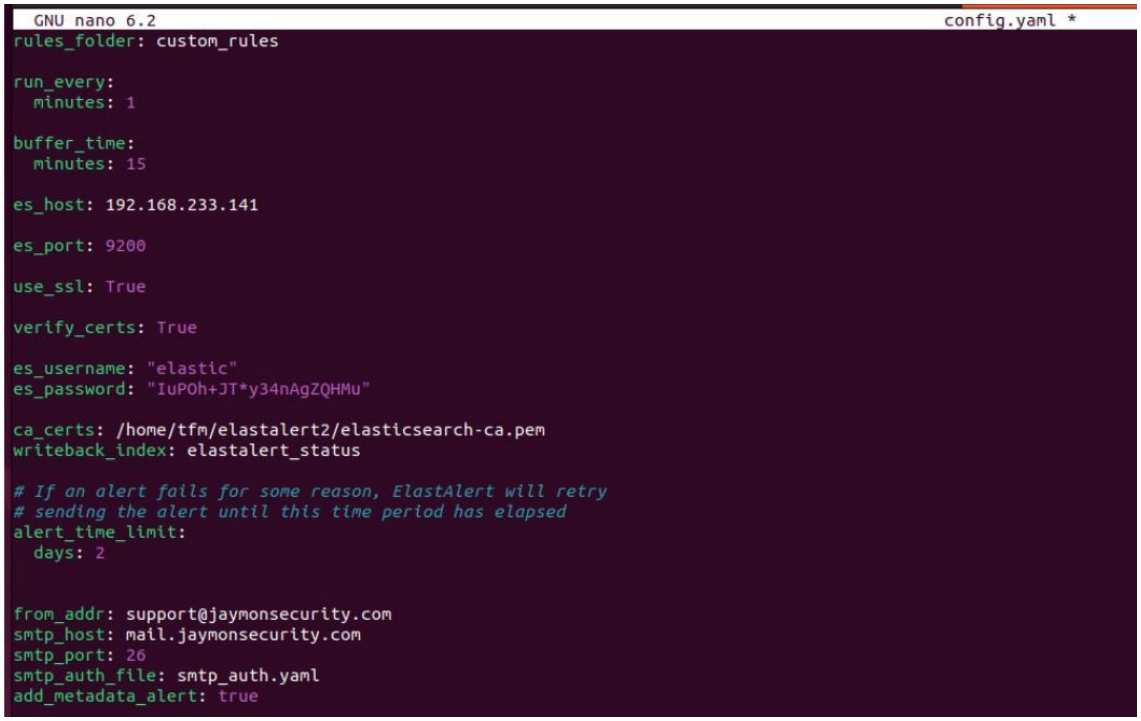


Figura 133: Detalle del fichero de configuración config.yaml.

El archivo “elastalert2/custom_rules/smtp_auth.yaml” guarda las credenciales de configuración de la cuenta de email.

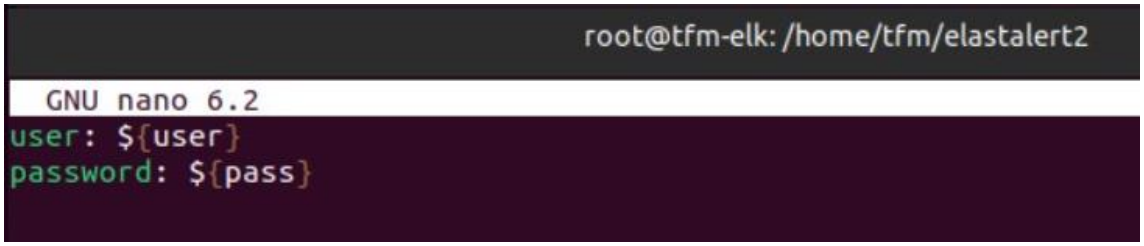


Figura 134: Detalle del fichero de configuración smtp_auth.yaml.

A continuación, se muestra la creación de índices necesarios para almacenar las alertas que se generarán y crear un histórico donde poder buscarlas.

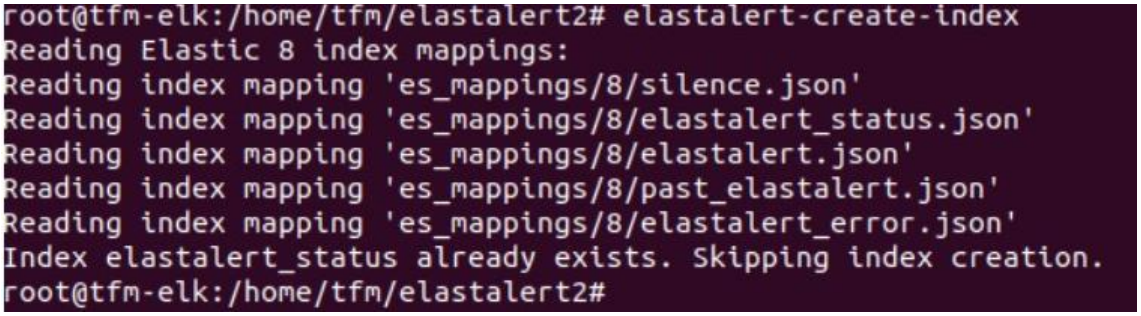


Figura 135: Detalle del comando para la creación de índices.

En la siguiente captura se muestra como ejemplo el archivo "elastalert2/custom_rules/test_rules.yaml", que corresponde a la configuración de una alerta que corresponde a "intento de login fallido". Tras detectarse una alerta de este tipo, se enviará un correo electrónico al email especificado.

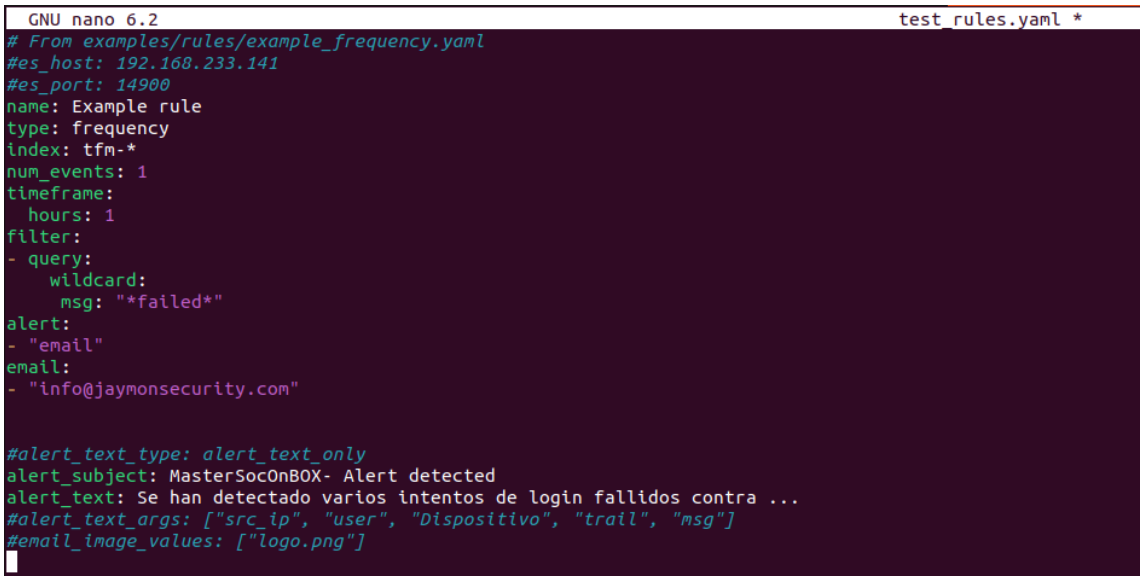


Figura 136: Detalle del fichero de configuración de alerta test_rules.yaml.

La manera de ejecutar ElastAlert2 para la generación de alertas y envío de estas será la siguiente.

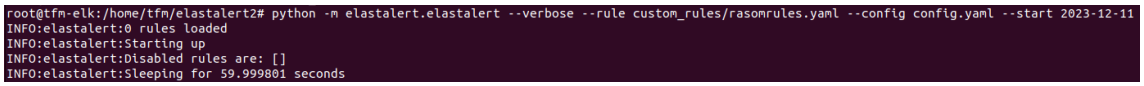


Figura 137: Detalle de la ejecución de ElastAlert2.

G.2. Creación de reglas de ElastAlert2.

A continuación, se muestran las distintas reglas de alertas que se han programado en este Trabajo Fin de Máster.

- En la siguiente captura se muestra cómo se ha creado el archivo "ransomrules.yaml" correspondiente a la alerta de ransomware detectada.

```
name: Ransomware rule
type: frequency
index: tfm-*
num_events: 1
timeframe:
  hours: 24
filter:
- query:
    wildcard:
     msg: "*ransomware*"
alert:
- "email"
email:
- "info@jaymonsecurity.com"


alert_subject: MasterSocOnBOX- Alert detected
alert_text: Se ha detectado ransomware ...
```

Figura 138: Detalle del fichero de configuración de alerta ranwomrules.yaml.

- En la siguiente captura se muestra cómo se ha creado el archivo “exploit.yaml” correspondiente a la alerta de exploit detectada.

```
name: Exploit rule
type: frequency
index: tfm-*
num_events: 1
timeframe:
  hours: 24
filter:
- query:
    wildcard:
     msg: "*exploit*"
alert:
- "email"
email:
- "info@jaymonsecurity.com"

alert_subject: MasterSocOnBOX- Alert detected
alert_text: Se ha detectado exploit ...
```

Figura 139: Detalle del fichero de configuración de alerta exploit.yaml.

- En la siguiente captura se muestra cómo se ha creado el archivo “sshbruteforce.yaml” correspondiente a la alerta de fuerza bruta al servidor SSH detectada.

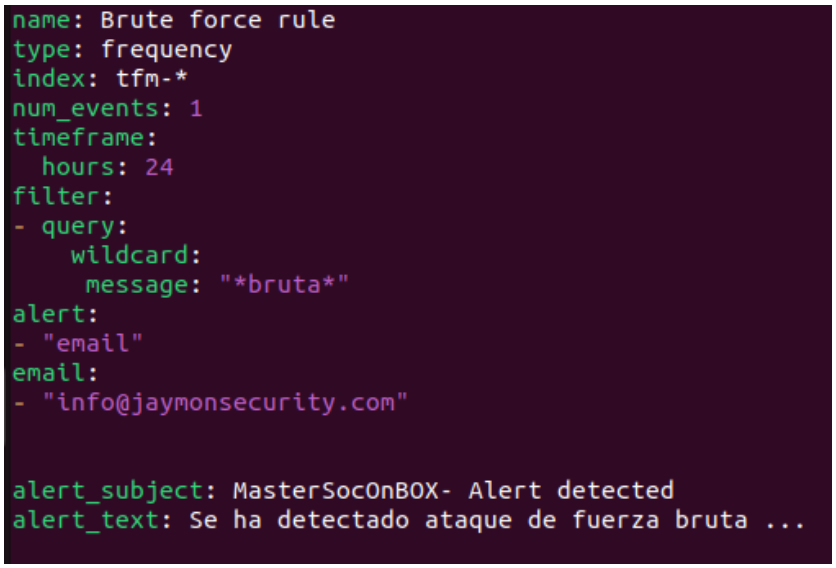


Figura 140: Detalle del fichero de configuración de alerta sshbruteforce.yaml.

- En la siguiente captura se muestra cómo se ha creado el archivo "logonfailure.yaml" correspondiente a la alerta de inicio de sesión fallido detectada.

Figura 141: Detalle del fichero de configuración de alerta logonfailure.yaml.

- En la siguiente captura se muestra cómo se ha creado el archivo "malwareinjection.yaml" correspondiente a la alerta de malware detectada.

```
name: Malware rule
type: frequency
index: tfm-*
num_events: 1
timeframe:
  hours: 24
filter:
- query:
    wildcard:
     msg: "*malware*"
alert:
- "email"
email:
- "info@jaymonsecurity.com"


alert_subject: MasterSocOnBOX- Alert detected
alert_text: Se ha detectado malware ...
```

Figura 142: Detalle del fichero de configuración de alerta malwareinjection.yaml.

- En la siguiente captura se muestra cómo se ha creado el archivo “scanports.yaml” correspondiente a la alerta de escaneo de puertos detectada.

```
name: Scan ports rule
type: frequency
index: tfm-*
num_events: 1
timeframe:
  hours: 24
filter:
- query:
    wildcard:
     message: "*scan*"
alert:
- "email"
email:
- "info@jaymonsecurity.com"


alert_subject: MasterSocOnBOX- Alert detected
alert_text: Se ha detectado escaneo de puertos ...
```

Figura 143: Detalle del fichero de configuración de alerta scanports.yaml.

- En la siguiente captura se muestra cómo se ha creado el archivo “sqli.yaml” correspondiente a la alerta de SQLi detectada.

Figura 144: Detalle del fichero de configuración de alerta sqli.yaml.

- En la siguiente captura se muestra cómo se ha creado el archivo "webcontrolviolation.yaml" correspondiente a la alerta de seguridad de navegación web detectada.

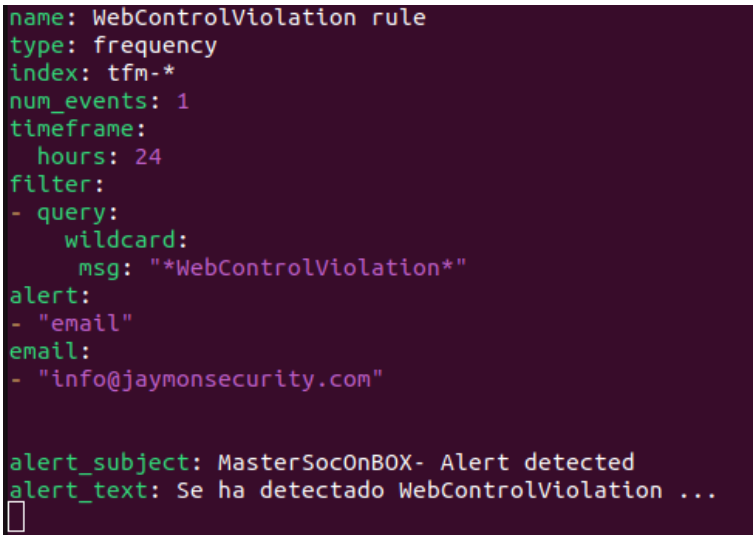


Figura 145: Detalle del fichero de configuración de alerta webcontrolviolation.yaml.

De esta manera se podrán crear todas las alertas que se estimen necesarias.

H. Montaje de aplicación Web vulnerable a SQLi para pruebas del SOC.

Para llevar a cabo el montaje del escenario que servirá de laboratorio de pruebas para observar la eficacia del "Master SOC on Box", se va a instalar la solución XAMPP en una máquina con Sistema Operativo Windows. A continuación, se muestra la página web oficial desde donde se debe descargar el instalador para proceder a su instalación.

Figura 146: Web oficial para la descarga de Xampp para Windows.

Una vez realizada dicha instalación, se procede a activar el servidor Web Apache (que incluye PHP) y el servidor MySQL que será el encargado de la Base de Datos (BBDD).

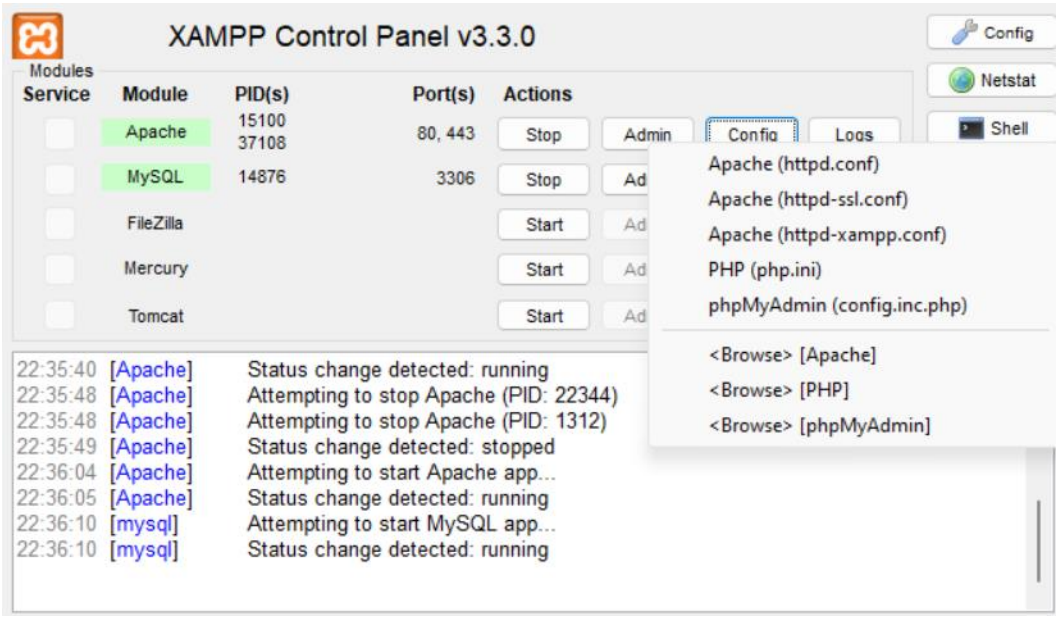


Figura 147: Detalle de activación de servidor web Apache y servidor de BBDD MySQL.

Una vez realizado lo anterior, se deberá acceder a la interfaz web de “phpMyAdmin” a través del botón “Admin” de MySQL, para montar la BBDD que será necesaria para el funcionamiento de la página Web.

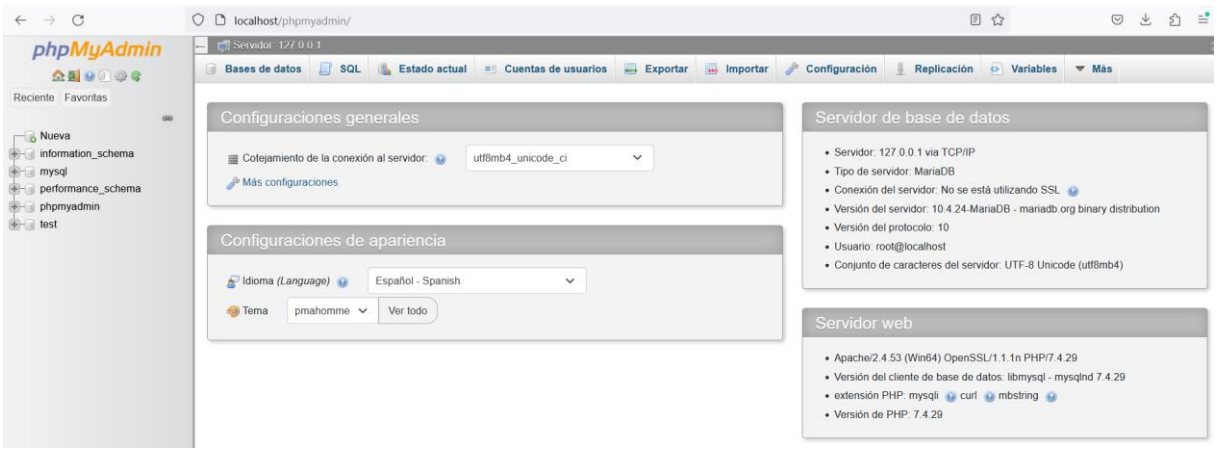


Figura 148: Detalle de acceso a la interfaz web de phpMyAdmin.

Los comandos que ejecutar para montar la BBDD se encuentran en el anexo H.1 “Comandos para la creación de la Base de Datos”.

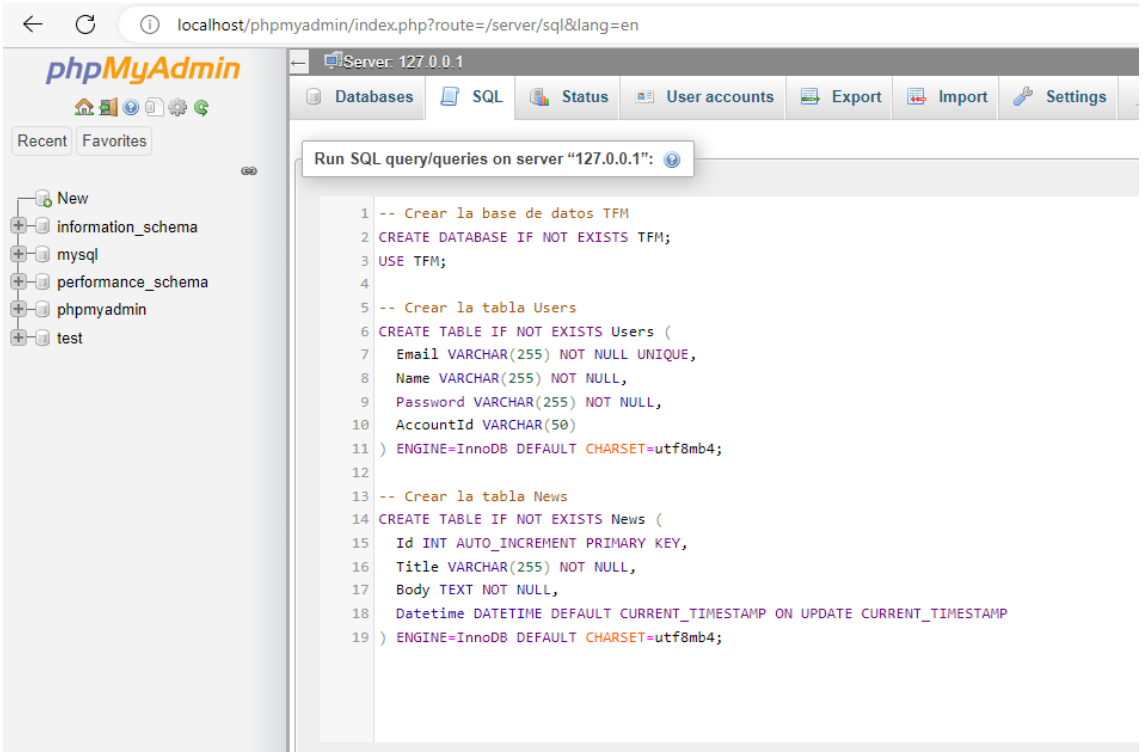


Figura 149: Detalle de la creación de BBDD, tablas y columnas.

Tras ejecutar las instrucciones correspondientes, se observa la creación de la BBDD con sus tablas y columnas.

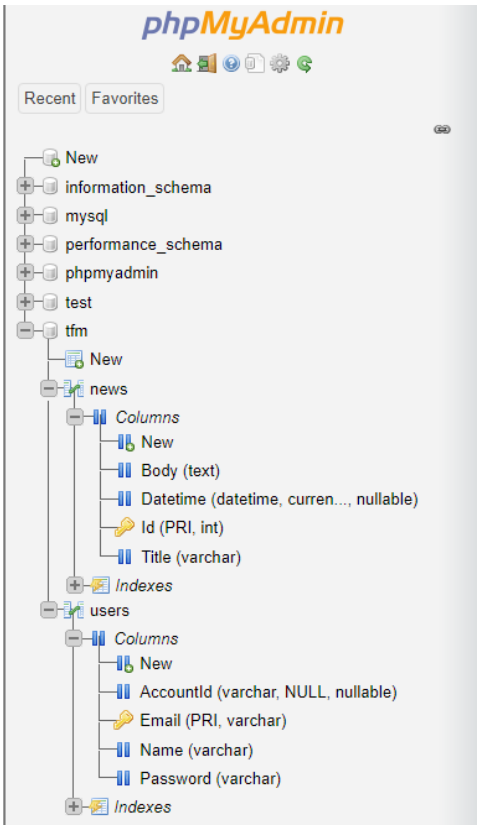


Figura 150: Detalle de las BBDD, tablas y columnas creadas.

A continuación, se crea un usuario con los privilegios necesarios para manejar la BBDD.

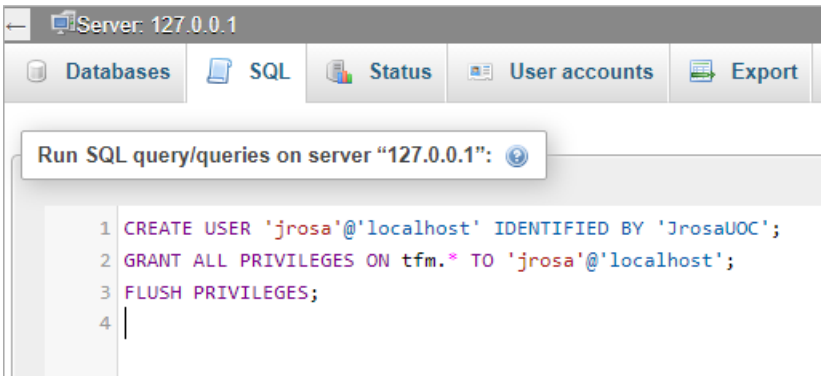


Figura 151: Detalle de la creación del usuario para la BBDD TFM.

Finalmente, se aloja en el directorio "htdocs" el archivo "index.php" con el código fuente presentado en el anexo H.2 "Código fuente de index.php".

Tras haber realizado con éxito los pasos anteriores, se podrá observar que la página web está lista para llevar a cabo las pruebas de inyecciones que se estimen convenientes.

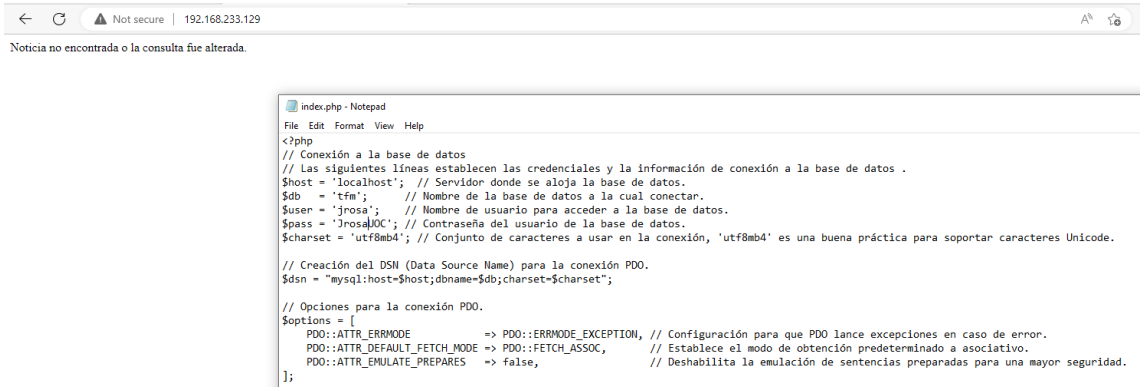


Figura 152: Detalle del correcto funcionamiento de la aplicación Web.

H.1 Comandos para la creación de la Base de Datos.

```
-- Crear la base de datos TFM
CREATE DATABASE IF NOT EXISTS TFM;
USE TFM;

-- Crear la tabla Users
CREATE TABLE IF NOT EXISTS Users (
  Email VARCHAR(255) NOT NULL UNIQUE,
  Name VARCHAR(255) NOT NULL,
  Password VARCHAR(255) NOT NULL,
  AccountId VARCHAR(50)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

-- Crear la tabla News
CREATE TABLE IF NOT EXISTS News (
  Id INT AUTO_INCREMENT PRIMARY KEY,
  Title VARCHAR(255) NOT NULL,
  Body TEXT NOT NULL,
  Datetime DATETIME DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

-- Crear usuario con privilegios sobre la BBDD
CREATE USER 'jrosa'@'localhost' IDENTIFIED BY 'JrosaUOC';
GRANT ALL PRIVILEGES ON tfm.* TO 'jrosa'@'localhost';
FLUSH PRIVILEGES;
```

Figura 153: Detalle del código para la creación de BBDD, tablas y columnas, y usuario.

H.2 Código fuente de “index.php”.

```
<?php
// Conexión a la base de datos
// Las siguientes líneas establecen las credenciales y la información de conexión a la base de datos .
$host = 'localhost';  // Servidor donde se aloja la base de datos.
$db   = 'tfm';      // Nombre de la base de datos a la cual conectar.
$user = 'jrosa';    // Nombre de usuario para acceder a la base de datos.
$pass = 'JrosaUOC'; // Contraseña del usuario de la base de datos.
$charset = 'utf8mb4'; // Conjunto de caracteres a usar en la conexión, 'utf8mb4' es una buena práctica
para soportar caracteres Unicode.
// Creación del DSN (Data Source Name) para la conexión PDO.
$dsn = "mysql:host=$host;dbname=$db;charset=$charset";
// Opciones para la conexión PDO.
$options = [
PDO::ATTR_ERRMODE           => PDO::ERRMODE_EXCEPTION, // Configuración para que PDO
lance excepciones en caso de error.
PDO::ATTR_DEFAULT_FETCH_MODE => PDO::FETCH_ASSOC,       // Establece el modo de
obtención predeterminado a asociativo.
PDO::ATTR_EMULATE_PREPARES   => false,                  // Deshabilita la emulación de sentencias
preparadas para una mayor seguridad.
];
// Intento de conexión a la base de datos utilizando PDO.
try {
$pdo = new PDO($dsn, $user, $pass, $options); // Intenta crear una nueva instancia de PDO con las
opciones definidas.
} catch (\PDOException $e) { // Captura de excepciones en caso de fallo en la conexión.
throw new \PDOException($e->getMessage(), (int)$e->getCode()); // Relanza la excepción con el
mensaje y código de error original.
}
// Obtención del parámetro 'id' de la URL
$id = isset($_GET['id']) ? $_GET['id'] : ''; // Obtiene el parámetro 'id' de la URL a través del método GET.
// Código vulnerable a Blind SQL Injection.
$sql = "SELECT EXISTS(SELECT 1 FROM News WHERE Id = '$id' AND SLEEP(2))"; // Se incluye el
parámetro 'id' directamente en la consulta
// Si la condición WHERE se cumple, la consulta se retrasará.
// Medición del tiempo de ejecución de la consulta
$startTime = microtime(true); // Marca el inicio del tiempo antes de ejecutar la consulta.
$stmt = $pdo->query($sql);     // Ejecuta la consulta directamente, lo cual es inseguro en un contexto
real.
$endTime = microtime(true);    // Marca el final del tiempo después de ejecutar la consulta.
// Análisis del tiempo de respuesta para inferir la existencia de la noticia
if ($endTime - $startTime > 2) { // Si el tiempo de ejecución supera los 2 segundos, se asume que la
noticia existe.
// Recuperación segura de los detalles de la noticia
$sql = "SELECT Title, Body, Datetime FROM News WHERE Id = ?"; // Consulta segura con marcador
de parámetro.
$stmt = $pdo->prepare($sql); // Prepara la consulta.
$stmt->execute([$id]);       // Ejecuta la consulta con el ID proporcionado.
$news = $stmt->fetch();      // Obtiene los datos de la noticia.
// Verificación y presentación de la noticia
if ($news) {
// Si se encontró la noticia, imprime su título, fecha y cuerpo.
echo "<h1>{$news['Title']}</h1>";
echo "<p>{$news['Datetime']}</p>";
echo "<p>{$news['Body']}</p>";
} else {
// Si no se encontró la noticia, imprime un mensaje indicándolo.
echo "Noticia no encontrada.";
}
} else {
// Si la consulta se ejecuta rápidamente, se asume que la noticia con ese ID no existe.
echo "Noticia no encontrada o la consulta fue alterada.";
}
?>
```

Figura 154: Detalle del código fuente de index.php.

I. Montaje de dashboards de Kibana.

Se debe entrar en los ajustes “Analytics – Dashboard” como se observa en la siguiente captura, y posteriormente pulsar sobre el botón “Create dashboard”.

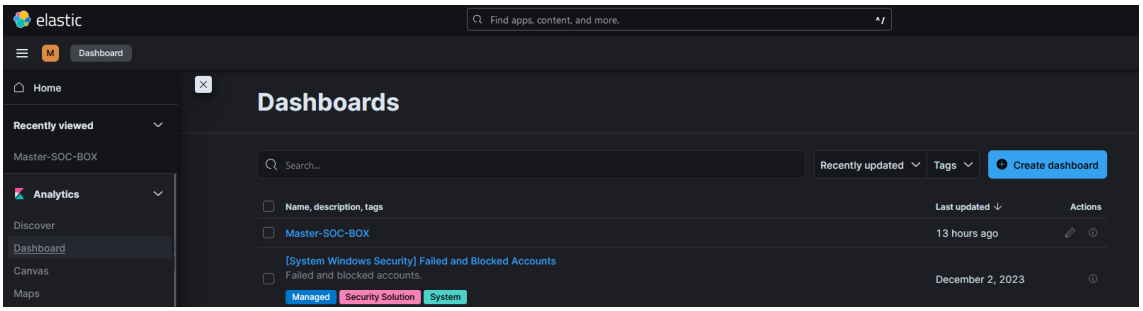


Figura 155: Detalle de creación del dashboard.

Llegados a este punto, basta con ir a la sección “Analitycs”, pulsar sobre el indicador o indicadores que se requieran presentar en el dasboard y pulsar la opción de “visualizar”, como se muestra en la siguiente captura.

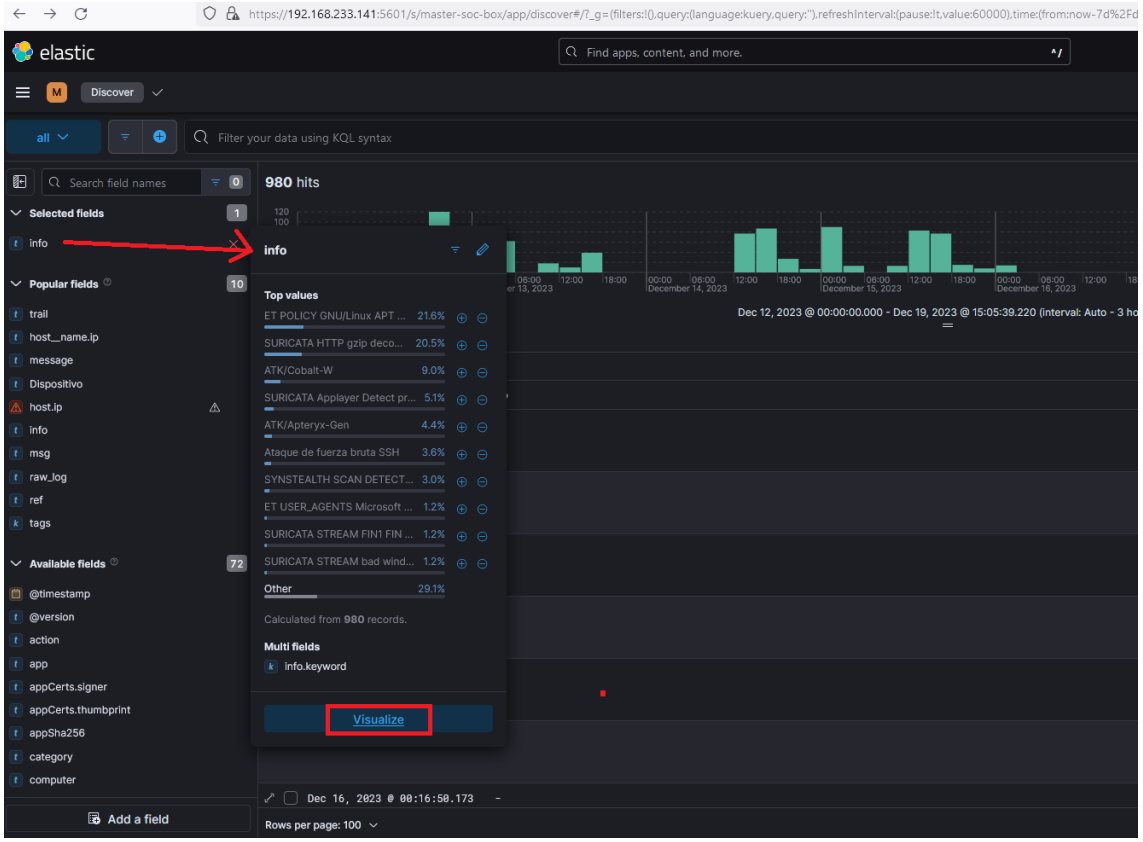


Figura 156: Detalle de creación del gráfico con indicador “info”.

Posteriormente, se presentará el gráfico con los datos de los indicadores elegidos.

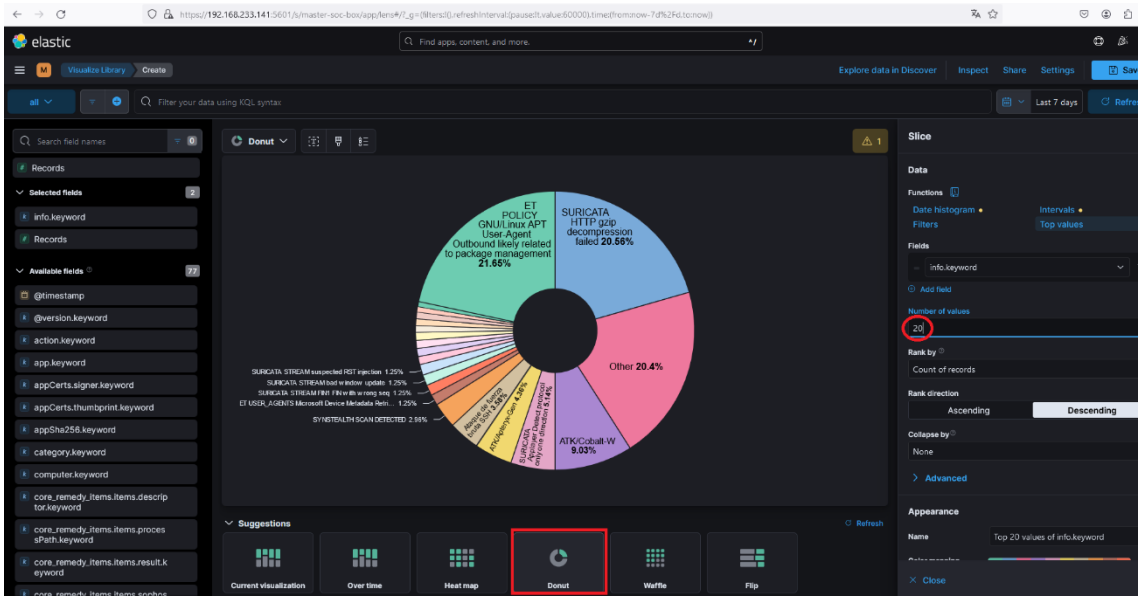


Figura 157: Detalle de creación del gráfico con indicador “info”.

Finalmente, se deberán guardar los avances realizados indicando título y dashboard. En este caso se le ha indicado guardar en el dashboard “Master-SOC-BOX”, como se muestra en la siguiente captura.

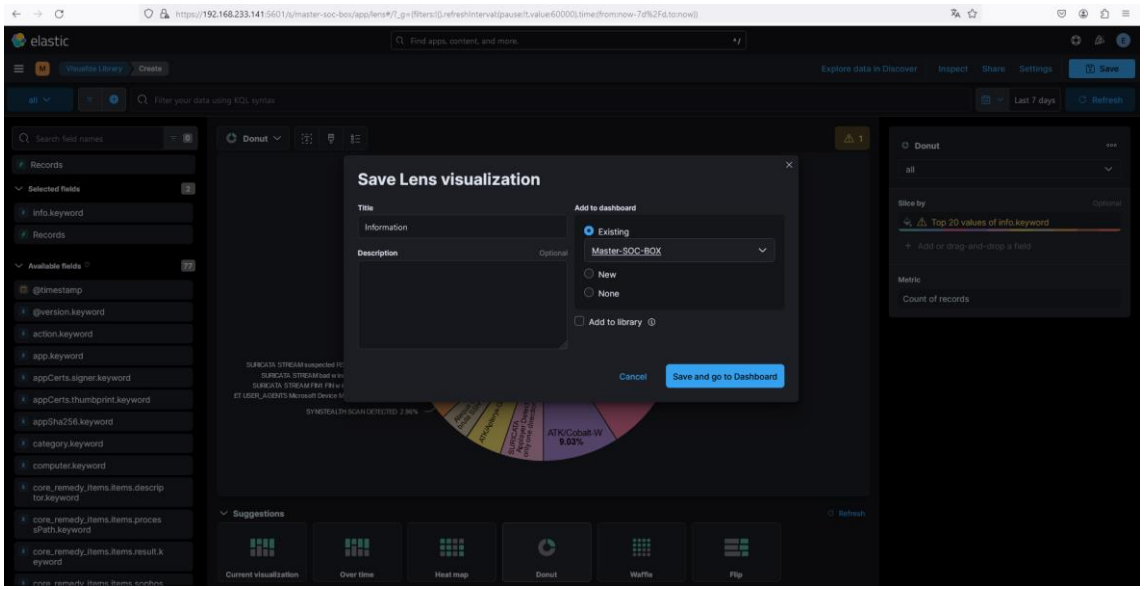


Figura 158: Detalle del proceso de almacenamiento del gráfico en el dashboard.

Huelga comentar que hay distintos tipos de gráficos, como se muestra en la parte inferior de la captura anterior. De este modo, se ha procedido a crear distintas gráficas donde mostrar información diversa sobre detecciones y alertas clasificadas por indicadores que comprenden dispositivos y aplicaciones.

Así pues, como se ha descrito anteriormente se pueden montar tantos paneles como se requieran, mostrando en cada uno de ellos las distintas variables que contengan la información que se estime oportuno mostrar.

En cuanto a lo que acontece al “Master SOC on BOX”, tras finalizar la configuración de todos los paneles, en la siguiente captura se puede observar cómo se visualizan por gráficos las detecciones de cada dispositivo integrado.

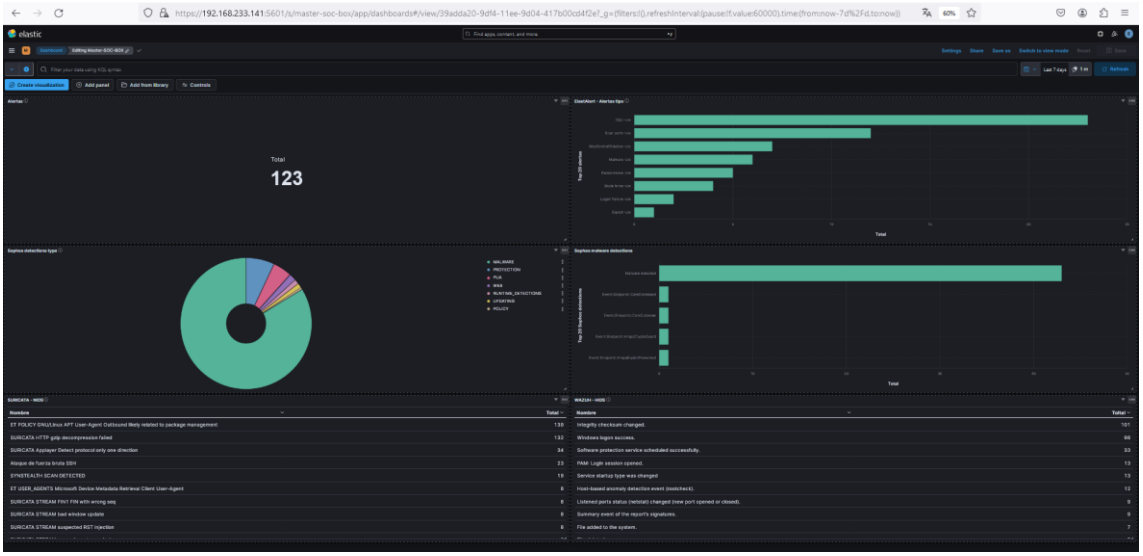


Figura 159: Detalle del aspecto del dashboard final.

J. Casos de uso.

A continuación, se muestra una lista de casos de uso. Es importante consultar la documentación específica de cada SIEM para obtener la lista de reglas que vienen incluidas.

- **Windows:**
    - Apagado/reinicio de Servidor.
    - Medios extraíbles detectados.
    - Apagado anormal de Windows.
    - Intentos de inicio de sesión con la misma cuenta desde diferentes escritorios.
    - Detección de apagado-reinicio de servidor después de horas de oficina.
    - Cambio de membresía en el grupo administrativo.
    - Inicios de sesión no autorizados de cuenta predeterminada.
    - Uso interactivo de cuenta de servicio.
    - Inicio de sesión remoto: éxito y falla.
    - Detención/reinicio de servicio de Windows.
    - Conjunto de ACL en miembros del grupo Admin.
    - Cuenta de Windows habilitada/deshabilitada.
    - Varias cuentas de Windows bloqueadas.
    - Múltiples inicios de sesión de Windows por el mismo usuario.
    - Intento de fuerza bruta desde la misma fuente.
    - Inicios de sesión fuera del horario comercial habitual.
    - Inicios de sesión en múltiples cuentas de usuario desde la misma fuente.

- Intento de fuerza bruta desde la misma fuente con inicio de sesión exitoso.
- Cuenta de Windows creada/eliminada.
- Fallo de hardware de Windows.
- Inicio de sesión fallido a múltiples destinos desde la misma fuente.
- Cuentas administrativas: Múltiples fallos de inicio de sesión.
- Detección de cuenta de usuario agregada/eliminada en grupo administrativo.
- Detección de cambios en la hora del sistema (hora de arranque).
- Detección del uso de cuentas predeterminadas del proveedor del producto.
- Usuario eliminado dentro de las 24 horas de haber sido creado.
- Servicio crítico detenido en servidores Windows.
- Registro de seguridad de Windows está lleno.
- Múltiples cambios de contraseña en poco tiempo.
- Tipo de grupo de Windows fue cambiado.
- Cambio de política de auditoría.
- Registro de auditoría borrado.
- Registro de seguridad de Windows está lleno.
- Detección de cuenta de usuario agregada.
- Fallo de inicio de sesión: Se hizo un intento de inicio de sesión con una cuenta caducada.
- Alto número de usuarios creados/eliminados en un corto período de tiempo.
- Tráfico saliente observado desde servidores a Internet.
- Inicios de sesión fallidos/intentos con cuentas deshabilitadas/ex-empleados/caducadas.
- Eliminación de archivo/carpeta de Windows.
- Cambios de permiso de archivo/carpeta de Windows.
- Alto número de usuarios creados/eliminados en un corto período de tiempo.

- **Unix:**

  - Eventos de importación y exportación de archivos FTP de Unix.
  - Sistema de archivos de Unix lleno.
  - Apagado del servidor.
  - Usuarios creados/eliminados en un corto período.
  - Grupo de usuarios creado/eliminado en un corto período.
  - Intentos de inicio de sesión en Unix con la misma cuenta desde diferentes escritorios.
  - Inicios de sesión fallidos.
  - Inicios de sesión fallidos con cuentas deshabilitadas.
  - Acceso a inicio de sesión FTP de Unix.
  - Múltiples conexiones SFTP de Unix.
  - Inicios de sesión fallidos desde acceso ”root”.
  - Múltiples fallos de inicio de sesión de SU en Unix.
  - Intentos de inicio de sesión remoto usando el usuario Root en el nodo de producción.
  - Acceso Sudo desde usuarios no Sudo.

- Detección del uso de cuentas predeterminadas del proveedor del producto.
- Agregar o eliminar usuarios al grupo "root".
- Detención de servicio crítico.
- Alto número de fallos de inicio de sesión para la misma cuenta en un corto tiempo.
- Cambio de contraseña.
- Agregar, eliminar y modificar trabajos “cron”.
- Fallos de inicio de sesión de SU.
- Detección de cambio en la configuración de “SYSLOG”.
- Detección de cambio en la configuración de red.

- **Firewall, IPS:**

  - Fallo de inicio de sesión del administrador.
  - Fuerza bruta con cambios de configuración exitosos.
  - Evento de conmutación por error del firewall.
  - Conexión exitosa desde IP de internet después de bloqueos repetitivos en el firewall.
  - Intentos de acceso en protocolos y puertos no identificados.
  - Evento de explotación seguido de host de escaneo.
  - Acceso saliente a IPs de destino inválidas.
  - Inicio de sesión exitoso entre horas no laborales.
  - Reinicios del firewall.
  - Detección de modificaciones de cuenta de usuario/grupo.
  - Usuario agregado/eliminado a la base de datos del firewall.
  - Detección de tráfico inseguro como FTP, telnet, en servidores críticos.
  - Detección de adición/eliminación de un administrador de Firewall.
  - Inicio de sesión denegado (fuerza bruta) .
  - Alto número de eventos denegados.
  - Cambio de configuración detectado.
  - El enlace al dispositivo par está inactivo debido a un problema de cableado físico o un problema de configuración de NSRP.
  - Intentos de escaneo de puerto y host de red.
  - Detección de cambio de primario a secundario.
  - Un administrador ha permitido/eliminado el acceso al firewall desde una IP específica.
  - Tráfico P2P detectado.
  - Alerta de alta utilización de CPU en el firewall.
  - Fallo del firewall al asignar memoria RAM.
  - Detección de cualquier tipo de fallo relacionado con el firewall en espera.
  - Tráfico superior rechazado desde DMZ, FW.
  - Tráfico saliente observado en puertos importantes.
  - Tráfico saliente exitoso a dirección IP de amenaza en lista negra.
  - Múltiples tráficos salientes fallidos a dirección IP de amenaza en lista negra.

- **Correo electrónico:**
    - Fuga de datos identificada a través de archivos grandes enviados por correo.
    - Adjuntos maliciosos/sospechosos identificados.
    - Monitoreo de correos salientes del dominio de la compañía a otros dominios después del horario de oficina.
    - Alta utilización del ancho de banda de correo electrónico por usuarios individuales.
    - Detección de mensajes no entregados.
    - Acceso al buzón por otro usuario.
    - Usuario logado en el sistema enviando un email como otro usuario.
    - Usuario enviando un mensaje en nombre de otro usuario.
    - Detección de usuarios que inician sesión en el buzón que no es su cuenta principal.
    - Detección de correos redirigidos automáticamente.

- **VPN:**
    - Tráfico de red no autorizado detectado.
    - Las principales cuentas de VPN iniciaron sesión desde múltiples ubicaciones remotas.
    - Intentos de inicio de sesión no autorizados.
    - Inicio de sesión anónimo desde dirección IP desconocida.
    - Cuenta de VPN iniciada desde múltiples ubicaciones en un corto período de tiempo o desde países sospechosos.
    - Inicio de sesión simultáneo desde múltiples ubicaciones para un solo usuario.
    - Conexión VPN más allá de 24 horas.
    - Acceso VPN desde dirección IP interna.
    - Acceso VPN desde el extranjero.

- **Proxy:**
    - Intentos de acceso en protocolos y puertos no identificados.
    - Acceso a dominio/IP de malware.
    - Acceso a software potencialmente no deseado.
    - Host DNS dinámico.
    - Fuentes maliciosas/Malnets.
    - Datos maliciosos salientes/Botnets.
    - Peer-to-Peer (P2P).
    - Evasión de proxy.
    - Herramientas de acceso remoto.
    - Acceso desde agente de usuario inusual.
    - Solicitud de post a sitios no categorizados después del horario de oficina.
    - Cambios en la configuración del proxy.
    - Intento fallido de inicio de sesión en proxy.
    - Violación de acceso a contenido.
    - Acceso anónimo a proxy.
    - Acceso a sitio web de herramientas de hacker.

- Intentos de acceso por BOTNET identificados por encabezado de solicitud HTTP.

- **Bases de Datos (BBDD):**

  - Contraseña caducada.
  - Uso de comando crítico.
  - Comandos críticos ejecutados en la base de datos durante horas no laborables.
  - Comandos de actualización o inserción.
  - Usuario creado/eliminado.
  - Múltiples fallos de inicio de sesión observados para la base de datos.
  - Creación/modificación de esquema de base de datos.
  - Principales fallos de ejecución de consultas.
  - Uso de cuentas predeterminadas del proveedor en contra de la política.
  - Acceso a la base de datos durante horas no laborables.
  - Fallos de inicio de sesión para cuentas sys/system o privilegiadas.
  - Conexión a bases de datos de producción desde segmentos de red no permitidos.

- **Routers y Switches:**

  - Mensajes de error de emergencia del router.
  - Cambio de configuración.
  - Mensajes críticos observados desde el SWITCH.
  - Mensajes de alerta observados desde el SWITCH.
  - Archivo descartado debido a gran tamaño.
  - Detección de nueva adición de política.
  - Detección de violación de política.
  - Detección de filtrado de contenido.
  - Fallo/éxito de autenticación.

- **Anti-virus (AV):**

  - Detección de tráfico de backdoor en la red.
  - Identificación de almacenamiento removible.
  - Infección de malware identificada (troyano, ransomware, etc.).
  - Múltiples infecciones de malware identificadas desde el mismo host.
  - Múltiples fuentes accediendo a la misma URL de malware.
  - Fallo de detección de actualización de DAT de Antivirus en máquinas de usuario final.
  - Detección de brote de malware Worm en la red.
  - Intento de detener los horarios de escaneo Ad hoc/diarios.
  - Intento de detener los Servicios AV.
  - Intento de detener los módulos críticos AV.
  - Identificación de máquinas Rogue en la red.
  - Detección del escaneo que se detiene antes de completarse.

- Detección de que el escaneo programado se detiene/pausa (retrasado).
- Detección del equipo que no está protegido con las últimas definiciones.
- Detección de la nueva instalación de software del cliente.
- Detección de la desinstalación del software del cliente.
- Múltiples recurrencias de infección única identificada desde la misma máquina.
- Monitorización de tráfico emergente hacia/desde la máquina infectada en dominios/IP en lista negra.
- Intento de fuerza bruta/escaneo de puerto o host/intento de elevación de privilegios desde la máquina infectada.
- Intento de reiniciar el servicio AV o proceso, módulos AV desde la máquina infectada.
- Acceso a compartir archivo crítico por recursos compartidos (movimientos laterales), SSH o RDP desde el host Infectado.

- **No categorizado:**

  - Uso de cuenta de usuario por defecto.
  - Cuentas de usuario inactivas.
  - Monitoreo de acceso VPN fuera de horario.
  - Escaneo de puerto de host distribuido.
  - Escaneo de host de red distribuido.
  - Inundación SYN por IDS/Firewall.
  - Alto número de conexiones denegadas para un solo host.
  - Barrido de red saliente/entrante.
  - Fuga de datos.
  - Detección de infección BOTNET en LAN interna.
  - Acceso no autorizado desde redes de terceros o proveedores.
  - Actividades de host infectado.
  - Actividades sospechosas, Adware, Phishing y Hacking.
  - Software no deseado.
  - Monitorización del acceso del equipo de desarrollo a sistemas de producción.
  - Paso de IP en lista negra después de múltiples bloqueos de Firewall.
  - Tráfico saliente a países sospechosos.
  - Tráfico saliente a puerto sospechoso.
  - Tráfico saliente a servicios sospechosos.
  - Tráfico malicioso a activo vulnerable.
  - Comunicaciones a Dominios/IP en lista negra.
  - Transferencia de datos involucrada en Dominios/IP en lista negra.
  - Tráfico saliente que involucra bases de datos.
  - Inyecciones tipo SQLi, XSS, Trasversal, entre otros.
  - Uso de protocolo inseguro: Detección de tráfico inseguro como FTP, telnet, VNC en servidores críticos.
  - Detección de apagado/reinicio de servidores ESX u otros.
  - Detección de inicio/parada/reanudación/reinicio de máquina virtual.
  - Solicitud HTTP diferente a GET, POST, HEAD y OPTIONS.

- Ataque web y sistemas: Escaneo de vulnerabilidad usando Nessus, Openvas, acunetix, Nmap, entre otras herramientas.