DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA INTEGRADO DE MONITORIZACIÓN DE EVENTOS DE SEGURIDAD

Autor: Bogdan Davygora Eduardovych

Área: Administración de redes y sistemas operativos

Enero 2024

RESUMEN

Los imparables avances de Internet de los últimos años han hecho posible que cada vez haya más dispositivos conectados lo que se ha traducido en un enorme incremento de tráfico en la red. Junto a este crecimiento también ha incrementado el número de amenazas cibernéticas a los que se tienen que enfrentar las organización, empresas y particulares. Este trabajo se enfoca en abordar esta problemática a través del diseño e implementación de un Sistema Integrado de Monitorización de Eventos de Seguridad adaptable a entornos industriales, comerciales y domésticos.

La propuesta se distingue por basarse en software libre, permitiendo así su accesibilidad universal sin incurrir en costos adicionales de licenciamiento. La búsqueda de un equilibrio entre capacidad de cómputo y costos de hardware guiará el proceso de desarrollo. El enfoque de este proyecto implica un estudio de herramientas disponibles, la selección de las más idóneas y su integración en un sistema que cubra funciones propias de un SIEM.

La investigación se centrará en herramientas para la supervisión de red y de dispositivos finales. La selección se regirá por criterios de eficiencia y operatividad. Todo el trabajo se llevará a cabo en un entorno virtual simulado con el fin de dar una solución válida para cualquier entorno. Con este enfoque, se busca proporcionar una herramienta efectiva y accesible para la detección oportuna de intrusiones y la respuesta proporcional a las amenazas del ciberespacio.

ABSTRACT

The unstoppable Internet progress in recent years have made it possible for more and more connected devices, resulting in a huge increase in network traffic. Alongside this growth, the number of cyber threats facing organizations, businesses, and individuals has also increased. This project focuses on addressing this issue through the design and implementation of an Integrated Security Event Monitoring System adaptable to industrial, commercial, and domestic environments.

The proposal stands out for its reliance on open-source software, allowing for universal accessibility without incurring additional licensing costs. The search for a balance between computing capability and hardware costs will guide the development process. This project's approach involves a study of available tools, selection of the most suitable ones, and their integration into a system that covers functionalities of a SIEM system.

The research will focus on tools for network and host monitoring. The selection will be based on criteria of efficiency and operability. All work will be carried out in a simulated virtual environment to provide a valid solution for any setting. With this approach, the aim is to deliver an effective and accessible tool for the timely detection of intrusions and a proportional response to cyberspace threats.

Índice general

1 Planificación del trabajo final de grado

1.1 Justificación y motivación del trabajo

La Internet o la red de redes se ha convertido en una parte indispensable de nuestra vida cotidiana. Cada vez más y más personas interactúan y vinculan su vida a esta red global. Todos los aspectos de nuestra vida tales como comercio, negocios, operaciones bancarias y un largo etcétera, dependen en mayor o menor medida de esta red.

Esta creciente digitalización de nuestros entornos, empresarial y doméstico, atrae cada vez un mayor número de delincuentes cibernéticos. En los últimos años esta situación ha elevado el nivel de preocupación de las empresas, organizaciones e incluso usuarios domésticos por la seguridad de su información. Por lo tanto, cada vez se hace más patente la necesidad de una monitorización constante de nuestras redes y sus activos, sea cual sea su tamaño, los servicios a los que se da soporte o las tecnologías que se usen. El fin último de esta monitorización es poder detectar a tiempo las posibles intrusiones y poder reaccionar de manera proporcional.

Por esta razón, este trabajo se va a centrar en el diseño e implementación de un Sistema Integrado de Monitorización de Eventos de Seguridad para cualquier ámbito sea este industrial, comercial o doméstico. Se pretende que la base de este sistema sea el uso de software libre con el fin de poder cubrir las necesidades de cualquier tipo de usuario y entorno sin ningún gasto adicional en lo que a software se refiere. Además, se buscará el equilibrio entre la capacidad de cómputo y los costes en lo que a hardware se refiere.

Para llevar a cabo este trabajo se va a realizar un estudio de las herramientas disponibles, selección de las más idóneas y posterior despliegue e integración de estas con el fin de obtener un sistema que englobe diferentes capacidades propias de un SIEM. Se analizarán soluciones tanto de supervisión de red, NIDS como de supervisión de dispositivos finales como servidores o estaciones de trabajo, HIDS y se escogerán las más equilibradas en lo que a instalación y operación se refiere.

Todo el trabajo se realizará en un entorno virtual simulado debido a las limitaciones físicas de los recursos del estudiante. Este entorno simulado estará basado en una red o parte de una red empresarial con el fin de obtener un producto que se adapte a cualquier tipo de hardware, desde un portátil o PC de sobremesa para monitorizar una pequeña red local hasta un servidor empresarial con capacidad suficiente para monitorizar múltiples segmentos de una red empresarial.

1.2 Objetivos del trabajo

El principal objetivo de este TFG es obtener una solución integral con capacidades de monitorizar una red y los equipos que la componen y detectar las posibles intrusiones que pueda sufrir. Esta tarea lleva asociada una serie de objetivos secundarios que también se pretende alcanzar:

1. Realizar el estudio de las herramientas disponibles en la escena del software libre y elegir las más idóneas para su implementación.
2. Entender los principios de funcionamiento y el proceso de despliegue de las soluciones escogidas.

3. Determinar los requisitos mínimos necesarios para un sistema de monitorización orientado a cubrir las necesidades de monitorización de una red local de un tamaño intermedio.
4. Desplegar el sistema en entorno virtual simulado y documentar el proceso de puesta a punto del sistema final.
5. Realizar pruebas de detección de intrusiones tanto a nivel de red como a nivel de host en un entorno de pruebas para verificar el correcto funcionamiento del sistema desplegado.
6. Crear una guía de despliegue y manejo para los administradores/analistas de sistemas informáticos en red.

1.3 Requisitos

Para el llevar a cabo este proyecto con éxito son necesarios determinados recursos materiales tanto de hardware como de software.

En cuanto al hardware se utilizarán los siguientes dispositivos:

- Portátil Lenovo ThinkPad → será el encargado de alojar las máquinas virtuales que ejecuten diferentes soluciones de software y también se usará como medio para la realización de la parte documental de la memoria y como estación trabajo del analista. El equipo dispone de una CPU Intel Core i7 de 9ª generación, un SSD de 2TB y memoria RAM de 64GB.
- Almacenamiento HDD WD Elements de 4 TB para las copias de seguridad.

En lo a que software se refiere, se utilizaran soluciones tales como:

- Virtual Box 7 como hipervisor en el equipo portátil.
- Sistemas operativos de las familias Windows y Linux.
- Herramientas NIDS, HIDS y otros de diferentes desarrolladores.
- La plataforma draw.io para creación de diagramas de red.
- GanttProject para creación de diagrama de Gantt.

Finalmente, la documentación a usar será la que esté disponible para cada solución/herramienta escogida. Siendo la fuente principal los repositorios web de las herramientas.

También se dispondrá de una conexión a Internet para la descarga y la instalación de todo el software y paquetes necesarios para el desarrollo del proyecto.

1.4 Planificación temporal

Tarea 1: PLANIFICACIÓN DEL TRABAJO

Descripción de la tarea:

Definición de la justificación y objetivos del proyecto. Elaboración de un plan de ejecución del trabajo estableciendo franjas temporales para cada tarea definida.

Objetivos de la tarea:

Obtener una planificación de trabajo segmentada en tarea claramente definidas en tiempo. Creación de un índice de la memoria para facilitar el proceso de documentación del proyecto.

Entrega de la PEC 1.

Tarea 2: DEFINICIONES Y BUSQUEDA DE LAS SOLUCIONES

Descripción de la tarea:

Definición de los conceptos claves en relación a la ciberseguridad. Estudio y comparativa de las soluciones disponibles en el mercado.

Objetivos de la tarea:

Clarificar los términos relacionados con la ciberseguridad que se van a tratar a lo largo del proyecto. Conocer las soluciones y herramientas disponibles en el mercado.

Tarea 3: SELECCIÓN DE LAS SOLUCIONES

Descripción de la tarea:

Selección de las soluciones idóneas y definición de la plataforma que permita integrar todas las soluciones.

Objetivos de la tarea:

Establecer que soluciones se van a implementar y como se van a integrar unas con otras. Definir y escoger la arquitectura del sistema a desplegar.

Tarea 4: ANALISIS DE LAS NECESIDADES Y DEFINICION DE REQUISITOS

Descripción de la tarea:

Definición del entorno de despliegue escogido teniendo en cuenta la arquitectura del sistema a desplegar y usando como referencia la arquitectura de red tipo de una empresa. Establecimiento de requisitos de las máquinas virtuales que van a albergar el sistema.

Objetivos de la tarea:

Obtener el entorno necesario para el despliegue de la solución.

Entrega de la PEC 2.

Tarea 5: DESPLIEGUE DE LAS SOLUCIONES E INTEGRACIONES

Descripción de la tarea:

Instalación de las soluciones escogidas y configuración de las integraciones. Verificación del correcto funcionamiento inicial y monitorización del uso de los recursos de hardware.

Objetivos de la tarea:

Poner a punto el sistema y confirmar que los requisitos escogidos son los idóneos.

Tarea 6: PRUEBAS DEL SISTEMA DESPLEGADO

Descripción de la tarea:

Monitorización de la red en condiciones normales con reglas por defecto. Estudio de alertas generadas. Simulación de intrusiones y estudio de las alertas generadas con reglas definidas por el administrador de seguridad.

Objetivos de la tarea:

Comprobación de la efectividad del sistema desplegado en un escenario simulado.

Entrega de la PEC 3.

Tarea 7: CONCLUSIONES, RETOS FUTUROS Y BIBLIOGRAFIA

Descripción de la tarea:

Recapitulación del trabajo realizado y exposición de las conclusiones sacadas. Planteamiento de futuros retos para la ampliación del sistema diseñado. Recopilar todas las fuentes bibliográficas.

Objetivos de la tarea:

Concluir el proyecto confirmando que se han cumplido los objetivos establecidos y plantear posibles tareas para seguir investigando y ampliando el trabajo de este proyecto. Elaboración de la bibliografía.

Tarea 8: RETOQUES Y PREPARACION DE LA PRESENTACION

Descripción de la tarea:

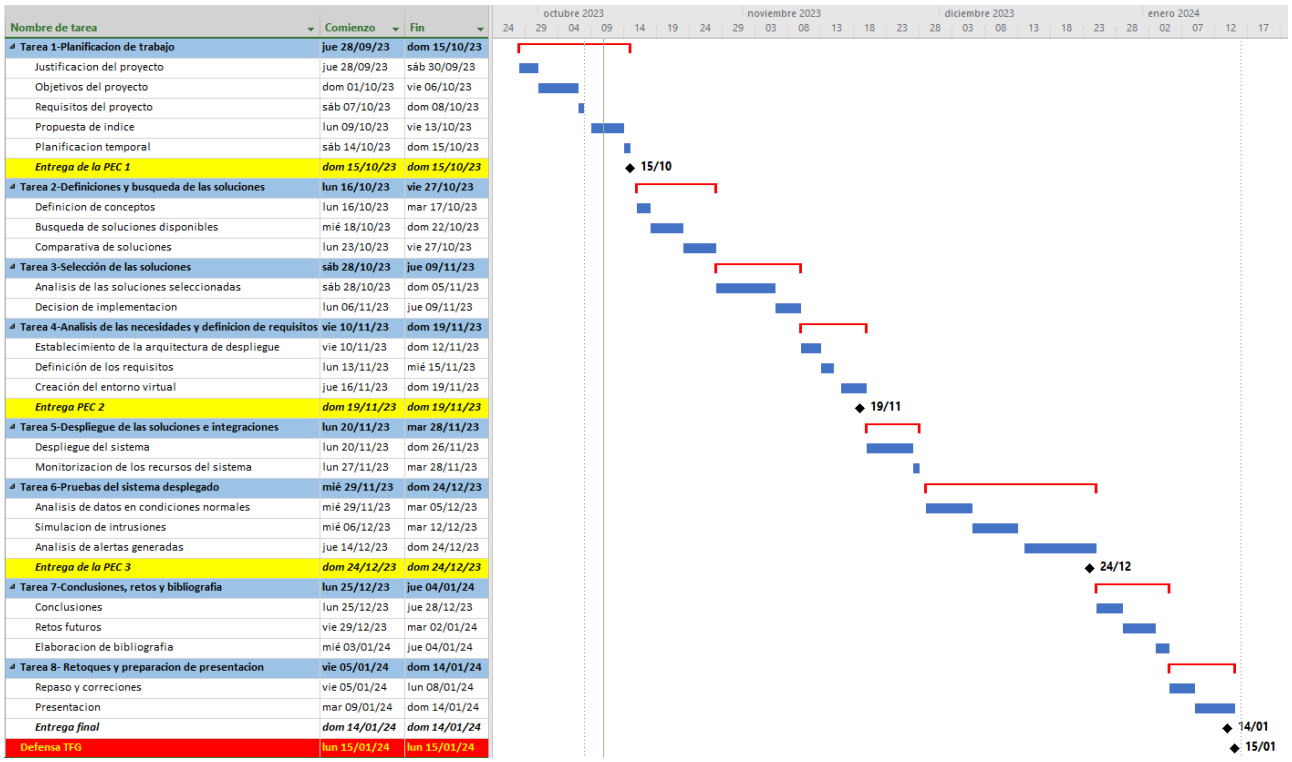
Revisión de todo el trabajo realizado y aplicación de retoques y correcciones. Elaboración de la presentación para la defensa del proyecto ante el tribunal.

Objetivos de la tarea:

Obtener los entregables revisados y corregidos.

Entrega Final.

A continuación, se adjunta el diagrama de Gantt de la planificación anterior que contiene los periodos temporales para cada tarea.



Nombre de tarea	Comienzo	Fin
Tarea 1-Planificacion de trabajo	jue 28/09/23	dom 15/10/23
Justificacion del proyecto	jue 28/09/23	sáb 30/09/23
Objetivos del proyecto	dom 01/10/23	vie 06/10/23
Requisitos del proyecto	sáb 07/10/23	dom 08/10/23
Propuesta de indice	lun 09/10/23	vie 13/10/23
Planificacion temporal	sáb 14/10/23	dom 15/10/23
Entrega de la PEC 1	*dom 15/10/23*	*dom 15/10/23*
Tarea 2-Definiciones y busqueda de las soluciones	lun 16/10/23	vie 27/10/23
Definicion de conceptos	lun 16/10/23	mar 17/10/23
Busqueda de soluciones disponibles	mié 18/10/23	dom 22/10/23
Comparativa de soluciones	lun 23/10/23	vie 27/10/23
Tarea 3-Selección de las soluciones	sáb 28/10/23	jue 09/11/23
Analisis de las soluciones seleccionadas	sáb 28/10/23	dom 05/11/23
Decision de implementacion	lun 06/11/23	jue 09/11/23
Tarea 4-Analisis de las necesidades y definicion de requisitos	vie 10/11/23	dom 19/11/23
Establecimiento de la arquitectura de despliegue	vie 10/11/23	dom 12/11/23
Definición de los requisitos	lun 13/11/23	mié 15/11/23
Creación del entorno virtual	jue 16/11/23	dom 19/11/23
Entrega PEC 2	*dom 19/11/23*	*dom 19/11/23*
Tarea 5-Despliegue de las soluciones e integraciones	lun 20/11/23	mar 28/11/23
Despliegue del sistema	lun 20/11/23	dom 26/11/23
Monitorizacion de los recursos del sistema	lun 27/11/23	mar 28/11/23
Tarea 6-Pruebas del sistema desplegado	mié 29/11/23	dom 24/12/23
Analisis de datos en condiciones normales	mié 29/11/23	mar 05/12/23
Simulacion de intrusiones	mié 06/12/23	mar 12/12/23
Analisis de alertas generadas	jue 14/12/23	dom 24/12/23
Entrega de la PEC 3	*dom 24/12/23*	*dom 24/12/23*
Tarea 7-Conclusiones, retos y bibliografia	lun 25/12/23	jue 04/01/24
Conclusiones	lun 25/12/23	jue 28/12/23
Retos futuros	vie 29/12/23	mar 02/01/24
Elaboracion de bibliografia	mié 03/01/24	jue 04/01/24
Tarea 8- Retoques y preparacion de presentacion	vie 05/01/24	dom 14/01/24
Repaso y correciones	vie 05/01/24	lun 08/01/24
Presentacion	mar 09/01/24	dom 14/01/24
Entrega final	*dom 14/01/24*	*dom 14/01/24*
Defensa TFG	lun 15/01/24	lun 15/01/24

Imagen 1.1: Diagrama de Gantt

1.5 Estado del arte

Hoy en día, los términos SIEM y Ciberseguridad van unidos de la mano en el mundo empresarial. Los Sistemas de Gestión de Información y Eventos de Seguridad permiten a los equipos de seguridad supervisar en tiempo real todo lo que sucede en la red y reaccionar de manera ágil ante posibles amenazas y vulnerabilidades. Además de monitorizar el tráfico externo de la red, los SIEM también se encargan de vigilar el tráfico interno, incluyendo las actividades de los empleados, como las páginas web que visitan y los inicios de sesión. Asimismo, los SIEM son capaces de detectar posibles ataques, como el phishing, para proteger la integridad de la red.

Las soluciones SIEM comerciales disponibles en el mercado son diversas destacando Alienvault USM de AT&T, Splunk o QRadar de IBM. Estas soluciones son de pago y su forma facturar está evolucionando hacia un modelo “paga por EPS”, es decir, el coste va en función del tráfico monitorizado y analizado.

La imparable digitalización de los todos los procesos empresariales hace que el volumen de datos a analizar y proteger aumenta constantemente independientemente de que se trate de una empresa grande o una empresa de pequeño y mediano tamaño (a partir de ahora PYME). Por ello, el gasto para mantener un SIEM es cada vez más grande. Tal y como dice el informe “Security Information & Event Management: Key Trends, Competitor Leaderboard & Market Forecasts” elaborado por Juniper los gastos en ciberseguridad de las empresas, en concreto en los SIEM superaran los 6.400 millones de dólares para 2027. [1]

Esta situación puede ser sostenible para una gran multinacional que dispone de recursos casi ilimitados, pero es frecuente que las PYMEs no puedan abordar el costo de un servicio de monitorización de eventos de seguridad TI. Por esta razón es interesante invertir tiempo y recursos en la investigación, el desarrollo y la implementación de sistemas de monitorización basados en herramientas gratuitas. Y es lo que se pretende llevar a cabo a lo largo de este trabajo de fin de grado.

1.6 Análisis de riesgos

Al tratarse de un trabajo de fin de grado y teniendo en cuenta que la única persona implicada en su elaboración es el alumno, podemos definir dos áreas bien diferenciados de riesgo. Estas áreas son los riesgos derivados de la situación del autor y los riesgos derivados del propio proyecto.

-Riesgos derivados de la situación del autor:

- Experiencia y motivación → si el tema o idea del trabajo escogido excede los conocimientos del autor en la materia podría suponer problemas a la hora de comprender y aplicar los conceptos claves. Además, si el tema escogido no despierta interés o genera compromiso suficiente en el autor podría afectar a la calidad del trabajo.
  - Impacto: Alto.
  - Mitigación: Si existe la posibilidad es recomendable escoger algún tema relacionado con el ámbito profesional y si no buscar un tema que despierte un interés especial en el autor.

- Salud, situación laboral y/o familiar → las enfermedades y los accidentes son inevitables y pueden afectar a las capacidades del autor y provocar retrasos en las entregas. A estos problemas hay que sumar la posibilidad de tener dificultades en ámbito laboral y/o familiar lo que también llevaría a retrasos y desajustes en el desarrollo de las tareas planificadas.
  - Impacto: Muy alto.
  - Mitigación: Este tipo de riesgos son inevitables en la mayoría de los casos por lo que la forma de enfrentarlos seria replanteando ciertas tareas del proyecto o aplazando todo el conjunto hasta un momento más favorable.

-Riesgos derivados del propio proyecto:

- Complejidad técnica → diseño e implementación de un sistema nuevo puede ser técnicamente desafiante. La complejidad técnica del proyecto podría generar retrasos o dificultades en su ejecución.
  - Impacto: Medio
  - Mitigación: Durante la fase de anteproyecto o elaboración de la propuesta del TFG es recomendable hacer un pequeño estudio sobre lo que se pretende hacer y la viabilidad técnica del asunto.

- Requisitos cambiantes → si la planificación de las fases del proyecto no está bien definida desde el principio y los hitos van cambiando constantemente se puede provocar una situación de confusión y retrasos en el desarrollo.

- ♦ Impacto: Medio
- ♦ Mitigación: Para evitar este problema es necesario tener una buena planificación, semanal si es posible, con todos los hitos y fechas claves bien definidas.

- Problemas de integración → al tratarse de un proyecto cuyo objetivo es crear un sistema formado por diversas herramientas que se integren entre sí, puede darse la situación de que no todas las soluciones se puedan integrar como se ha planteado inicialmente. Esto conllevaría pérdidas de tiempo en búsqueda de herramientas alternativas o resolución de errores que surjan.
  - ♦ Impacto: Medio
  - ♦ Mitigación: Dedicar tiempo suficiente al estudio y selección previos de las herramientas que se pretenden utilizar comparando su arquitectura y requisitos.

- Metas demasiado amplias o ambiciosas → la intención de abarcar todas las posibles áreas relacionadas con el proyecto e intentar profundizar en todas puede conllevar a excesos en los tiempos planificados y descuido de otros aspectos no menos importantes.
  - ♦ Impacto: Bajo
  - ♦ Mitigación: Repartir la carga de trabajo por prioridades, dando mayor importancia a los puntos clave y dejar los puntos secundarios para el final y en caso de no poder abarcarlos poder citarlos como retos futuros.

1.7 Implicaciones éticas y legales

En nuestro caso al tratarse de un trabajo cuyo desarrollo e implementación se va a realizar en un entorno de laboratorio las **implicaciones legales** son mínimas y estarán relacionadas con las licencias de software, ya que aun siendo libre tiene su propia regulación.

En el caso de implantación del sistema resultado de este proyecto en un entorno empresarial sería necesario tener en cuenta también el cumplimiento de RGPD y LOPDGDD.

En cuanto a las **implicaciones éticas** en un entorno empresarial hay que tener en cuenta los siguientes aspectos:

- Privacidad de los empleados → la monitorización de eventos de seguridad implica la recopilación y análisis de datos relacionados con el comportamiento de los empleados por lo que hay que definir políticas y límites de las acciones de monitorización.
- Consentimiento y notificación → los empleados deben comprender cómo se recopilan y utilizan sus datos y cuáles son los propósitos legítimos para la monitorización y por ello deben ser informados correctamente por el órgano responsable.
- Transparencia y responsabilidad → las empresas deben ser transparentes en cuanto a sus prácticas de monitorización y asumir la responsabilidad de proteger la privacidad de los empleados. Esto incluye la adopción de medidas para prevenir el acceso no autorizado a los datos recopilados.

En el entorno de laboratorio como el utilizado durante el desarrollo de este proyecto las implicaciones éticas son inexistentes ya que no afectan a terceros.

1.8 Estudio económico

En este apartado se pretende realizar un pequeño análisis de ventajas y desventajas que puede suponer el uso de soluciones de software libre para despliegue de un SIEM.

-Ventajas:

Un aspecto muy importante para una empresa a la hora de implementar un sistema es su coste inicial. Las soluciones de software libre ofrecen la ventaja de que este coste inicial sea muy reducido o incluso nulo. Esto se debe a que los únicos costes suelen ser derivados del hardware que va a ejecutar las soluciones escogidas. A veces puede darse la situación en la que se pueden aprovechar los recursos de hardware existentes en la empresa por lo que la inversión inicial queda reducida a cero.

Otro aspecto a tener en cuenta a la hora de usar soluciones de software libre es su soporte. En este caso, las herramientas de esta índole suelen contar con una amplia comunidad de personas que hacen uso de las mismas y se encargan de su soporte y mantenimiento. Este soporte se suele materializar mediante wikis, foros y comunidades en línea, reduciendo así los gastos derivados de servicios de soporte de pago.

La flexibilidad y la escalabilidad no limitadas por las restricciones de las licencias también son una ventaja que ofrecen los sistemas basados en software libre. Gracias a ello una empresa puede afrontar el crecimiento de su infraestructura y sus necesidades de seguridad sin enfrentar restricciones impuestas por licencias o costos adicionales.

-Desventajas:

Un aspecto negativo al optar por soluciones de software libre puede ser la necesidad de disponer de una plantilla de personal más experto para la implementación y la administración de los sistemas. Cuando se trata de soluciones comerciales, suelen ser herramientas muy automatizadas y en las que las tareas de despliegue y administración del sistema recaen sobre la empresa que ofrece el producto dejando al personal analista de la empresa cliente más centrado en los aspectos de vigilancia y monitorización.

Soporte técnico es un aspecto que ofrece la ventaja en lo que a costes se refiere si se trata de software libre. Sin embargo, puede ser un desafío, al depender las organizaciones de foros y comunidades en línea para resolver problemas. Esta dependencia y ausencia de soporte personalizado puede traducirse en tiempos de respuesta más largos.

La garantía de continuidad de las soluciones escogidas también es un aspecto importante. Las soluciones comerciales suelen tener un tiempo de vida garantizado con actualizaciones y mejoras periódicas. Las soluciones de software libre populares también suelen ofrecer una continuidad en el tiempo, pero no ofrecen ninguna garantía respecto al tiempo que seguirán recibiendo soporte.

La elección entre las herramientas gratuitas o comerciales pasa por la búsqueda de un equilibrio entre la inversión inicial y los desafíos que puede suponer su implantación en producción. Las organizaciones tienen que tener en consideración las capacidades de sus

plantillas, el crecimiento previsto de sus infraestructuras y las necesidades operativas de los sistemas de seguridad.

En última instancia, la elección entre software libre y comercial dependerá de los objetivos y la infraestructura específicos de cada organización, siendo las soluciones de software libre más interesantes para las PYMEs en un momento inicial, pudiendo migrar en caso de necesidad hacia soluciones comerciales siempre y cuando sea viable a nivel económico.

2 Definiciones y conceptos

2.1 Ciberseguridad

Cada día el número de dispositivos conectados a la red aumenta exponencialmente con lo que cada vez mayor número de estos dispositivos queda expuesto a los ataques por parte de agentes externos que su vez cada vez son más creativos e ingeniosos. Por ello el termino de ciberseguridad o seguridad del ciber-espacio resulta más actual que nunca.

Según Cisco la ciberseguridad se puede definir como el conjunto de acciones encaminadas a proteger sistemas, redes y aplicaciones de los ataques cibernéticos. Esta ciberseguridad se basa en la implementación de múltiples capas de prevención y protección que se traducen en **detección**, **investigación** y corrección. [2]

También podemos definir la ciberseguridad como un conjunto de medidas encaminadas a garantizar la disponibilidad, confidencialidad e integridad de la información y los medios de acceso a la misma. [3] Donde:

- Disponibilidad es la propiedad que garantiza que la información este accesible cuando sea necesario.
- Confidencialidad es la propiedad que asegura que la información solo sea accesible para el personal autorizado.
- Integridad es la propiedad que garantiza que la información no ha sido alterado ni modificada por un agente no autorizado.

En nuestro caso, en este TFG vamos a diseñar un sistema de monitorización basado en **detección** e **investigación** de las amenazas para asegurar los 3 pilares básicos que hemos definido anteriormente.

2.2 Software libre

La idea de este proyecto consiste en obtener un sistema que integre soluciones de software libre y gratuito con el fin de hacerlo accesible a todo tipo de entidades, particulares u organizaciones. Por ello es muy relevante conocer que tipos de software existen, sus licencias y limitaciones que puede haber según un tipo u otro. De esta manera se evitarán los posibles problemas derivados en lo que al uso se refiere.

Software propietario [4] es aquel que tiene un dueño legal con la potestad de limitar o prohibir la copia, redistribución y modificación no autorizada o si no se ha efectuado el abono de las tasas que habiliten para ello.

Software libre [4] es aquel que no tiene derechos de autor (copyright), es decir, el usuario puede usarlo, copiarlo, modificarlo y distribuirlo libremente. Este software puede ser gratuito o no según la decisión de su creador. Dentro del software libre se define diversos tipos o licencias [5]:

- Licencias de dominio público → son las licencias más abiertas ya que no imponen restricción alguna de uso. De esta manera los usuarios pueden crear sus soluciones comerciales o no sin tener que compensar económicamente al autor del código base.

- Licencias Non-Copyleft → son conocidas como licencias permisivas ya que ofrecen a los usuarios requisitos mínimos para poder usar, copiar, modificar o redistribuir el código. Son similares a las licencias de dominio público, pero con ciertas condiciones que sirven para proteger la propiedad intelectual.
- Licencias LPGL (Lesser General Public License) → son las que permiten a sus usuarios enlazar sus trabajos con bibliotecas de código abierto y a pesar de ello poder aplicar al producto final cualquier licencia que deseen incluso propietaria.
- Licencias Copyleft o GPL (General Public License) → son licencia conocidas como reciprocas o restrictivas. Esta reciprocidad o restricción consiste en que los usuarios que usen o modifiquen el código o el programa original deben publicar el resultado bajo la misma licencia inicial.

2.3 Partes de una red informática

Dado que el objetivo de este trabajo es diseño e implementación de un sistema de supervisión de red informática es de vital importancia conocer todos los dispositivos que pueden llegar a formar parte de esta red.

- Dispositivos finales (hosts) [6] → son los dispositivos que hacen de interfaz entre los usuarios y la red informática. Se limitan a solicitar u ofrecer servicios en la red. Pueden ser ordenadores, teléfonos IP, dispositivos móviles, impresoras, cámaras, etc.
- Electrónica de red → son los dispositivos intermedios que proporcionan la conectividad y el enrutamiento de la información en las diferentes partes de una red. Los dispositivos más empleados son:
    - Conmutador (switch) [7] → es un dispositivo de interconexión que sirve para conectar todos los equipos dentro de una red local. Se encarga de dirigir el tráfico de red local de un dispositivo de red a otro.
    - Enrutador (router) [8] → es un dispositivo de interconexión que sirve para conectar entre si diferentes redes y además sirve para conectar estas redes a Internet. Se encarga enrutar el tráfico de una red a otra mediante el uso de protocolos de enrutamiento.
    - Cortafuegos (firewall) [9] → es un dispositivo que controla el tráfico entrante y saliente de una red privada con la finalidad de bloquear la entrada de datos que no cumplan con algunos criterios de seguridad.
    - Punto de acceso inalámbrico (WAP) [10] → es un dispositivo de red que interconecta equipos de comunicación inalámbricos. Son el equivalente a un switch, pero para conexiones inalámbricas.
- Servidores [11] → es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red. En teoría, se consideran servidores aquellos ordenadores que comparten recursos con máquinas cliente. Existen muchos tipos de servidores, como los servidores web, los servidores de correo y los servidores virtuales.
- Medios de transmisión → son los encargados de proporcionar un canal físico para que los datos viajen entre los distintos dispositivos que componen la red. Los medios empleados comúnmente son cables de cobre, fibra óptica y ondas electromagnéticas.

Todos estos dispositivos, exceptuando los medios de transmisión, serán los que alimenten nuestro sistema de monitorización con información importante para detectar cualquier tipo de anomalía en la red.

2.4 Ataques y técnicas de intrusión

Un ataque [12] o ataque informático es un intento planificado de explotar alguna debilidad de un sistema con el fin de conseguir acceso no autorizado a los sistemas, información u otros medios de una organización o entidad y comprometer alguno o todos los pilares de la seguridad. Esto ataques pueden ser motivados por beneficios económicos o llevarse acabó únicamente con el fin de alterar el correcto funcionamiento del sistema. Los ataques pueden ser perpetrados por ciberdelincuentes que no pertenecen a organización alguna, grupos organizados o incluso por gobiernos.

Los ataques informáticos pueden ser pasivos o activos. Los primeros tienen como objetivo únicamente acceder al sistema y recopilar información de forma no autorizada. Sin embargo, los ataques activos a parte de acceder al sistema buscan alterar su funcionamiento o la información que alberga.

Los ataques pasivos resultan difíciles de detectar, por lo que hay trabajar en políticas de prevención de los mismos. En cambio, los ataques activos sí que se pueden detectar y por ello serán el objetivo de detección de nuestro sistema de monitorización.

Entre los ataques más empleados actualmente se pueden clasifican en [13]:

- Ataques de reconocimiento → este tipo de ataques consisten en levantamiento de activos de una red informática. En otras palabras, lo que se busca es mapear todos los dispositivos de la red y los servicios a los que da soporte. Entre estos ataques están:
    - Escaneo de direcciones IP (Ping Sweep) → consiste en realización de consultas ICMP para ver que equipos de la red están activos.
    - Escaneo de puertos (Port Scan) → consiste en realización de peticiones hacia diferentes puertos para conocer cuales están a la escucha.
    - Captura de trafico de red (Packet Capture & Sniffing) → captura de trafico de red para su posterior análisis y obtención de información en caso de que no esté cifrado.
    - Ingeniería social y OSINT → obtención de la información mediante engaño de usuarios o mediante la investigación de fuentes información públicas como redes sociales.

- Ataques de acceso → este tipo de ataques consiste en la obtención de acceso al sistema por medio de engaño o por fuerza. Entre estos ataques están:

    - Ruptura de contraseñas (Password Cracking) → sirve para obtener las contraseñas por el método de prueba y error usando diccionarios o listas de palabras definidas en basa a inteligencia obtenida durante el reconocimiento.
    - Suplantación→ (Spoofing) → consiste en suplantar la identidad de usuario legitimo para acceder a un dispositivo con confianza o permisos dentro del sistema para posteriormente escalar privilegios.

    - Redirección o pivotaje (Port Redirection) → se basa en la explotación de la confianza entre dispositivos de una misma red. Lo que se busca es atacar a un dispositivo no accesible a través de otro que sí que es accesible al atacante.

- Ataques de denegación de servicio → tienen como objetivo alterar la disponibilidad de los sistemas colapsándolos o bloqueando el acceso de los mismo. Los ataques más conocidos se conocen como DDoS y se llevan a cabo mediante el uso de redes de dispositivos infectados que inundan el sistema objetivo con peticiones hasta llegar a colapsarlo.

2.5 Sistemas de monitorización

El problema a la hora de proteger un sistema informático reside en la necesidad de abarcar todos los elementos que lo componen. Como en cualquier sistema de seguridad sea informático, físico o de otra índole, cuanto mayor es la superficie a proteger frente a un ataque mayor es la dificultad de implantar las medidas para evitar los ataques [14]. La manera más eficiente de implantar estas medidas es hacerlo por capas:

- Capa de la red
- Capa del dispositivo
- Capa de los datos
- Capa de la aplicación

Para poder atender la defensa de todas estas capas se requiere de un sistema que sea capaz de detectar las amenazas de forma eficiente emitiendo alertas de manera estratégica, para lograr una respuesta temprana y recopilar toda la información posible sobre el agresor.

Este sistema se denomina en el campo de ciberseguridad como sistema de monitorización y se materializa como un conjunto de herramientas combinadas que recopilan y analizan diferentes fuentes de información para dar una imagen completa de un posible incidente.

2.5.1 SIEM

SIEM es una de las soluciones del campo de ciberseguridad que más se acerca a la definición anterior. Es un sistema de seguridad que permite a las organizaciones a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir las operaciones. Muestra anomalías en el comportamiento del usuario y utiliza diferentes técnicas y mecanismos para automatizar muchos de los procesos manuales asociados con la detección de amenazas y la respuesta de incidentes. Se ha convertido en un elemento básico en los centros de operaciones de ciberseguridad (COCS) modernos para casos de uso de gestión de seguridad y conformidad. [15]

Este sistema resulta de la combinación y evolución de dos tecnologías [16]:

- Security Information Management (SIM) o Gestión de Información de Seguridad que se encarga de monitorización en tiempo real, correlación de eventos, notificaciones y visualización grafica de la información de seguridad.
- Security Event Management (SEM) o Gestión de Eventos de Seguridad que se encarga del almacenamiento a largo plazo, el análisis y la comunicación de los datos de seguridad.

Las funciones básicas [14] que debe ofrecer una solución SIEM son:

- Gestión de registros → consiste en la captura de datos procedentes de todos los dispositivos que componen la red. Estos registros de aplicaciones, dispositivos y red se recopilan, almacenan y analizan en tiempo real. Esta capacidad permite administrar los flujos de datos de la red de manera centralizada y automatizada.
- Correlación de eventos y análisis → es una capacidad vital de un sistema de monitorización ya que permite identificar y comprender los patrones que sigue los datos complejos y correlacionar diferentes sucesos para poder detectar las amenazas. Permite reducir los tiempos de detección y respuesta a los analistas de ciberseguridad.
- Monitoreo de incidentes y alertas de seguridad → gracias a la automatización y centralización de los procesos de detección es posible obtener una monitorización completa de todas las entidades y generación de alarmas precisas para avisar a los administradores de seguridad de los sistemas con el fin de mitigar los problemas cuanto antes.
- Integración con fuentes de inteligencia de amenazas → es muy importante tener la capacidad de poder enriquecer el sistema de monitorización con firmas y patrones de amenazas emergentes que se pueden obtener a partir de diferentes APIs.

2.5.2 NIDS

NIDS es una herramienta que se instala en uno o varios puntos de la red para la captura y el análisis de tráfico. Estas soluciones suelen combinar métodos de detección basados en firmas y anomalías. [17]

- La detección basada en firmas implica comparar las características de los paquetes de datos recopilados con archivos de firmas que se sabe que son maliciosos.
- La detección basada en anomalías utiliza análisis de comportamiento para monitorear eventos en comparación con una línea de base de actividad de red "típica".

Cuando surge una actividad maliciosa o anómala en una red, como un aumento repentino en el tráfico de la red, esta herramienta detecta la actividad y genera alertas para su investigación.

Resulta de vital importancia la colocación estratégica de los sensores que capturan el tráfico de red, centrando los esfuerzos en los segmentos de la red más expuestos como la DMZ.

A veces estos sistemas pueden llegar a tomar medidas protectoras para corregir las brechas de seguridad. En este caso estaríamos hablando de IPS que no son objeto de estudio de este trabajo.

2.5.3 HIDS

HIDS es una herramienta que se instala en los dispositivos (equipos de usuarios o servidores) que se conectan a la red. Se encargan de recopilación y análisis de datos procedentes únicamente del equipo en el que se encuentra instalado el agente HIDS. [18]

Los datos que se analizan principalmente suelen ser los registros de autenticación, que registran eventos de inicio de sesión. Sin embargo, un agente normalmente también analiza otros tipos de datos, como registros de aplicaciones y sistemas operativos. Aunque estos últimos tipos de datos no están relacionados específicamente con la seguridad, los patrones inusuales dentro de esos conjuntos de datos podrían estar relacionados con problemas de seguridad.

Existen dos tipos de HIDS:

- Basados en agentes → en este caso se puede obtener mayor cantidad de información del equipo, pero se requiere una cierta capacidad de cómputo de este.
- Sin agentes → su funcionamiento se resume en envío de ciertos datos por parte del equipo al servidor de gestión de HIDS. La cantidad de información obtenidas es inferior pero no requiere de un esfuerzo extra por parte del equipo afectado.

Al igual que las herramientas NIDS hay soluciones HIDS que tiene cierta capacidad para dar respuesta a las anomalías que detecten.

3 Herramientas y soluciones disponibles

Una vez definidos los conceptos clave y las herramientas involucradas vamos a proceder al análisis de las herramientas disponibles en el mercado que puedan satisfacer las necesidades de este trabajo.

3.1 SIEM

Tal y como se ha mencionado en el estado del arte, el mercado actual está repleto de soluciones SIEM comerciales. Muchas de estas soluciones comenzaron siendo proyectos gratuitos que con el paso de tiempo se han convertido en los titanes de la industria y por ello no son objeto de este estudio.

El mercado de las soluciones gratuitas o con licencias permisivas no es tan amplio como nos gustaría, pero aun así hay productos que son de interés para este trabajo.

AlienVault OSSIM (Open Source Security Information Management) es un sistema de monitorización y correlación de eventos de seguridad gratuito y basado en código abierto. Su base es el uso de herramientas bajo licencia GPL entre las cuales tenemos unas que están orientadas al análisis de hosts y electrónica de red y otras orientadas al análisis de trafico de la red. El mercado al que está orientado este sistema son las PYMEs y entusiastas de ciberseguridad que quieran monitorizar su red doméstica. [19]

OSSIM se compone de los siguientes módulos:

- Descubrimiento de activos
- Evaluación de vulnerabilidad
- Detección de intrusos
- Monitoreo de comportamiento
- Correlación de eventos
- Cumplimiento normativo → PCI-DSS e ISO/IEC 27001

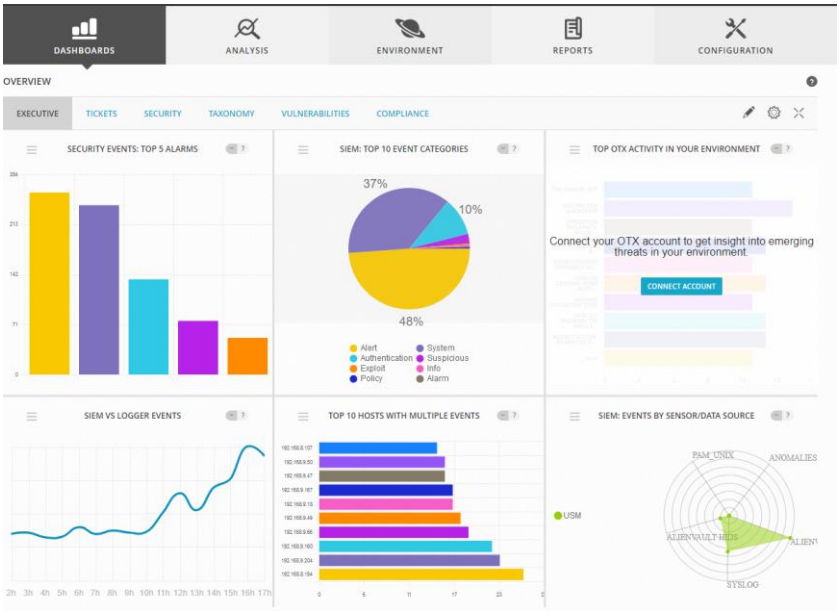


Imagen 3.1: OSSIM Dashboard [19]

Y las herramientas que en engloba en su núcleo son: [20]

- PRADS → se emplea para identificar hosts y servicio de red mediante la monitorización pasiva de la red.
- Snort → es utilizado como sistema de detección de intrusiones (IDS) que además realiza correlación cruzada con OpenVAS.
- Suricata → es utilizado como un sistema de detección de intrusiones alternativo.
- Tcptrack → utilizado para conocer la información de las sesiones, lo cual puede conceder información útil relativa a los ataques.
- Munin → se emplea para análisis de tráfico y servicios.
- NFSen/NFDump → se utiliza para captura y análisis de información del NetFlow.
- FProbe → es utiliza para generar NetFlow a partir de tráfico capturado en bruto.
- Nagios →se utiliza como monitor de host y puertos que tengas a la escucha.
- OpenVas → se utiliza como analizador de vulnerabilidades de host.
- OSSEC → es un sistema de detección de intrusos basado en hosts

Wazuh SIEM es una plataforma de seguridad gratuita y de código abierto que unifica las capacidades de XDR y SIEM. Se trata de una plataforma centralizada para agregar y analizar telemetría en tiempo real para la detección de amenazas y el cumplimiento. Wazuh recopila datos de eventos de diversas fuentes, como puntos finales, dispositivos de red, cargas de trabajo en la nube y aplicaciones para una cobertura de seguridad más amplia. [21]

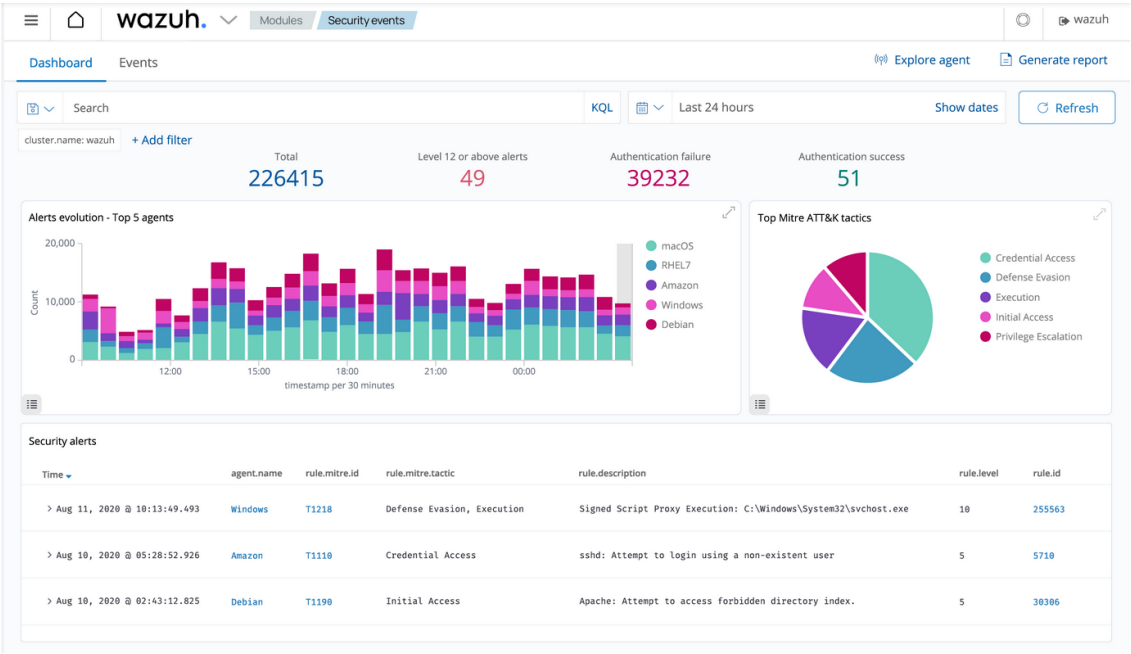


Imagen 3.2: Wazuh Dashboard [21]

Cuenta con las siguientes capacidades: [22]

- Análisis de logs de seguridad → es un proceso crucial que implica examinar y extraer información valiosa de archivos de registro creados por diferentes sistemas, aplicaciones o dispositivos. Wazuh es capaz de recopilar logs de diversos sistemas operativos tales como Linux, Windows y macOS pudiendo trabajar con syslog, auditd, registros de aplicaciones y otros desde puntos finales.

- Detección de vulnerabilidades → este módulo se encarga de descubrir vulnerabilidades en el sistema operativo y las aplicaciones instaladas en los puntos finales monitoreados. El módulo funciona utilizando la integración nativa de Wazuh con fuentes de vulnerabilidades externas indexadas por Canonical, Debian, Red Hat, Arch Linux, Amazon Linux Advisories Security, Microsoft y la base de datos nacional de vulnerabilidades.
- Respuesta a incidentes → esta capacidad se ofrece mediante el módulo Wazuh Active Response que logra una respuesta automatizada a incidentes Estas acciones pueden incluir aislar puntos finales comprometidos, bloquear direcciones IP maliciosas, poner en cuarentena dispositivos infectados o deshabilitar cuentas de usuarios comprometidas.
- Monitoreo de integridad archivos → este módulo se conoce como FIM y lleva a cabo el control de cambios en archivos y directorios y activa una alerta cuando un usuario o proceso crea, modifica y elimina archivos monitoreados. Ejecuta un escaneo de referencia, almacenando la suma de verificación criptográfica y otros atributos de los archivos monitoreados.
- Evaluación de la configuración de seguridad → este módulo permite identificar configuraciones erróneas y fallas de seguridad en la infraestructura. Cada agente Wazuh escanea el sistema final y compara los resultados con los benchmark de referencia de CIS. De esta manera consigue identificar y remediar vulnerabilidades, configuraciones incorrectas o desviaciones en las mejores prácticas y estándares de seguridad.
- Cumplimiento normativo → esta capacidad sirve para implementar requisitos de cumplimiento para el soporte y la visibilidad del cumplimiento normativo. El conjunto de reglas predeterminado de Wazuh brinda soporte para los marcos y estándares PCI DSS, HIPAA, NIST 800-53 y RGPD.

Gracias a estas capacidades el sistema Wazuh es capaz de correlar eventos de múltiples fuentes e integrarlos con fuentes de inteligencia sobre amenazas para poder generar alarmas y notificaciones en tiempo real.

SELKS de Stamus Networks es un sistema que engloba las capacidades de monitorización de seguridad de la red con las capacidades de sistemas de detección de intrusos y protección frente a estos. El corazón de este sistema es Suricata que es una solución IDS/IPS gratuita.

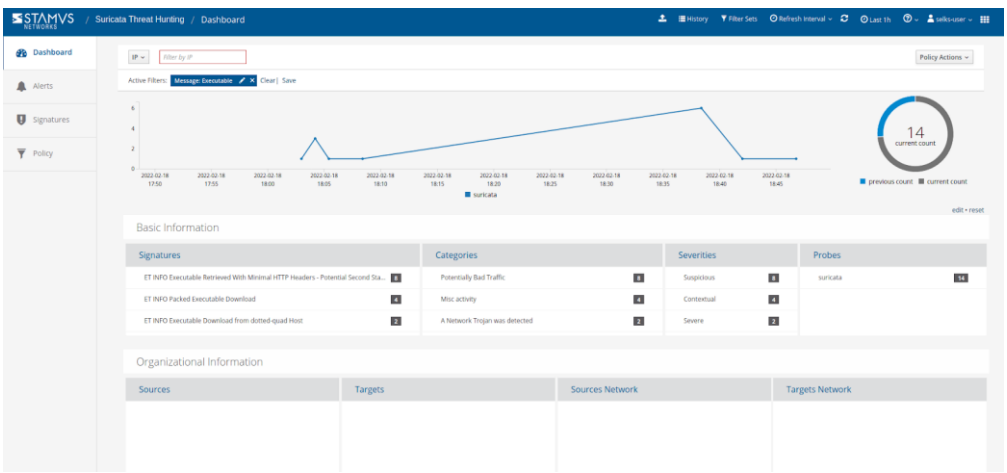


Imagen 3.3: SELKS Dashboard [23]

Para poder cumplir sus funciones basa su arquitectura en los siguientes componentes principales: [24]

- Suricata → que actúa como el sistema de detección de intrusiones y protección.
- Elasticsearch → actúa como la base de datos y motor de búsquedas de registros generados por suricata.
- Logstash → se encarga de inyectar los eventos de suricata con formato adecuado al Eslasticsearch.
- Kibana → se encarga de ofrecer la visualización del contenido de Elasticsearch. Además, permite creación de paneles personalizados para mejorar la exploración de eventos y registros.
- Arkime → se encarga de la captura de paquete y su almacenamiento en forma de PCAPs.

Además, SELKS cuenta con EveBox y CyberChef. El primero es una herramienta de gestión de eventos y alertas de Suricata y el segundo es una herramienta para cifrado, codificación, compresión y análisis de datos.

Security Onion (SO) es una distribución basada en Linux que ofrece una plataforma abierta y gratuita para la caza de amenazas, monitorización de seguridad tanto de red como de hosts y gestión de logs y eventos.

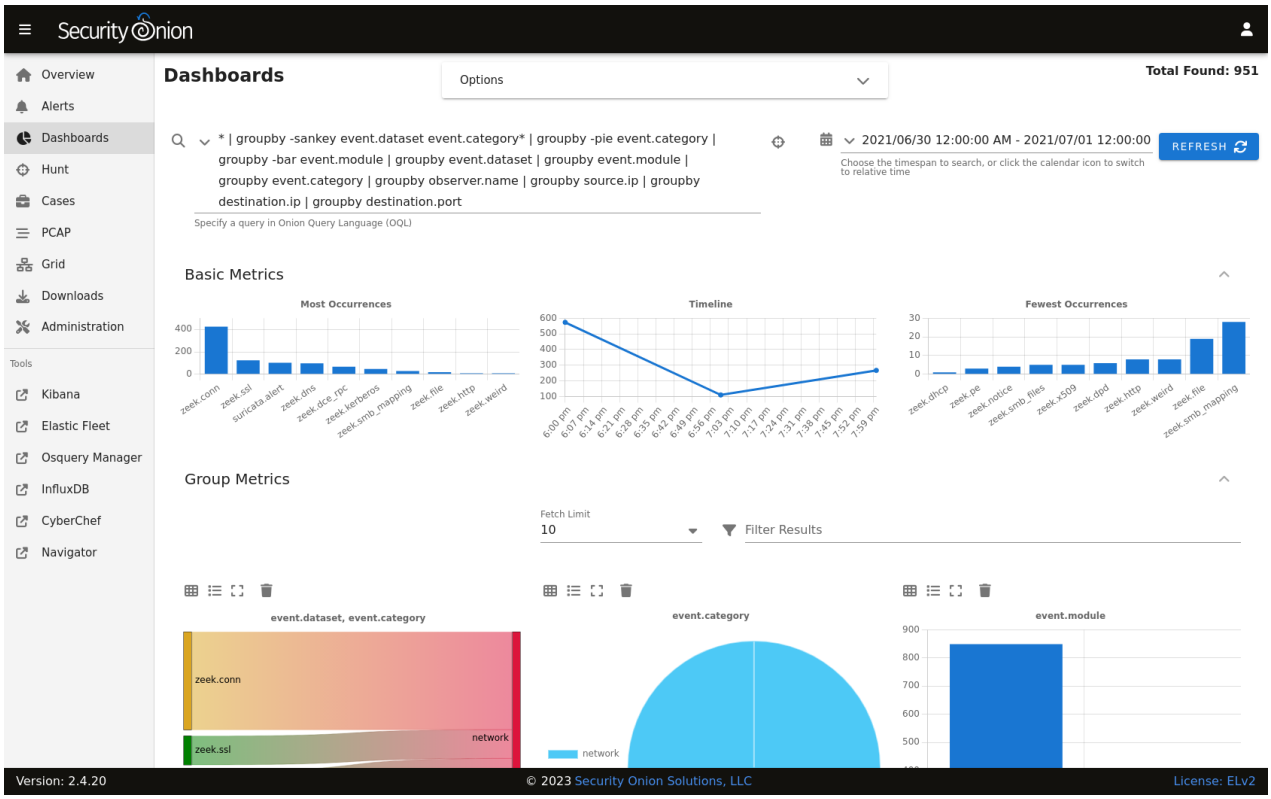


Imagen 3.4: SOC Dashboard

Entre sus capacidades se encuentran:

- Visibilidad de la red → se lleva a cabo mediante la detección basada en firmas a través de Suricata, metadatos de protocolos de enriquecidos y extracciones de archivos realizadas por Zeek. Este proceso se ve apoyado por captura de paquetes con Stenographer y análisis de archivos con Strelka.

- Visibilidad del host → se lleva a cabo mediante el despliegue de agentes en dispositivos finales, en este caso se trata de Elastic Agent. Los agentes son gestionados mediante servidor de Elastic Fleet y permiten la recopilación de datos y consultas en vivo gracias al módulo de Osquery.
- Visibilidad del sistema → consiste en monitorización de los recursos del propio sistema. Esta tarea se lleva a cabo con ayuda de Grafana.
- Honeypots de detección de intrusiones → existe la posibilidad de crear honeypots de detección de intrusiones basados en OpenCanary.
- Gestión de registros → toda la gestión, manejo y visualización de eventos se puede realizar mediante interfaces propias del SO o mediante Kibana de Elastic.
- Búsqueda activa (o caza) de amenazas e investigación → para esta tarea a parte de las herramientas anteriores se dispone de Cyberchef, Navigator y Playbooks. De esta manera se pueden abrir caso de investigación de intrusiones y seguir patrones de ataques con el fin de evitar brechas futuras.

Todas estas herramientas de análisis trabajan juntas para proporcionar capacidades de análisis eficientes e integrales. [26]

3.2 NIDS

En el apartado anterior hemos visto que las soluciones SIEM gratuitas usan como base múltiples herramientas NIDS también gratuitas. Por ello vamos a hacer un estudio de las capacidades de algunas de estas herramientas para poder tener una imagen más clara a la hora de tomar la decisión final de implementación.

Suricata de OISF, su desarrollador, es una herramienta multiplataforma basada en código libre cuya función principal es actuar como IDS/IPS en red. [27]

Como podemos ver esta herramienta la comparten soluciones tales como OSSIM, SELKS y Security Onion por lo que su efectividad esta más que demostrada.

Su funcionamiento se basa en recogida de trafico de la red con la posterior comparación del mismo contra una serie de reglas y firmas para poder detectar amenazas. Una vez la amenaza es detectada Suricata ofrece la posibilidad de aplicar respuesta para paliar la misma.

Una de sus características estrella es la capacidad de ejecución multihilo pudiendo ejecutar varias etapas de la detección simultáneamente y dar mayor prioridad a unas etapas frente a otras. Esta característica también ofrece una mayor escalabilidad al sistema en entornos que tienden a hacerse más grandes.

Las etapas en las que se divide el proceso de detección son las siguientes: [28]

- Adquisición de paquetes → adquiere paquetes de la red.
- Seguimiento de flujo y decodificación de la capa de aplicación → decodifica los datos, maneja el reensamblaje de TCP, etc.
- Detección → compara los datos decodificados con las reglas.
- Salida → se ocupa del registro y las alertas

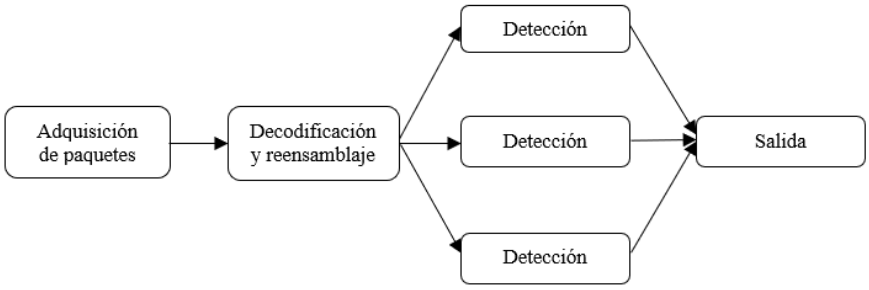


Imagen 3.5: Pipeline Suricata

El output o salida final se guarda en el formato .yaml lo que permite que estos datos sean tratados por otras herramientas como Logstash de Elastic.

Los logs de funcionamiento y ejecución se guardan en el formato .log pudiendo ser fácilmente analizados por el administrador para detectar cualquier anomalía.

Entre otras características de Suricata podemos encontrar la detección automática de protocolo que permite detectar el protocolo que circula por la red independientemente del puerto que se esté utilizando.

En lo que a reglas se refiere puede trabajar tanto con reglas de Snort como con sus propias reglas o incluso con reglas personalizadas y escritas desde cero por el analista de seguridad.

SNORT es un potente NIDS e IPS de código abierto que proporciona análisis del tráfico de red en tiempo real y registro de paquetes de datos. SNORT utiliza un lenguaje basado en reglas que combina métodos de inspección de anomalías, protocolos y firmas para detectar actividades potencialmente maliciosas. [29]

Su funcionamiento es similar al de Suricata, pero con la diferencia de que Snort no soporta multihilo por lo que resulta menos eficiente para redes grandes o que escalan constantemente. Las etapas en las que se divide el funcionamiento son:

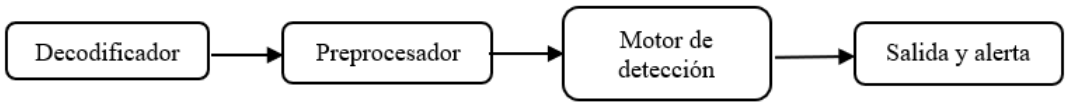


Imagen 3.6: Pipeline Snort

- El paquete recibido por Snort desde la red pasa por decodificador que es el módulo que se encarga de almacenar toda la información del paquete en una base de datos para su posterior análisis.
- Seguidamente el paquete pasa por preprocesador donde se analiza o incluso puede ser modificado según el tipo de preprocesador. En esta tapa los paquetes se clasifican, unos se descartan y otros pasan a la fase de detección.
- Una vez en el motor de detección, la información del paquete tratada en las etapas anteriores es comparada con las reglas de detección y patrones con el fin de detectar si tiene o no anomalías.

- En la última fase, el paquete que resulta sospechoso genera una alerta y esta es mostrada al administrador. Además, en función de la alerta pueden tomarse acciones de prevención.

Entre sus funciones destacan las siguientes:

- Monitor de tráfico en tiempo real → monitoriza el tráfico en tiempo real y emite alertas a los usuarios cuando descubre paquetes o amenazas potencialmente maliciosos en las redes.
- Registro de paquetes → recopila cada paquete y lo registra en un directorio jerárquico basado en la dirección IP de la red host.
- Análisis de protocolo → rastrea la red con el fin de capturar datos en capas de protocolo para análisis adicional.
- Coincidencia de contenido → las reglas se agrupan por protocolo, por puertos, por paquetes con contenido y finalmente por paquetes sin contenido. Los paquetes que sí tienen contenido se pasan a un comparador de múltiples patrones que aumenta el rendimiento, especialmente cuando se trata de protocolos como HTTP. A pesar de afectar negativamente al rendimiento los paquetes sin contenido también se analizan.
- Detección del sistema operativo → se basa en el concepto de que todas las plataformas tienen una pila TCP/IP única. De esta forma es posible detectar el sistema operativo origen del paquete.

Al tratarse de una solución polivalente, Snort dispone de 3 modos de trabajo: [30]

- Analizador de paquetes → se rastrean y se muestran por pantalla todos los paquetes IP presentes en la red.
- Registrador de paquetes → toda la actividad de los paquetes IP queda registrada para que luego el administrador de la red pueda ver quién visitó su red y obtener información sobre el sistema operativo y los protocolos que estaban utilizando.
- NIPDS (Sistema de Detección y Prevención de Intrusiones en la Red) → en este caso solo se registran los paquetes que se consideran maliciosos. Este proceso se lleva a cabo en base al uso de las reglas preestablecidas y las creadas por el administrador. Es el modo más eficiente del funcionamiento.

Zeek es una herramienta de código abierto cuyo principal objetivo es el análisis pasivo del tráfico de red. Zeek también es aplicable para el análisis de tráfico más allá del ámbito de la seguridad permitiendo métricas de rendimientos y resolución de problemas de red. [31]

Zeek ofrece un amplio conjunto de logs sobre la actividad de red entre los que se encuentran logs de las sesiones completas de HTTP con los URIs, cabeceras, tipo de MIME y respuestas de servidor. También permite identificar solicitudes y respuestas DNS, SMTP, establecimientos de comunicaciones cifradas mediante certificados SSL.

Todos los logs se guardan en formato JSON y pueden ser analizados individualmente por el usuario o inyectados a un SIEM para su post-procesamiento y presentación grafica al usuario con la capacidad de realizar consultas.

A parte de ser un analizador de tráfico, Zeek puede definirse como un sistema de detección de intrusiones basado en anomalías. Para escribir las reglas se emplea su propio lenguaje de programación o scripting denominado Turing.

En lo que a funcionamiento se refiere, Zeek tiene una arquitectura dividida en dos bloques, su motor de eventos (núcleo) e intérprete de scripts. [32]

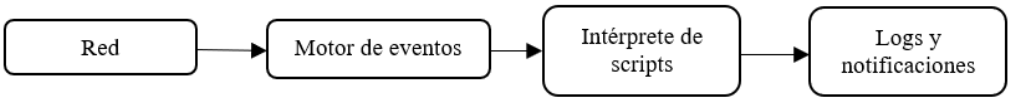


Imagen 3.7: Pipeline Zeek

El tráfico de red atraviesa el motor de eventos donde es analizado y convertido en eventos de nivel superior. Estos eventos reflejan la actividad de la red en términos neutrales es decir solo dicen que sucesos anómalos se han observado, pero no por qué han sucedido.

Seguidamente los eventos generados en el motor de eventos pasan al intérprete de scripts que en base a las reglas escritas en el lenguaje de Zeek determina si los eventos son de importancia para la generación de respectivas alertas

3.3 HIDS

En el apartado anterior hemos hecho el estudio de las soluciones NIDS disponibles en el mercado de forma gratuita. En este apartado nos vamos a centrar en el estudio de las soluciones HIDS para ver que herramienta será la más idónea para la implementación en nuestro sistema.

OSSEC es un sistema HIDS de código abierto. Se encarga de llevar a cabo el análisis de logs, verificación de integridad de los ficheros, monitorización del registro de Windows, detección de rootkits, alertas en tiempo real y respuesta activa. Es un sistema multiplataforma que soporta casi todos los sistemas operativos en los que están Linux, OpenBSD, FreeBSD, Mac OS X, Solaris y Windows. [33]

Su arquitectura se resume en tres componentes:

Imagen 3.8: Arquitectura OSSEC [33]

- Servidor → es la pieza responsable del almacenamiento de las bases de datos de todos los logs y registros relacionados con la verificación de integridad de archivos y eventos de los registros de sistemas operativos. También aquí es donde se realiza la gestión centralizada de todos los agentes desplegados, las reglas y decodificadores.
- Agentes → se trata del software que se despliega en los dispositivos cuya actividad se pretende monitorizar. Se encargan de recopilar la información tiempo real y periódicamente y hacerla llegar al servidor para análisis y correlación con las reglas de detección. Requieren de una cantidad mínima de recursos del sistema para la ejecución por lo que no afectan apenas al rendimiento del mismo.
- Agentless → el soporte de la funcionalidad sin agente permite la monitorización de dispositivos en lo que no es posible instalar el agente. Suelen ser firewalls, routers u otros sistemas con un software específico. Él envió de los datos se realiza directamente usando el protocolo syslog y estos son enviado al servidor desde los dispositivos a monitorizar.

El agente **Wazuh** es un HIDS multiplataforma gratuita que forma parte del ecosistema Wazuh SIEM. Para la monitorización se ejecuta en los dispositivos finales y envía los datos al servidor (Wazuh Manager) en tiempo real por medio de un canal cifrado. [21]

Está diseñado para poder funcionar en un amplio abanico de sistemas operativos tales como Linux, Windows, Mac OS, Oracle, AIX, HP-UX, etc. Su despliegue apenas afecta al rendimiento del dispositivo final ya que consume de media unos 35 MB de memoria RAM.

Entre sus funciones principales están:

- Recolección de logs
- Monitorización de integridad de ficheros (FIM)
- Inventario del sistema
- Respuesta activa
- Evaluación de configuración de seguridad
- Detección de malware

En lo que a arquitectura se refiere, esta es similar a la del OSSEC ya que Wazuh HIDS es una derivación del desarrollo de este, pero con más funcionalidades. Actualmente existen varias arquitecturas de despliegue:

-Wazuh Standalone → se compone de server, indexer, dashboard y agentes

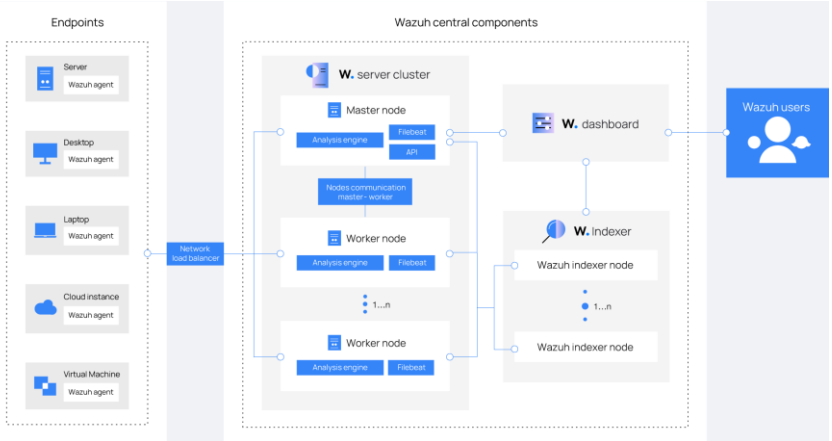


Imagen 3.9: Arquitectura Wazuh [22]

-Integración con Elastic Stack (ELK)→ está cayendo en desuso, debido a los cambios en la licencia de ELK siendo la última versión de Elasticsearch soportada por Wazuh la 7.X.

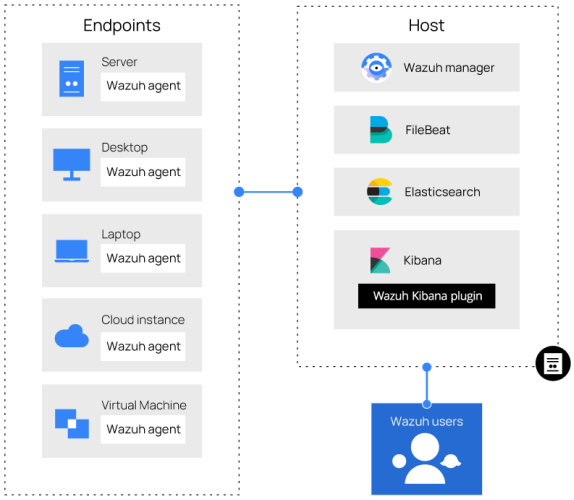


Imagen 3.10: Arquitectura Wazuh-ELK [22]

Samhain es un HIDS de código abierto. Permite visibilizar múltiples hosts o usarse únicamente como aplicación independiente en un solo host. Ofrece siguientes funcionalidades:

- Verificación de integridad de archivos
- Monitoreo/análisis de archivos de registro
- Monitoreo de puertos
- Detección de ejecutables Set User ID (SUID) no autorizados y procesos ocultos

La consola web de monitorización de Samhain se denomina Beltane y permite visualización centralizada de todos los agentes desplegados, la actividad del servidor, ver informes de clientes y actualización de bases de datos de referencia. [34]

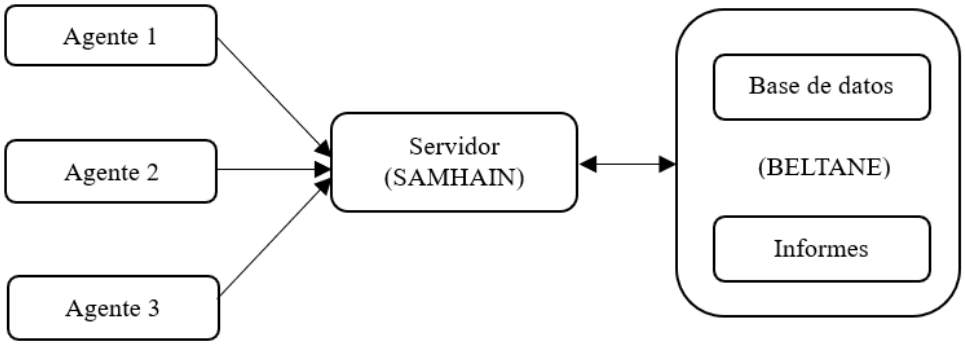


Imagen 3.11: Arquitectura SAMHAIN

Elastic Agent es un software de la suite Elastic, se trata de un agente único y unificado para observabilidad y seguridad. No es un HIDS propiamente dicho, pero puede actuar como tal haciendo uso de determinadas integraciones de las que dispone de forma nativa.

Este agente puede ser desplegado de forma independiente en un equipo o de forma centralizada en múltiples equipos siendo gestionado todo el conjunto por un servidor denominado Fleet también de la suite Elastic. [35]

Cada agente es capaz de monitorizar registros, métricas y otros datos de un host. Además, puede proteger el host frente a amenazas de seguridad gracias a las diferentes integraciones como por ejemplo Elastic Defend. Para cada agente se puede definir una política de gestión única a través de la cual se pueden añadir integraciones para nuevas fuentes de datos, protecciones de seguridad, etc.

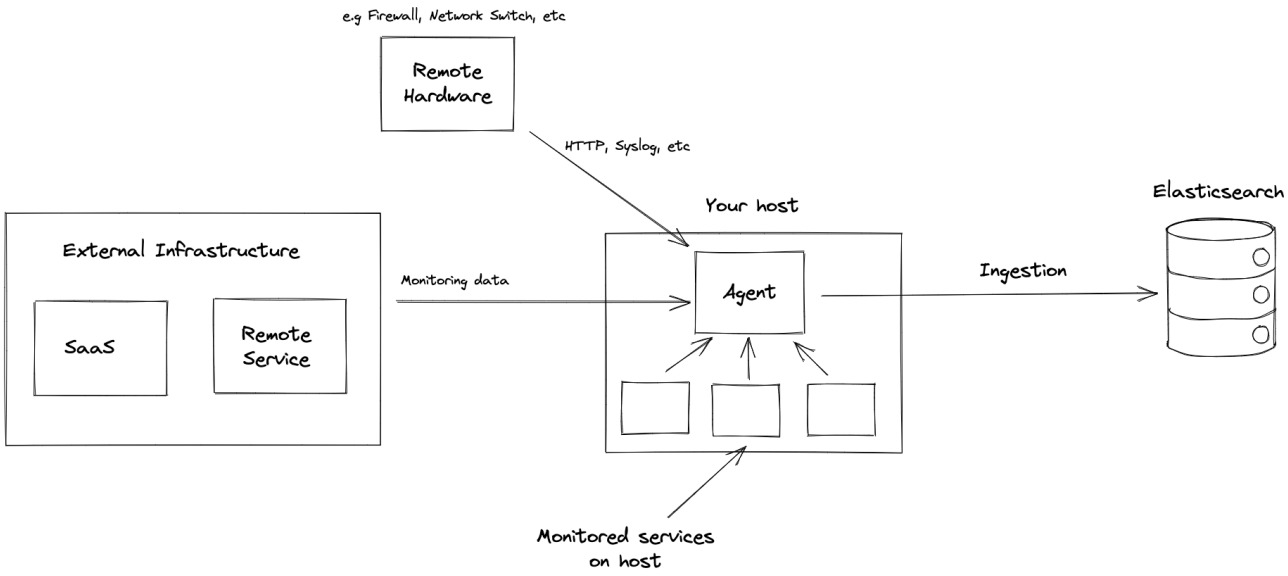


Imagen 3.12: Arquitectura Elastic Agent [35]

La integración de Elastic Defend para Elastic Agent proporciona capacidades como la recopilación de eventos, la detección y prevención de actividades maliciosas, excepciones y entrega de artefactos. [35]

3.4 Otras herramientas

Arkime o Moloch en sus versiones anteriores es un sistema de código abierto independiente de captura completa de paquetes (FPC) que permite a los analistas de redes y seguridad ver exactamente qué sucede desde el punto de vista de la red. Su funcionamiento consiste en captura de todo el tráfico de red, su almacenamiento en formato PCAP y su indexación en una base de datos para posterior análisis y búsqueda en función de metadatos.

Es un sistema cuyo despliegue es compatible con sistemas operativos basados en Linux como CentOS, Ubuntu, Arch, etc. Dispone de diferentes arquitecturas de despliegue pudiendo instalarse en un servidor único o de forma distribuida. Los dos servicios principales son el CAPTURE y el VIEWER, donde el primero se encarga de la captura de los paquetes y el segundo lleva a cabo la visualización de los paquetes. [36]

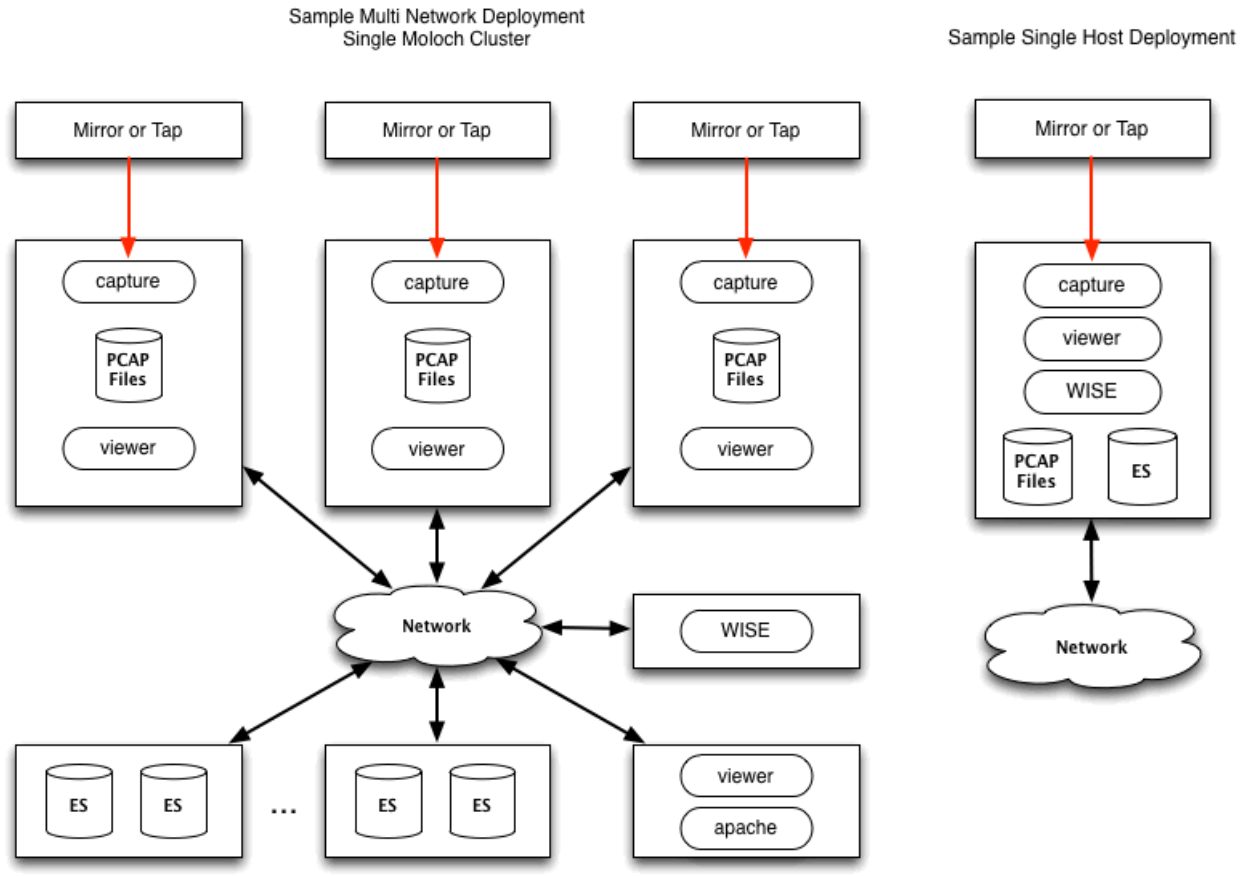


Imagen 3.13: Arquitecturas Arkime [36]

La base de datos que se utiliza para el almacenamiento de los índices de los paquetes capturados puede ser Elasticsearch o Opensearch.

Stenographer es una solución de captura completa de paquetes similar a Arkime que sirve para almacenar paquetes en el disco con fines de detección de intrusiones y respuesta a incidentes. Proporciona una implementación de alto rendimiento de escritura de paquetes de tarjeta de red a disco, gestiona la eliminación de esos archivos a medida que el disco se llena y proporciona métodos para leer conjuntos específicos de paquetes de forma rápida y sencilla. [37]

A diferencia de Arkime, únicamente ofrece indexado básico de paquetes y no permite indexado de protocolos ya que no soporta reensamblaje paquetes. Para suplementar esta carencia puede complementarse con otras soluciones como Zeek o Suricata.

3.5 Comparativa

En este apartado vamos a enumerar los parámetros clave de cada solucione y valor las mismas en base a esos parámetros para posterior toma de la decisión final.

Comparativa de las soluciones SIEM estudiadas:

	AlienVault OSSIM	**Wazuh**	**SELKS**	**Security Onion**
Licencia	GNU GPL v2	GNU GPL v2 y ALv2	GNU GPLv3	ELv2

Soporte	Soporte limitado al ser un producto secundario de la empresa AT&T	Gran comunidad. Actualizaciones periódicas	Actualizaciones y soporte limitados al ser un producto secundario de la empresa Stamus Networks	Gran comunidad. Actualizaciones periódicas
Integraciones	No existen	Con Splunk, Opensearch y Elasticsearch	Al estar basado en ELK stack existen, pero son limitadas	Multitud de integraciones gracias al uso como base de ELK stack y su ElasticAgent
Correlación de eventos	Si	No	No	No
Limitaciones	No recomendable para entornos muy grandes	Únicamente cubre los eventos de seguridad en los hosts	Únicamente cubre los eventos de seguridad en la red	No observadas
Arquitectura	Servidor único	Servidor único o distribuido	Servidor único	Servidor único o distribuido

Comparativa de las soluciones FPC estudiadas:

	Arkime	**Stenographer**
Licencia	ALv2	ALv2
Indexado básico	Si	Si
Indexado de protocolos	Si	No
Interfaz de usuario	Si	No

Comparativa de las soluciones NIDS estudiadas:

	Suricata	**Snort**	**Zeek**
Licencia	GNU GPL v2	GNU GPL v2	BSD
Documentación	Bien elaborada y con gran soporte por parte de la comunidad	Bien elaborada y con gran soporte por parte de la comunidad	Bien elaborada y con gran soporte por parte de la comunidad
Sistemas operativos	Linux, Windows, FreeBSD, OpenBSD	Linux, Windows, FreeBSD	Linux, Windows, FreeBSD y MacOS
Rendimiento	Soporte de multihilo con balanceo de carga	Sin soporte de multihilo	Sin soporte de multihilo
Escalabilidad	Orientado a entornos grandes. Altamente escalable.	Orientado a entornos de tamaño mediano o pequeño.	Altamente escalable. Apto para cualquier entorno.
Detección	Mediante reglas	Mediante reglas	Mediante reglas y scripts

Comparativa de las soluciones HIDS estudiadas:

	OSSEC	Wazuh SIEM	Samhain	Elastic Agent
Licencia	GNU GPL v2	GNU GPL v2 y ALv2	GNU GPL v1	ELv2
Documentación	Bien elaborada y con gran soporte por parte de la comunidad	Bien elaborada y con gran soporte por parte de la comunidad	Bien elaborada y actualizada	Bien elaborada y actualizada por parte de elastic.co
Sistemas operativos	Linux, OpenBSD, FreeBSD, Mac OS X, Solaris y Windows	Linux, Windows, Mac OS, Oracle, AIX, HP-UX	Linux, FreeBSD, Solaris, HP-UX, IRIX	Linux, Windows, Mac OS
Rendimiento	Alto rendimiento sin consumo relevante de recursos del sistema anfitrión	Alto rendimiento sin consumo relevante de recursos del sistema anfitrión	Alto rendimiento sin consumo relevante de recursos del sistema anfitrión	Alto rendimiento sin consumo relevante de recursos del sistema anfitrión
Escalabilidad	Gran escalabilidad	Gran escalabilidad	Gran escalabilidad	Gran escalabilidad
Funcionalidades	Monitorización de eventos, detección de intrusiones y respuesta activa Comprobación de integridad de ficheros	Monitorización de eventos, detección de intrusiones y respuesta activa Comprobación de integridad de ficheros	Monitorización de eventos en el host	Monitorización de eventos en el host. Funciones de seguridad gracias a las integraciones.

3.6 Alternativas comerciales

A pesar de que el abanico de las soluciones basadas en software libre ofrece múltiples opciones para conformar un sistema completo, también resulta interesante conocer algunas de las herramientas comerciales más empleadas. Las razones para ello son:

- Ausencia de personal formado técnicamente para despliegue de sistema propio desde cero.
- Necesidad de monitorizar durante un periodo de tiempo los activos mientras se realiza puesta en producción del sistema propio.
- Posibilidad de dedicar cierta cantidad de fondos a probar soluciones comerciales para obtener una imagen clara de ventajas y desventajas de estas frente a soluciones gratuitas.

Se trata de ofrecer un breve listado de soluciones con pequeñas descripciones para poder conocer las posibles alternativas comerciales a emplear en los casos anteriores. [43]

Splunk Enterprise Security

Es una solución que ofrece las funciones propias de un SIEM, tales como buscar, monitorizar y analizar macrodatos generados por miembros de una red informática. [44], [45] Entre sus funciones destacan:

- Análisis y clasificación de incidentes
- Protección de dispositivos finales permitiendo integraciones con soluciones de otras marcas.
- Protección de red mediante búsquedas, correlaciones, informes y alertas basados en eventos de la red.
- Marco de inteligencia de amenazas formado por fuentes abiertas, suscripciones, e inteligencia compartida.
- Análisis de riesgos mediante indexación de todas las fuentes de información y su posterior tratamiento.

Al ser una solución comercial dispone de dos planes de cobro:

- Basado en la carga de trabajo → en este caso se cobra en función de los recursos de cómputo consumidos durante búsqueda y análisis.
- Basado en la ingesta de tráfico → en este caso de cobra por la cantidad de datos en analizados en GB/día.

LogRythm SIEM

Es un sistema que consolida los datos y la actividad del usuario o del host en una sola vista, ayudando a los analistas a comprender y solucionar rápidamente los incidentes de seguridad. Al igual que Splunk permite integraciones con productos de diferentes proveedores incluso con el propio Splunk. [46]

Además de contar con las funcionalidades similares a las de Splunk, su ventaja frente a este radica en que ofrece soluciones tanto en la nube como en local y dispone de un plan de cobro que en el cual solo se paga una vez por contrato y se obtiene un servicio completo sin preocupaciones por el computo o ingesta de tráfico.

IBM QRadar SIEM

Es una solución SIEM que ofrece muchos beneficios, tales como:

- Maximización del tiempo y talento de los analistas gracias a uso de inteligencia artificial en tareas que pueden ser automatizadas.
- Aceleración de la detección y respuesta frente a amenazas gracias una integración nativa con comunidad SIGMA e IBM X-Force Threat Intelligence.
- Reducción de la complejidad operacional al incluir más de 700 integraciones y extensiones para compartir información e integrarse con otras herramientas.

Entre sus funcionalidades destacan:

- Análisis de amenazas de red
- Análisis de comportamiento de usuarios para detección de insiders.
- Inteligencia de amenazas basada en librerías de IPs, URLs, hashes de malware, etc.

Su modelo de cobro es similar al de Splunk, pudiendo pagar por número de clientes analizados o por número de eventos o flujos analizados por segundo. Además, ofrece soluciones en la nube y locales. [47]

En la siguiente tabla se puede ver una comparativa de las tres alternativas. [48]

	LogRhythm	Splunk	IBM QRadar
SIEM			
Flexible Data Collection	●	●	●
Log Management	●	●	●
Risk-based Monitoring	●	◐	●
Cloud Monitoring	◐	●	◐
Governance & Compliance	●	●	●
Intuitive Search	●	◐	◐
Security Analytics	●	●	●
MITRE ATT&CK Mapping & Support	◐	◐	◐
Custom Dashboards & Reporting	●	●	◐
UEBA			
Deterministic Rules	●	◐	●
Behavior Anomaly Detection	●	◐	◐
Insider Threat Detection	●	◐	◐

Imagen 3.14: Comparativa soluciones comerciales (I)

	LogRhythm	splunk>	IBM Radar
NDR			
Network Threat	●	○	●
Distrubted Analytics	●	○	◐
Threat Detection Workflows	●	○	◐
SOAR			
Rapid Automated Response	●	●	◐
Security Ecosystem Integrations	●	●	◐
Integrated Playbooks	◐	●	◐
Cross Platform			
Common Data Model	●	◐	◐
Rapid and Easy Implementation	●	○	○
Intuitive User Experience	◐	◐	◐
Responsive Support Options	●	◐	○
Flexible Deployment Options	●	◐	◐
Low Total Cost of Ownership	●	○	○
Security Analyst Focused Experience	●	◐	◐

Imagen 3.15: Comparativa soluciones comerciales (II)

4 Selección de las soluciones

En el apartado anterior hemos estudiado y comparado las soluciones NIDS, HIDS y SIEM más destacadas del mercado de software libre. Cada una de estas herramientas se puede desplegar y emplear de manera independiente obteniendo datos e información relativa a los eventos de seguridad de red o de host de manera relativamente sencilla. Sin embargo, lo que se busca en este trabajo es obtener un sistema que englobe las funcionalidades de todas estas soluciones y poder tener una visión global del estado de la seguridad de una red informática. Las soluciones como OSSIM, Wazuh SIEM o SELKS cuentan con muchas de las herramientas NIDS y HIDS analizadas tales como Suricata, OSSEC, Wazuh pero presentan ciertas limitaciones.

OSSIM es una solución que en sus principios era la pionera de las soluciones SIEM gratuitas, pero con el paso de tiempo sus creadores fueron desviando su atención y soporte hacia soluciones comerciales desarrollando herramientas derivadas como por ejemplo Alienvault USM. Por ello en la actualidad se trata de un sistema interesante pero que carece de un soporte periódico de calidad, no soporte integraciones y **no es escalable** al tratarse de un sistema de servidor único. Por estos motivos entre otros ha sido descartado como base para este trabajo.

Wazuh SIEM es otra solución muy interesante que cuenta con un gran abanico de funcionalidades para la monitorización de los **dispositivos finales**, detección de amenazas y cumplimiento normativo. Sin embargo, está limitado únicamente a los eventos que ocurren en un host sin tener información alguna sobre lo que sucede en la red. Este precisamente es el motivo por el que este sistema ha sido descartado como base para este trabajo.

SELKS al igual que Wazuh es una solución muy completa en su área, en este caso para monitorización, detección y prevención de amenazas a **nivel de red**. No obstante, este sistema también ha sido descartado por no cubrir la parte de monitorización de los dispositivos finales y no tener soporte solido para integraciones con otros sistemas.

Tras el análisis y descarte de todas las soluciones anteriores y teniendo en cuenta que lo que se busca es un sistema gratuito, capaz de monitorizar tanto la red como los dispositivos finales, escalable, con buen soporte por parte de la comunidad y que este abierto a las integraciones con otras soluciones, se ha escogido **Security Onion** como plataforma base para la realización de este trabajo.

A pesar de contar SO con Stenographer como solución FPC, se ha escogido el **Arkime** para tener un lugar que ofrezca una visualización clara y concisa de todo el tráfico de la red en forma de paquetes. Además, se ha optado por ciertas integraciones que ofrece el Elastic Agent tales como **Sysmon** y **Elastic Defend** para cubrir las necesidades de monitorización de los dispositivos finales.

4.1 Security Onion

Tal y como se ha comentado en el apartado 3.1 y como lo definen sus creadores es una plataforma abierta y gratuita creada por defensores para defensores que dispone de herramientas para visibilidad de la red, visibilidad del host, honeypots de detección de intrusiones, gestión de registros y gestión de casos. Entre estas herramientas destacan

Suricata, Zeek, Elasticsearch, Logstash, Kibana, Osquery, Fleet, CyberChef, Playbook, Grafana, etc. [25]

4.1.1 Licencia

El grueso del software incluido en SO tiene licencias de código abierto. Al ser el corazón del sistema los componentes de Elastic, SO adopta la misma licencia que este y es Elastic License 2.0 (ELv2). Se trata de una licencia Non-Copyleft. [26]

Esta licencia ofrece al usuario una licencia de por vida, no exclusiva, no sublicenciable e intransferible para usar, copiar, distribuir, poner a disposición y preparar trabajos derivados del software. Y presenta las siguientes limitaciones:

- No se puede proporcionar el software a terceros como un servicio alojado o administrado, donde el servicio brinda a los usuarios acceso a cualquier conjunto sustancial de características o funcionalidades del software
- No se puede mover, cambiar, deshabilitar ni eludir la funcionalidad de la clave de licencia en el software, y no se puede eliminar ni ocultar ninguna funcionalidad del software que esté protegida por la clave de licencia.
- No se puede alterar, eliminar ni ocultar ninguna licencia, derecho de autor u otros avisos del licenciante en el software. Cualquier uso de las marcas comerciales del licenciante está sujeto a la ley aplicable.

En cuanto a este trabajo, su propósito es ofrecer un sistema de monitorización de eventos de seguridad a usuarios domésticos o entidades privadas, y nunca como un servicio a terceros con fines lucrativos. Por lo tanto, las limitaciones de esta licencia no afectan al desarrollo de este proyecto.

4.1.2 Composición y capacidades

SO es una plataforma polivalente en la que todas las herramientas que a pesar de estar interrelacionadas pueden dividirse en varios grupos bien definidos.

-Base o núcleo

ELK, compuesto por elasticsearch, logstash, kibana y complementado por beats y agentes, actúa como núcleo para agregación, procesamiento, almacenamiento, análisis y visualización de los logs.

- **Elasticsearch** es un motor de búsqueda que se encarga de buscar e indexar los datos en diferentes formatos y generar índices de estos datos.
- **Logstash** es un motor que se encarga de la recopilación de datos, unificación de diversas fuentes y normalización de los formatos de datos para su posterior distribución.
- **Kibana** es la herramienta que sirve para exploración y visualización de datos en tiempo real.
- **Beats/agentes** son pequeñas aplicaciones que se encargan de recopilar los datos de los dispositivos finales y enviarlos a logstash.

Además del ELK, el SO hace uso de **Redis,** un almacén de estructura de datos en memoria que actúa como una base de datos intermediaria las consultas entre elasticsearch y

logstash. Es una implementación que mejora la eficiencia global del sistema cuando se trata de despliegue distribuidos.

Asimismo, la gestión de estos índices se lleva a cabo mediante **Curator**. Esta herramienta se encarga de:

- Listar todos los índices y generar una lista procesable.
- Definir una lista de filtros definidos por el usuario para eliminar de forma progresiva índices seleccionados
- Rotar de forma general los índices cuyo tiempo de vida supera los 30 días.

-Nivel de red

Para la visibilidad de la red SO cuenta con Suricata, Zeek, Stenographer y Strelka. Lo que ofrece SO es una fusión de IDS, metadatos de la red, análisis de archivos y captura completa de paquetes en un mismo sistema.

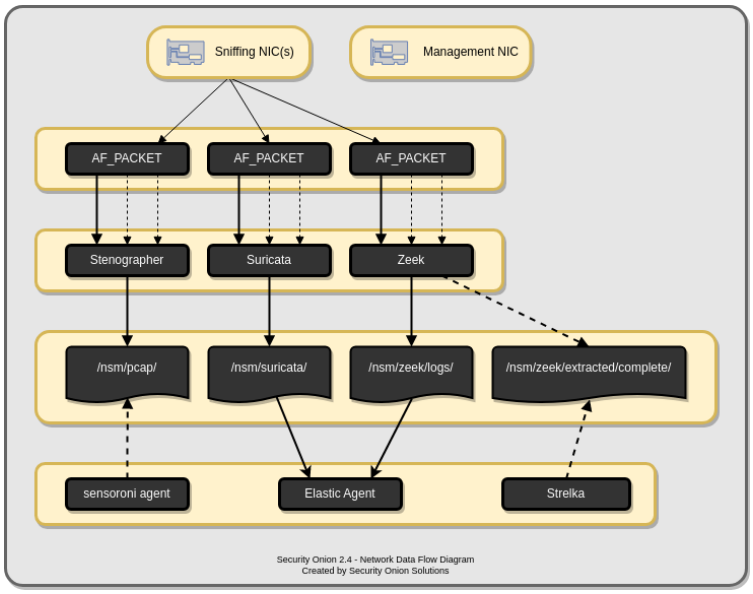


Imagen 4.1: Captura de trafico de red en SO [25]

- Detección de intrusiones consiste en la monitorización del tráfico de la red y generación de alertas en base a huellas/firmas e identificadores que identifiquen muestras de tráfico anómalas o maliciosas. De este proceso se encarga **Suricata** haciendo uso de las reglas escritas por la comunidad.
- Metadatos de la red a diferencia de la detección basada en firmas permiten recopilar logs de conexiones o información sobre protocolo que fluyen por la red ofreciendo una imagen más profunda de lo que sucede con los datos de la red. Para cubrir esta capacidad se puede emplear tanto Suricata como **Zeek** siendo el ultimo más eficiente en esta tarea.
- Captura completa de paquetes consiste en interceptar y guardar todo el tráfico de red en todo momento para su posterior análisis en caso de necesidad. Es útil para la identificación de amenazas, detección de congestión de red, detección de perdida de paquetes y análisis forense. Esta funcionalidad recaer sobre **Stenographer**.

- Análisis de archivos que atraviesan la red, que son extraídos por Suricata o Zeek, en búsqueda de metadatos relevantes. La información extraída es compara con las reglas YARA en búsqueda de malware. En este caso la herramienta responsable es **Strelka**.

Cada una de estas herramientas se alimenta a través de la interfaz de red física que a su vez recibe el tráfico de la red desde un puerto analizador de puertos de switch (SPAN) o punto de acceso de prueba (Network TAP).

-Nivel de host

Para la visibilidad del host SO cuenta con Elastic Agent, Elastic Fleet, Osquery, Syslog, Sysmon, Autoruns. Estas soluciones en su conjunto son capaces de recopilar una enorme cantidad de logs de dispositivos finales e incluso a realizar consultas específicas a los sistemas.

Elastic Agent es un agente de la suite de Elastic. Este agente es capaz de recopilar todo tipo de datos desde cualquier lugar de manera unificada por host. Todo se reduce en instalar, configurar y escalar. Cada nodo dentro de la arquitectura de SO cuenta con un agente para transportar a través de las diferentes integraciones los logs a ELK Stack sustituyendo en esta área los tradicionales beats. En cuanto a los dispositivos el agente se despliega de forma centralizada desde un gestor de agentes llamado Elastic Fleet.

Elastic Fleet es una consola de gestión de agentes Elastic integrada en la interfaz de Kibana. A través de esta consola es posible definir políticas para cada agente con sus respectivas integraciones, desplegar nuevos agentes, actualizar políticas y/o agentes y activar/desactivar diferentes métricas.

Para realizar las consultas con el de obtener información del sistema operativo o de lo que sucede en el dispositivo, SO hace uso de **Osquery** que también se integra con Elasticsearch por medio Elastic Agent. Esta herramienta es accesible desde la interfaz de Kibana y permite:

- Ejecutar consultas en vivo para uno o más agentes
- Ver un historial de consultas pasadas y sus resultados
- Programar consultas para capturar cambios de estado del sistema operativo a lo largo del tiempo
- Guardar consultas y crear una biblioteca de consultas para casos de uso específicos

Para manejar toda la información procedente tanto del host como de la red, el SO dispone de un conjunto de utilidades:

Security Onion Console o **SOC** es la interfaz de SO accesible vía web y contiene múltiples interfaces para realizar un seguimiento eficiente de las alertas y los eventos de seguridad.

- Alertas → muestra las alertas generadas por Suricata
- Dashboards → permite navegar por diferentes visualizaciones que recogen además de la información NIDS/HIDS diferentes logs y metadatos.
- Hunt → es una interfaz orientada para realización de caza de amenazas
- Cases → sirve para guardar o mapear logs, alertas o eventos relevantes durante la investigación de un incidente.

- PCAP → sirve para visualizar los PCAPs de Stenographer siendo solicitados previamente.
- Grid → permite ver el estado del despliegue de los nodos de SO y su estado
- Administration → permite realizar los ajustes del sistema

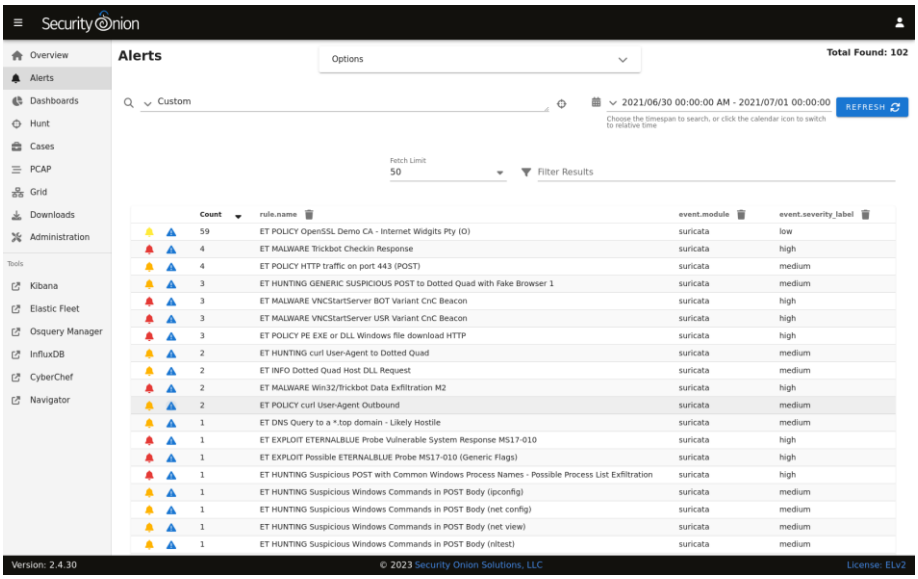


Imagen 4.2: Dashboard de alertas de SO [25]

Además, el SOC tiene accesos directos a herramientas como:

Playbook que permite la activación de diferentes escenarios detección usando reglas SIGMA. Una vez que un playbook se pone en activo comprueba recurrentemente los logs involucrados en la regla y en caso de cumplirse la regla lanza una alerta al analista por medio de Elast Alert. La alerta posteriormente puede ser consultada en los dashboard del SOC o de Kibana.

Cyberchef es una herramienta para manipulación rápida de los datos (decodificación, descompresión y análisis). [38]

4.1.3 Arquitectura

Uno de los motivos por los que se ha escogido SO como la plataforma para nuestro sistema es por sus capacidades de despliegue y escalabilidad que puede ofrecer a largo plazo en un entorno creciente. Esto es posible a gracias a que dispone de multitud de tipo de nodo para construir un entorno con una arquitectura apta para cualquier situación.

4.1.3.1 Tipos de nodos

Manager Node → cuenta con su propia instancia de Elasticsearch, pero se utiliza principalmente para la administración central, investigación de los casos y consulta de datos. Para ello cuenta con siguientes componentes SOC, Logstash, Kibana, Curator, ElastAlert, Redis.

Search Node → se encargan de extraer los registros de las colas de Redis en el manager node, analizarlos e indexarlos. Son los responsables de servidor los registros ordenados al usuario a través del manager node. Ejecuta los siguientes componentes Elasticsearch, Logstash, Curator.

Manager-Search Node → es la combinación de los dos nodos anteriores.

Forward Node → se encarga de canalizar alertas y logs Suricata y Zeek mediante Elastic Agent a Logstash del manager node. Los paquetes de tráfico capturados permanecen en el forward node por lo que resulta una solución idónea para actuar como sensor en ubicaciones remotas que no dispongan de un gran ancho de banda, pero suficiente para enviar alertas y logs. Únicamente ejecuta Zeek, Suricata y Stenographer.

Receiver Node → añade balanceo de carga al despliegue permitiendo que el procesado de logs continue, aunque el manager node este caído. Únicamente ejecuta Logstash y Redis.

Heavy Node → realizan tareas de sensores y almacenan sus propios registros en su propia instancia local de Elasticsearch. Esto da como resultado mayores requisitos de hardware y un menor rendimiento. Los nodos pesados NO extraen registros de la cola de Redis en el administrador como lo hacen los nodos de búsqueda. No son recomendados para entornos con mucha cantidad de tráfico. Cuentan con Elasticsearch, Logstash, Curator, Zeek, Suricata y Stenographer.

Elastic Fleet Standalone Node → tiene como función descargar la sobrecarga del manager node cuando el número de agentes de los dispositivos es muy elevado. También es útil para dispositivos fuera de la intranet por lo que permite su monitorización desde la DMZ.
Intrusion Detection Honeypot Node → tiene como función principal simular los servicios comunes de red como HTTP, FTP o SSH para exponerlos y recibir ataques. De esta manera se consigue incitar a los atacantes a interactuar para poder detectar un posible ataque futuro y conocer su forma de proceder. Cada vez que un servicio se ve atacado se genera una alerta y el usuario es avisado.

4.1.3.2 Tipos de despliegue

Import → es la arquitectura más simple cuya función principal es ejecutar las herramientas precisas y necesarias para importar y analizar paquetes en formato PCAP o EVTX.

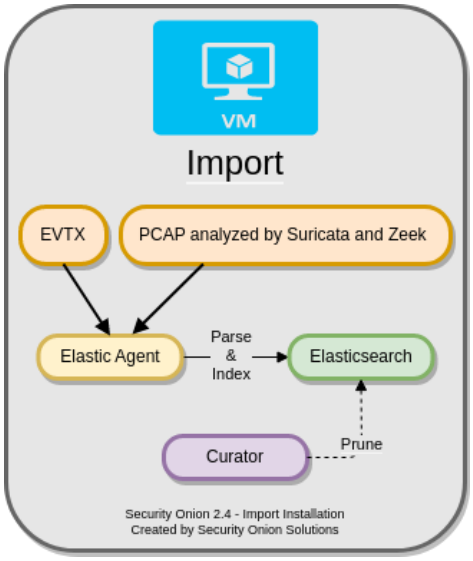


Imagen 4.3: Despliegue Import [25]

Evaluation → es una arquitectura pensada para realización de pruebas rápidas del sistema en un posible entorno de producción. Dispone de interfaz de red para captura de tráfico y

software mínimo para análisis de logs y alertas. Su particularidad es que no ejecuta Redis por lo que Elastic Agent envía los logs directamente al Elasticsearch.

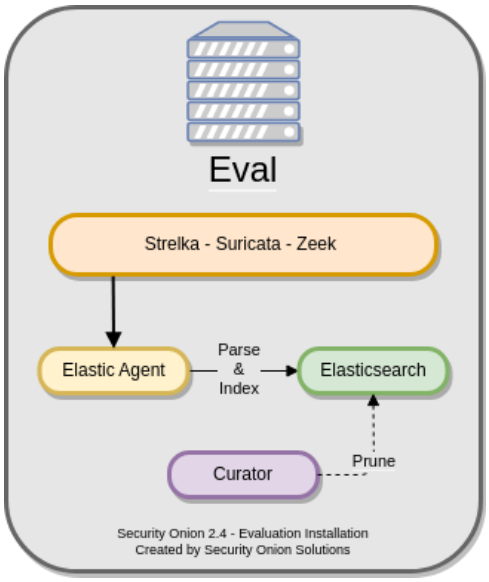


Imagen 4.4: Despliegue Evaluation [25]

Standalone → es un despliegue concebido para pruebas, laboratorios, pruebas de concepto o entornos con recursos muy limitados como puede llegar a ser un usuario doméstico. No es escalable por lo que no puede ser modificado a posteriori.

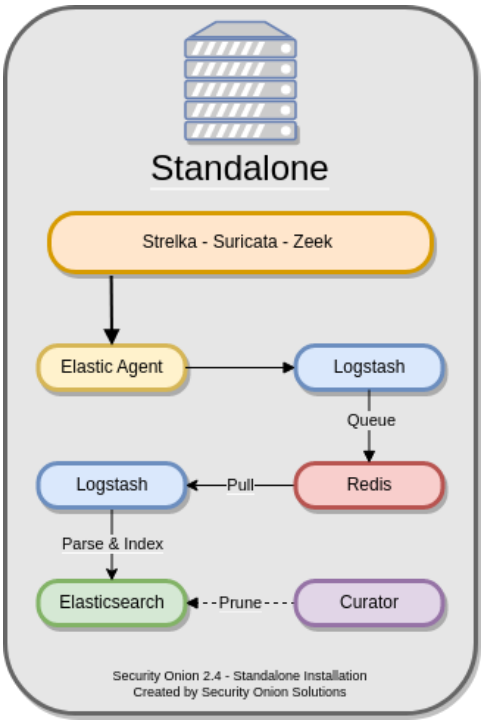


Imagen 4.5: Despiliegue Standalone [25]

Distributed → es la arquitectura pensada para un entorno de producción. Normalmente cuenta con un manager node, varios search nodes y varios forward nodes. También se admite la posibilidad de utilizar manager-search node. Es una arquitectura perfectamente escalable que puede ser cumplimentada por otros nodos secundarios.

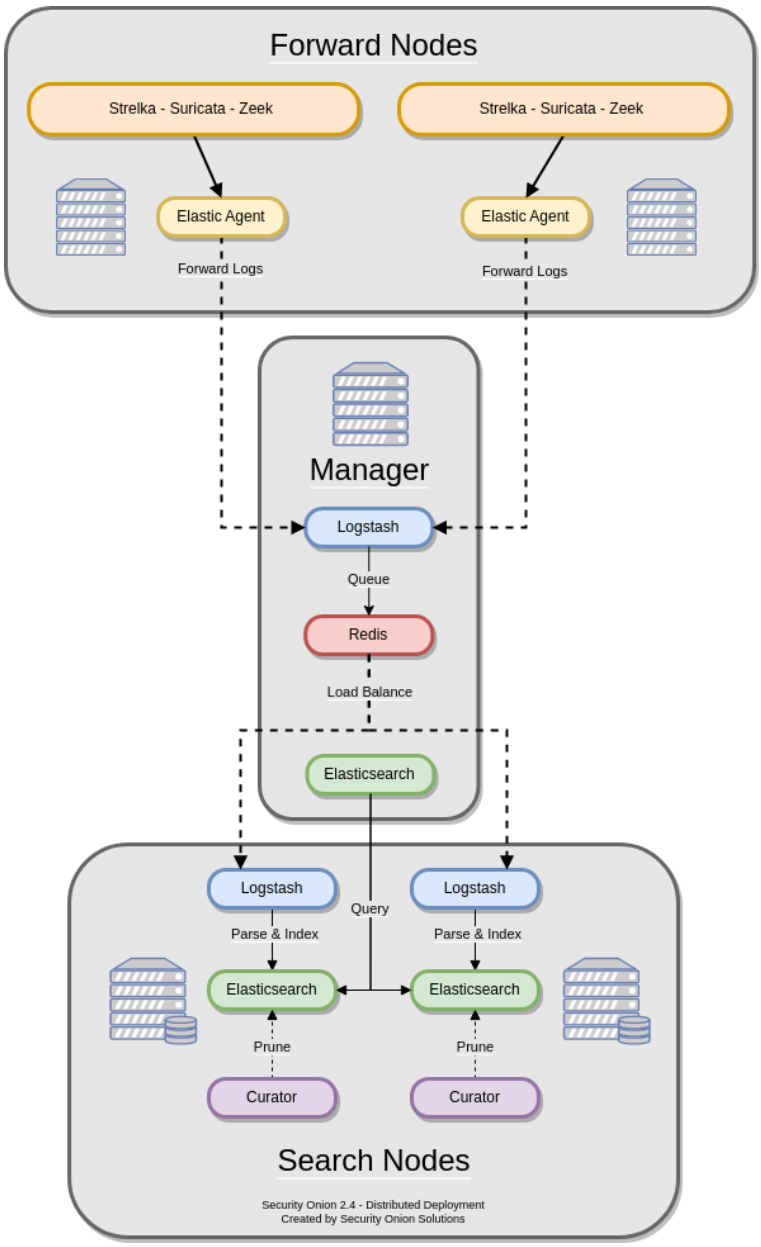


Imagen 4.6: Despliegue Distributed [25]

4.2 Arkime

Tal y como se ha tratado en el apartado 3.4 de este proyecto existe una herramienta muy interesante que puede servir como un buen complemento al SO a la hora de visualizar y manejar los paquetes de red capturados. Se trata de Arkime, que aparte de suplir las carencias de Stenographer puede servir como sistema de backup del tráfico capturado al disponer este de su propia interfaz y base de datos para almacenar el tráfico.

4.2.1 Arquitectura

Como ya dijimos en el apartado 3.4, la base de datos que se utiliza para el almacenamiento de los índices del Arkime puede ser Elasticsearch por lo que en este proyecto vamos a configurar e integrar el Arkime para trabajar con el Elasticsearch disponible en el SO. De esta manera conseguiremos ahorrar recursos de hardware y obtendremos visualizaciones adicionales de los PCAPs capturados, pudiendo hacer uso de Kibana y de Arkime Viewer.

La arquitectura a emplear será la siguiente:

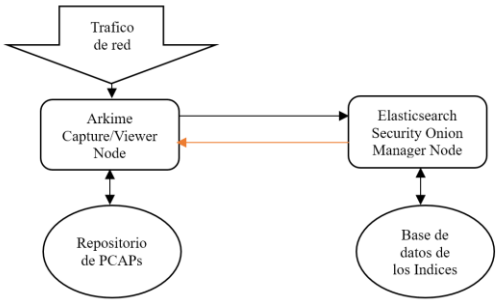


Imagen 4.7: Despliegue Arkime

4.3 Integraciones

Para conseguir un sistema aún más sólido y eficaz, además de Arkime gracias a las integraciones que ofrece Elastic Agent se van a desplegar varias herramientas para no solo mejorar la monitorización de los dispositivos finales sino añadir capacidades de protección a estos dispositivos frente a diversas amenazas.

4.3.1 Elastic Defend

Se trata de una integración que ofrece Elastic Agent con el módulo Elastic Security. El módulo Elastic Security es una solución de pago que ofrece Elastic a nivel corporativo, pero a pesar de ello Elastic Defend cuenta con ciertas funcionalidades gratuitas que resultan de gran interés para ofrecer una mayor protección a los hosts. [39]

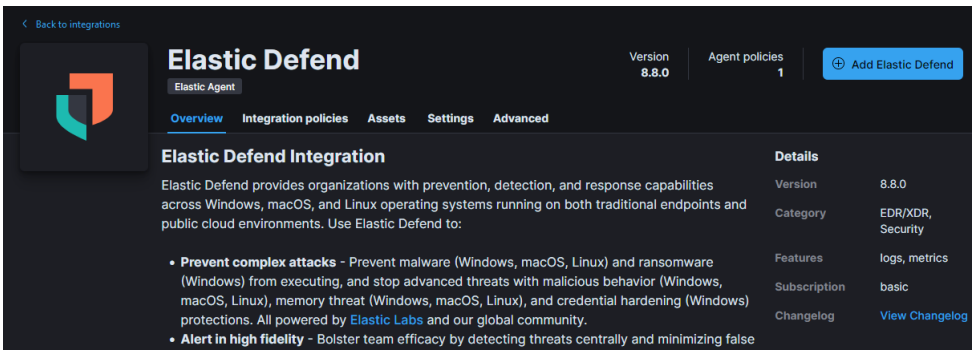


Imagen 4.8: Integracion Elastic Defend

Una vez activada la integración se produce el despliegue de un cliente endpoint en los dispositivos finales y todas las gestiones se realizan desde un panel dedicado dentro de Kibana. Durante la configuración de la integración y su política despliegue, se pueden configurar las siguientes funcionalidades:

- Listas de aplicaciones de confianza, filtros de eventos, listas de bloqueo.
- Detección y protección frente a malware tanto en Windows como en macOS y Linux
- Antivirus, en el caso de no disponer de un producto dedicado. Una alternativa muy interesante a Windows Defender.

Además, el endpoint es capaz de recoger los registros de los siguientes eventos y generar alertas en base en unas reglas que viene preconfiguradas para diferentes casos de uso:

- Acceso con/sin credenciales
- Carga de controladores y librerías (DLL)
- DNS
- Ficheros
- Red
- Procesos
- Registro
- Seguridad

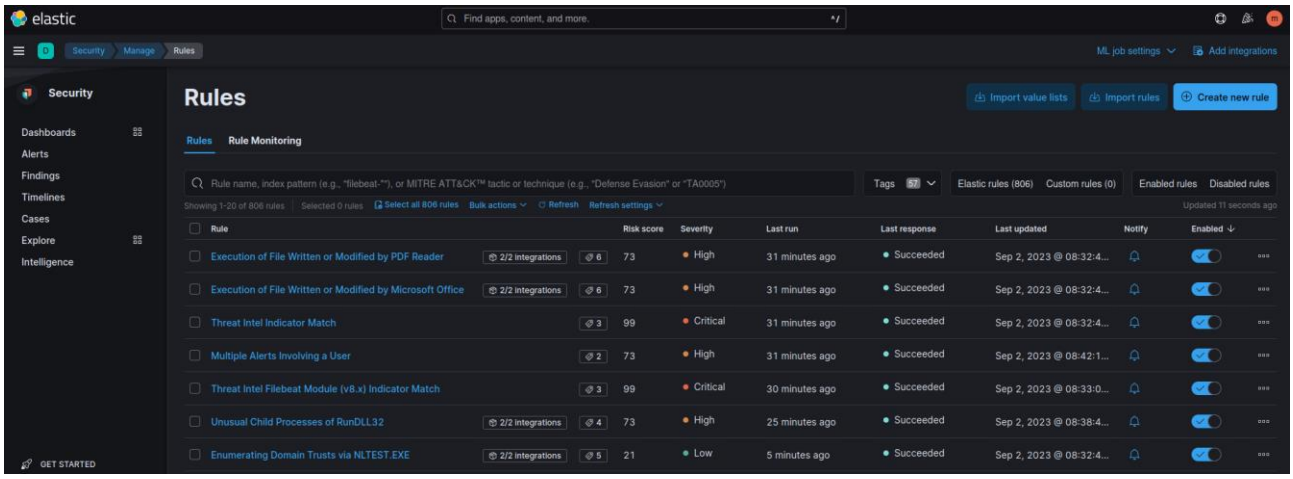


Imagen 4.9: Reglas de detección de Elastic Defend

Gracias a todas estas capacidades totalmente gratuitas podremos enriquecer notablemente la tarea de monitorización de dispositivos finales sin añadir sobrecarga a los recursos de estos dispositivos.

4.3.2 Sysmon

System Monitor (Sysmon) es un servicio de Windows y un controlador de dispositivo que, una vez instalado en un sistema, resulta persistente durante los reinicios del sistema con el fin de monitorizar y registrar la actividad del sistema a través del registro de eventos de Windows. Proporciona información detallada sobre la creación de procesos, conexiones de red y cambios en el tiempo de creación de archivos. Estos eventos una vez recopilados sirven para alimentar un SIEM que los procesa y analiza para identificar actividades maliciosas o anómalas. [40]

Esta herramienta es de gran interés para este trabajo ya que Elastic Agent dispone de una integración nativa para poder inyectar los logs procedentes de sysmon al Elasticsearch para su posterior análisis. Y al igual que Elastic Defend resulta ser un complemente excelente para mejorar la seguridad en los dispositivos finales.

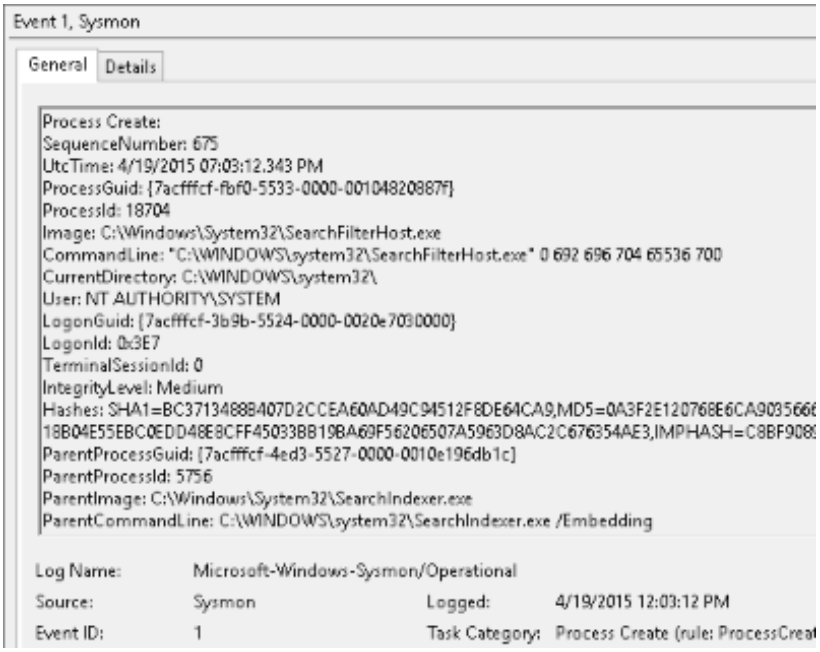


Imagen 4.10: Sysmon Event [40]

Entre sus capacidades más interesantes están:

- Registro de la creación de procesos con una línea de comandos.
- Registro del hash de los archivos de imagen de proceso usando SHA1 (el valor predeterminado), MD5, SHA256 o IMPHASH.
- Incluye un GUID de proceso en los eventos de creación del proceso para permitir la correlación de eventos incluso cuando Windows reutiliza los ID de proceso.
- Incluye un GUID de sesión en cada evento para permitir la correlación de eventos en la misma sesión de inicio de sesión.
- Registra la carga de controladores o DLL con sus firmas y hashes.
- Detecta cambios en el tiempo de creación de archivos para comprender cuándo se creó realmente un archivo.
- Recarga automáticamente la configuración si se modifica en el registro.
- Genera eventos desde las primeras etapas del proceso de arranque para capturar la actividad realizada incluso por malware sofisticado en modo kernel.

Su despliegue es muy rápido e intuitivo y su configuración es muy flexible y se realiza a través de un archivo en formato .xml.

4.3.2 Syslog

Syslog es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro. Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío. [41]

Al igual que sucede con otros tipos de datos y logs, Elastic Agent cuenta con integraciones de syslog para dispositivos de diferentes fabricantes que componen la electrónica de red tales como Fortinet, Cisco o pfSense. En nuestro caso vamos a hacer uso de la integración de logs procedentes de un sistema de enrutamiento simulado con pfSense.

Esta integración permite ver de forma centralizada y en un mismo lugar toda la información relativa a los primeros intentos de vulnerar la seguridad perimetral de una red. Lo consigue gracias al indexado de los logs de firewall, primera barrera de nuestra red, en Elasticsearch.

5 Definición de requisitos y creación del entorno virtual

5.1 Establecimiento de la arquitectura de despliegue

De todas las arquitecturas la más idónea para un entorno empresarial seria la distribuida. Debería contar con un nodo manager, un nodo search y varios nodos forward. Un posible ejemplo de despliegue podría ser el siguiente:

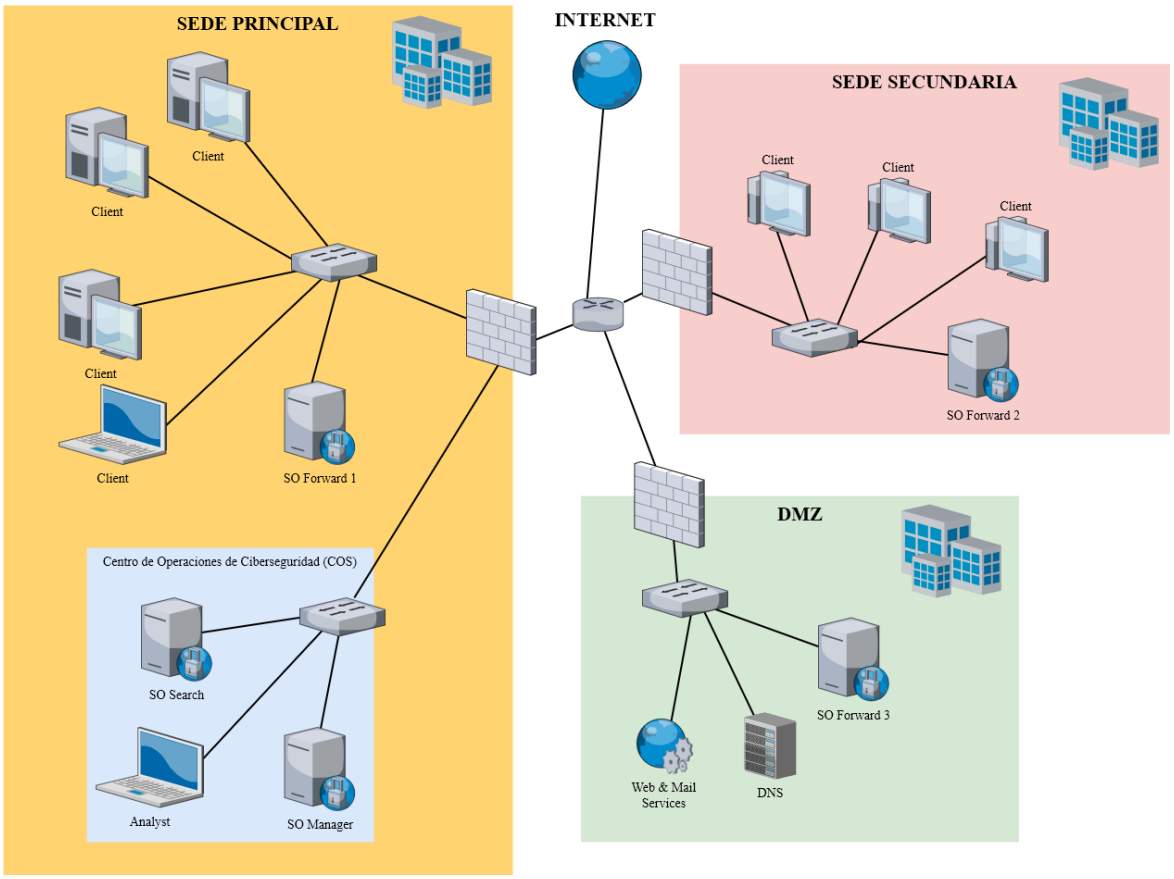


Imagen 5.1: Ejemplo de arquitectura de SO en un entorno empresarial

Tal y como podemos ver el nodo manager y el nodo search se ubicarían dentro de la célula de monitorización de la sede principal y el nodo forward-1 estaría capturando el tráfico de red del switch principal de la sede.

Otros nodos sensores forward-2 y forward-3 se ubicarían en la sede secundaria y DMZ respectivamente con el fin de capturar el tráfico de los switchs de estos segmentos de red.

En cuanto a los firewalls y el router perimetral, estos enviarían sus logs al SIEM mediante las integraciones de syslog que ofrece Elastic Agent. Los dispositivos finales a su vez reportarían también al SIEM mediante Elastic Agent.

Tomando como referencia el entorno anterior vamos definir la arquitectura del entorno simulado sobre el que se va a desplegar el sistema de monitorización objeto de este trabajo. En este entorno se va a simular una red compuesta por dos equipos con diferentes entornos, Windows y Linux, que serán atacados desde otro equipo con Kali Linux. Para la monitorización se desplegará el conjunto de SO adoptando una **arquitectura distribuida** basada en dos nodos, nodo **manager-search** y nodo **forward**.

De esta manera conseguiremos un despliegue lo más real posible y ahorraremos recursos de hardware al unificar capacidades de administración, indexado y búsqueda en una misma máquina virtual.
En cuanto a los sistemas complementarios el despliegue de SO será complementado por una máquina virtual que albergará **Arkime** que a su vez se integrará con Elasticsearch.

La arquitectura del entorno descrito quedara tal como así:

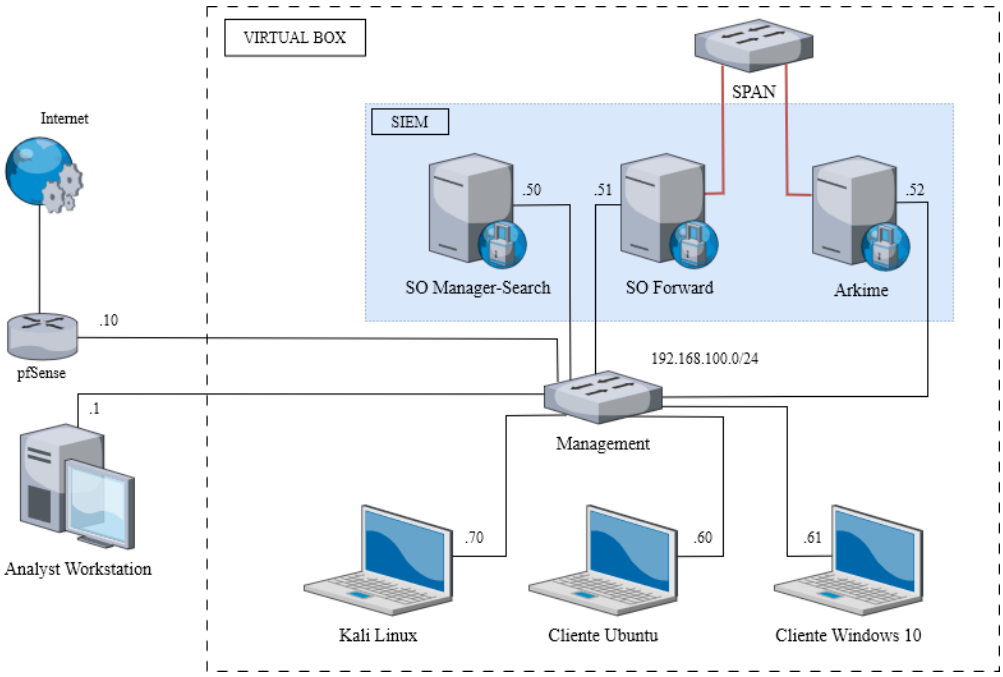


Imagen 5.2: Ejemplo de arquitectura de SO en un entorno empresarial

5.2 Selección de sistemas operativos

En cuanto a los sistemas operativos escogidos para el despliegue, estos son variados debido a los requisitos de las diferentes soluciones.

Oracle Linux 9 → es el sistema utilizado como base por la distribución 2.4.20 de Security Onion, por lo tanto, para evitar cualquier problema en el momento de instalación vamos a conservar este sistema, aunque SO tiene soporte para Rocky Linux 9, Alma Linux 9, CentOS Stream 9, RHEL 9, Ubuntu 22.04 y Debian 12.

CentOS 7 → es un sistema basado en el código de RHEL y tiene la máxima compatibilidad con las últimas versiones de Arkime. También, es posible usar otros sistemas operativos como CentOS 8 (sin soporte), Arch, EL 9 o Ubuntu 22.04.

FreeBSD → es el sistema utilizado como base para la distribución de pfSense.

Debian → es el sistema utilizado como base para la distribución de Kali Linux.

Microsoft Windows 10 → es el sistema escogido para despliegue de un cliente que formara parte de nuestra red a monitorizar y a la que realizaremos ataques con diferentes herramientas de Kali Linux.

Ubuntu 22.04 → es el sistema operativo escogido para el despliegue de un cliente adicional que formara parte de nuestra red a monitorizar y a la que realizaremos ataques con diferentes herramientas de Kali Linux

5.3 Definición de los requisitos según la arquitectura elegida

Al escoger la arquitectura de SO distribuida de dos nodos, es necesario definir los requisitos mínimos de las máquinas virtuales que albergaran cada nodo sin olvidarnos de Arkime.

Nodo Manager-Search

Sistema Operativo	Oracle Linux 9
Procesador	4 vCPUs
Memoria RAM	16 GB
Almacenamiento	200 GB
Adaptadores de red	1 x Management

Nodo Forward

Sistema Operativo	Oracle Linux 9
Procesador	4 vCPUs
Memoria RAM	8 GB
Almacenamiento	200 GB
Adaptadores de red	1 x Management, 1 x Sniffing

Arkime

Sistema Operativo	CentOS 7
Procesador	4 vCPUs
Memoria RAM	8 GB
Almacenamiento	200 GB
Adaptadores de red	1 x Management, 1 x Sniffing

Kali

Sistema Operativo	Debian
Procesador	1 vCPUs
Memoria RAM	2 GB
Almacenamiento	40 GB
Adaptadores de red	1 x Management

Cliente Windows

Sistema Operativo	Windows 10
Procesador	1 vCPUs
Memoria RAM	2 GB
Almacenamiento	50 GB
Adaptadores de red	1 x Management

Cliente Ubuntu

Sistema Operativo	Ubuntu 22.04
Procesador	1 vCPUs
Memoria RAM	2 GB
Almacenamiento	40 GB
Adaptadores de red	1 x Management

pfSense

Sistema Operativo	FreeBSD
Procesador	1 vCPUs
Memoria RAM	1 GB
Almacenamiento	16 GB
Adaptadores de red	1 x Management, 1 x WAN

5.4 Creación del entorno virtual

Para el despliegue del entorno virtual se va a utilizar el software de virtualización gratuito Oracle VM Virtual Box. [42] Previamente a la creación del entorno virtual vamos a crear la red de tipo *"Solo Anfitrión"* que será en la que se comunicaran todos los sistemas desplegados.

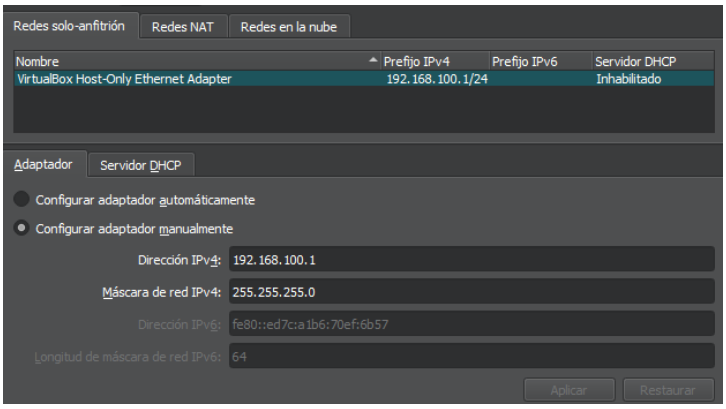


Imagen 5.3: Configuración de red en Virtual Box

Nodo Manager-Search

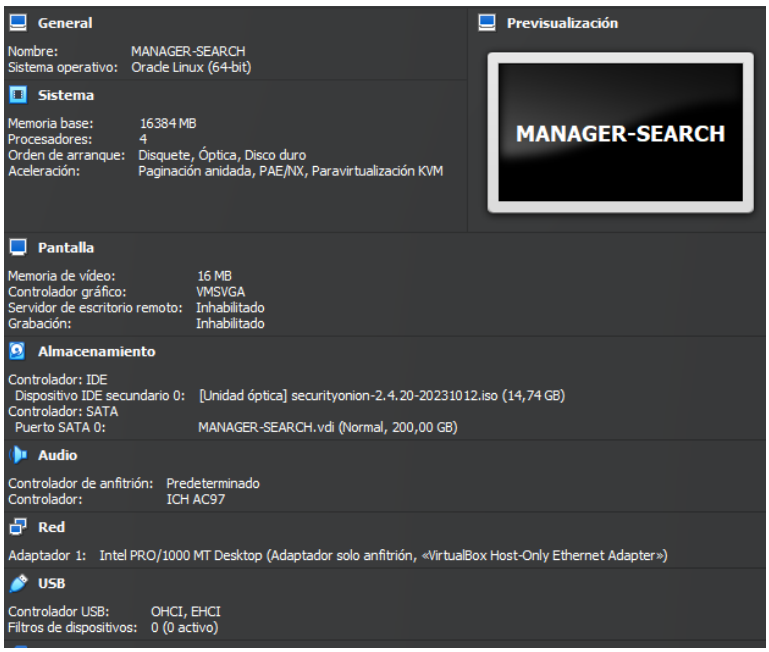


Imagen 5.4: Configuración Nodo Manager-Search

Nodo Forward

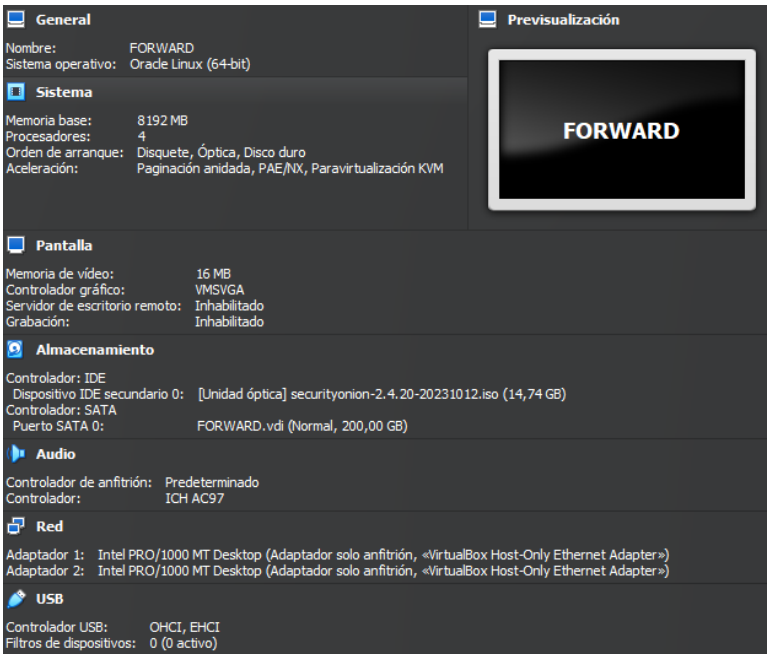


Imagen 5.5: Configuración general Nodo Forward

Es muy relevante configurar el modo promiscuo en la interfaz que va a capturar el tráfico. Para ello el modo promiscuo se tiene que poner en *"Permitir todo"*.

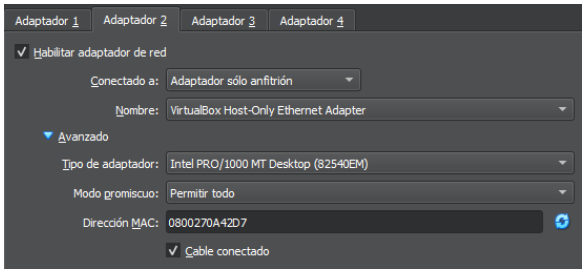


Imagen 5.6: Configuración de tarjetas de red en el Nodo Forward

Arkime

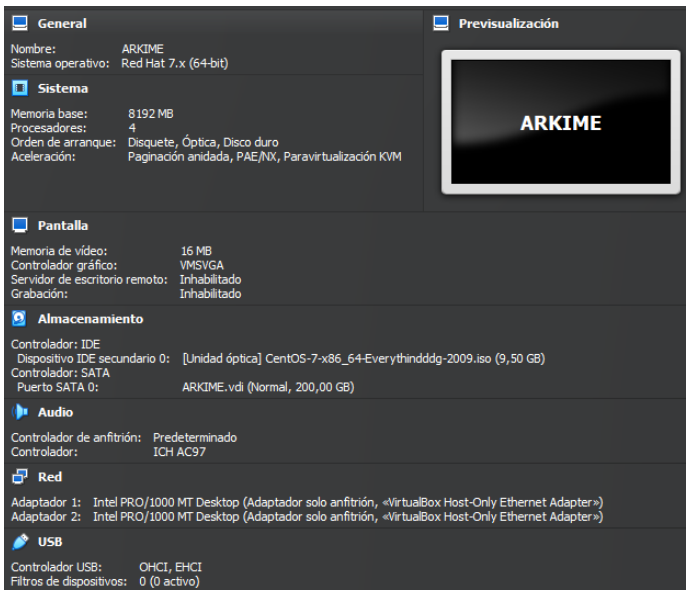


Imagen 5.7: Configuración general Arkime

Es muy relevante configurar el modo promiscuo en la interfaz que va a capturar el tráfico. Para ello el modo promiscuo se tiene que poner en *"Permitir todo"*.

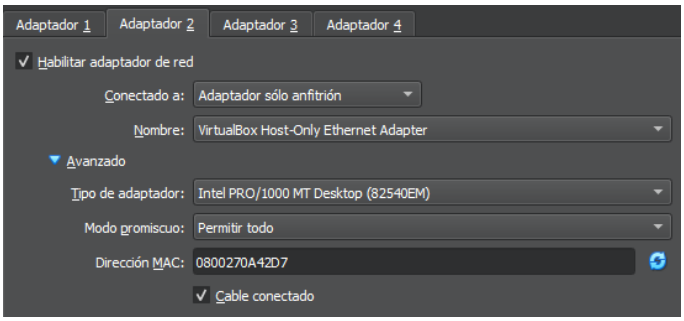


Imagen 5.8: Configuración de tarjetas de red en el Arkime

pfSense

Imagen 5.9: Configuración pfSense

Cliente Ubuntu

Imagen 5.9: Configuración cliente Ubuntu

Cliente Windows 10

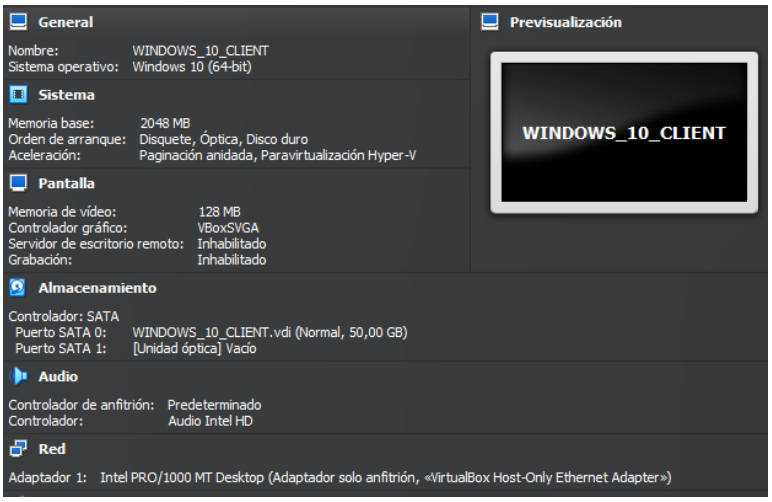


Imagen 5.10: Configuración cliente Windows 10

Cliente Kali Linux

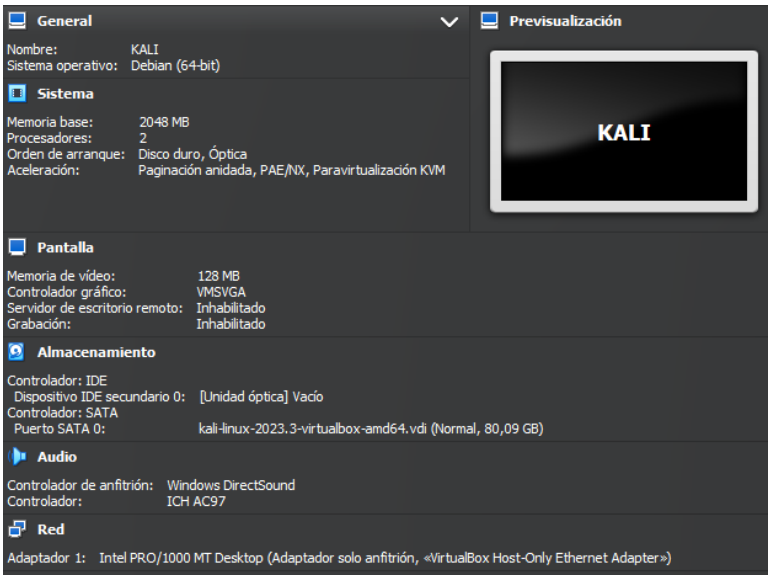


Imagen 5.11: Configuración cliente Kali Linux

El entorno creado se puede resumir en una red **LAN (192.168.100.0/24)** con salida a Internet a través de un firewall **pfSense** cuyo despliegue se especifica en el Anexo IV, que cuenta con dos interfaces, una para la red LAN y otra para la WAN (Internet). Dentro de la red LAN tenemos nuestro sistema de monitorización compuesto por dos nodos de **SO**, una máquina virtual con **Arkime**, dos máquinas virtuales cliente, una de **Windows** y otra de **Linux**, y una máquina virtual para realizar ataques con **Kali Linux**. El despliegue y configuración de estas últimas máquinas virtuales se especifica en el Anexo V.

Tal y como se ha mencionado en el apartado 1.3 todo el entorno es albergado por un equipo portátil Lenovo ThinkPad con una CPU Intel Core i7 de 9ª generación, un SSD de 2TB y 64GB de memoria RAM. Además, el mismo equipo es el que actúa como estación del analista de ciberseguridad.

6 Despliegue del sistema

Una vez preparado el entorno de virtualización se procederá con la instalación de las soluciones escogidas. El despliegue y la configuración de los nodos de Security Onion están recogidos en el anexo I. En cuanto a la instalación de Arkime y su integración con Security Onion, este proceso esta descrito en el anexo II.

Una vez cubierta la parte de red se desplegarán los agentes de Elastic Agent en los clientes simulados con Windows 10 y Ubuntu, según el anexo III.

6.1 Integraciones

Una vez realizado el despliegue del sistema de monitorización integrado por Security Onion y Arkime se va a complementar con herramientas adicionales mediante el uso de la capacidad “Integrations” de Elastic Agent.

6.1.1 Sysmon

Para despliegue de sysmon, es necesario descargar el paquete de instalación de la página oficial de Microsoft y un archivo de configuración, el más famoso y moldeable se puede obtener en Github.

-Paquete sysmon:

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

-Archivo de configuración:

https://github.com/SwiftOnSecurity/sysmon-config

Una vez descargado todo lo necesario, hay que descomprimirlo en una carpeta, por ejemplo, en el escritorio. Con todo los necesario en una carpeta hay que ejecutar línea de comandos de Windows con privilegios de administrador, dirigirse a la ruta donde están los archivos de instalación y lanzar el siguiente comando:

Sysmon64.exe -i sysmonconfig-export.xml

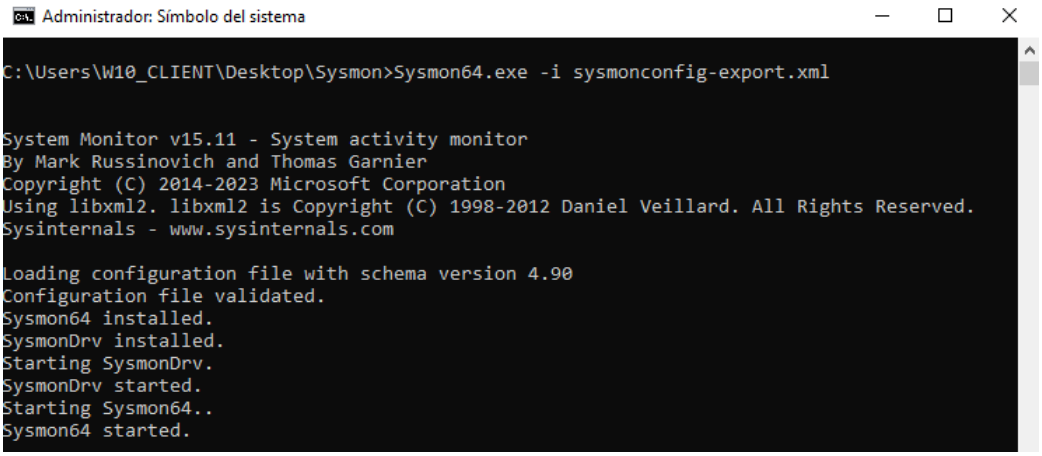


Imagen 6.1: Instalación Sysmon (I)

Una vez desplegado el sysmon en el cliente, es necesario modificar la política de los agentes en Elastic Fleet y habilitar la integración con sysmon.

Desde Kibana → Fleet → Agent policies → endpoints-initial → windows-endpoints → activar Sysmon Operational.

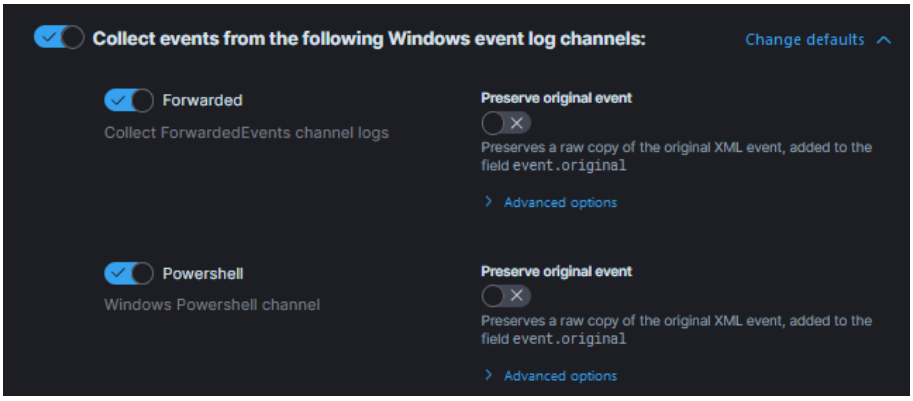


Imagen 6.2: Instalación Sysmon (II)

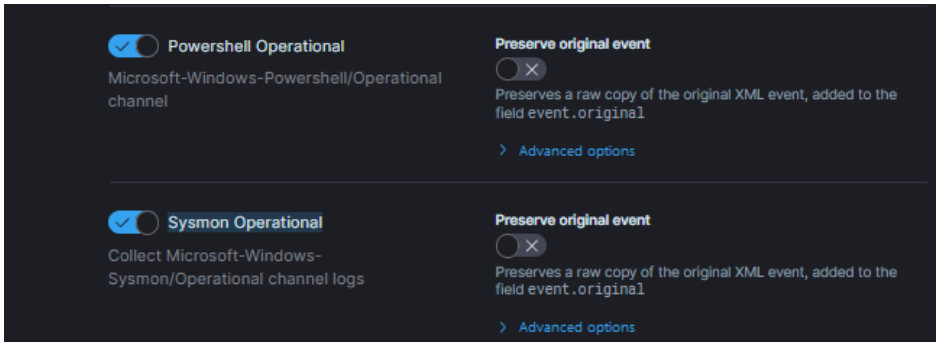


Imagen 6.3: Instalación Sysmon (III)

Una vez activado hay que aplicar los cambios en la política y esperar a que estos se refresquen en el agente del cliente. Para verificar el correcto funcionamiento de sysmon y recepción de logs desde el cliente hay que ir a Kibana → Dashboard→ Security Onion-Sysmon.

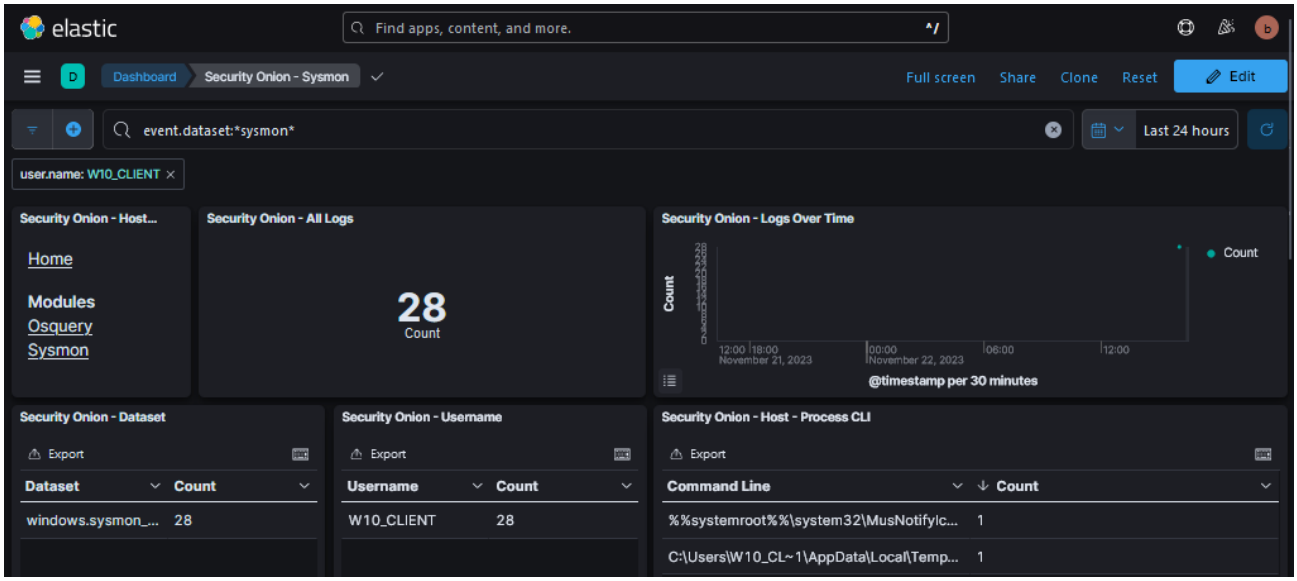


Imagen 6.4: Instalación Sysmon (IV)

6.1.2 Elastic Defend

Para despliegue de Elastic Defend únicamente hay que activar la integración correspondiente en la política de clientes de Elastic Fleet.

Desde Kibana → Fleet → Agent policies → endpoints-initial → Add integration → Elastic Defend → Add Elastic Defend.

Una vez añadida la integración hay que configurar la política correspondiente.

Desde Kibana → Fleet → Agent policies → endpoints-initial → elastic-defend-endpoints → realizar modificaciones → Save changes.

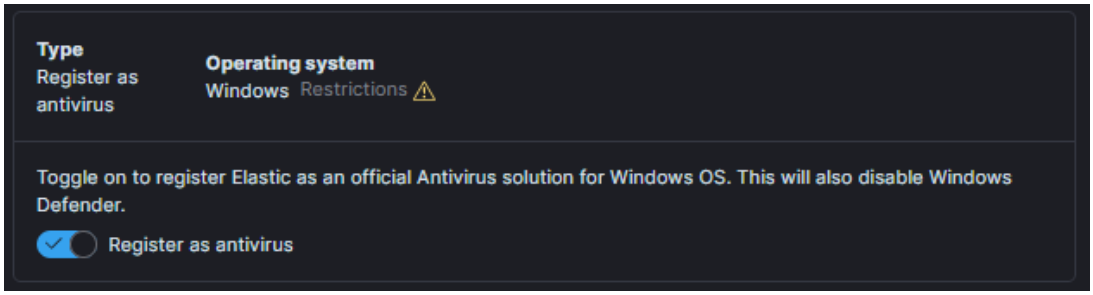


Imagen 6.5: Instalación Elastic Defend (I)

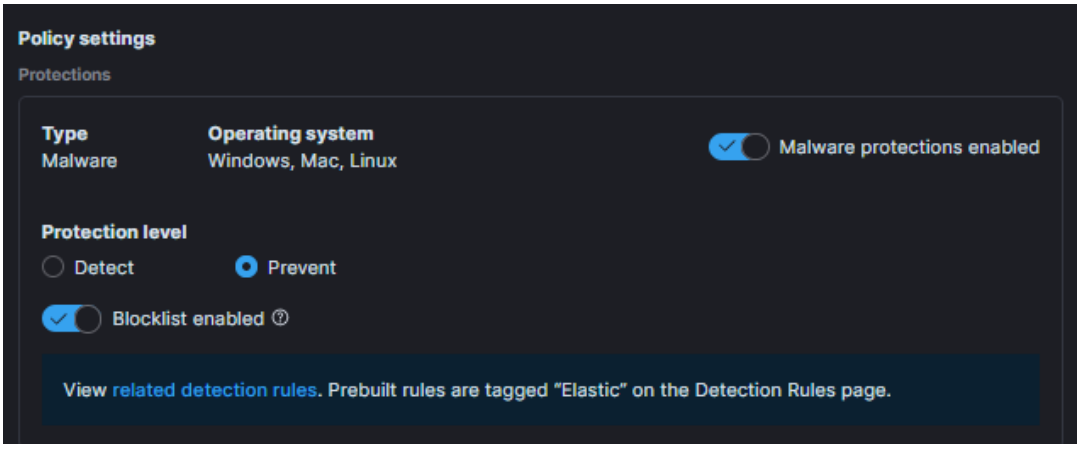


Imagen 6.6: Instalación Elastic Defend (II)

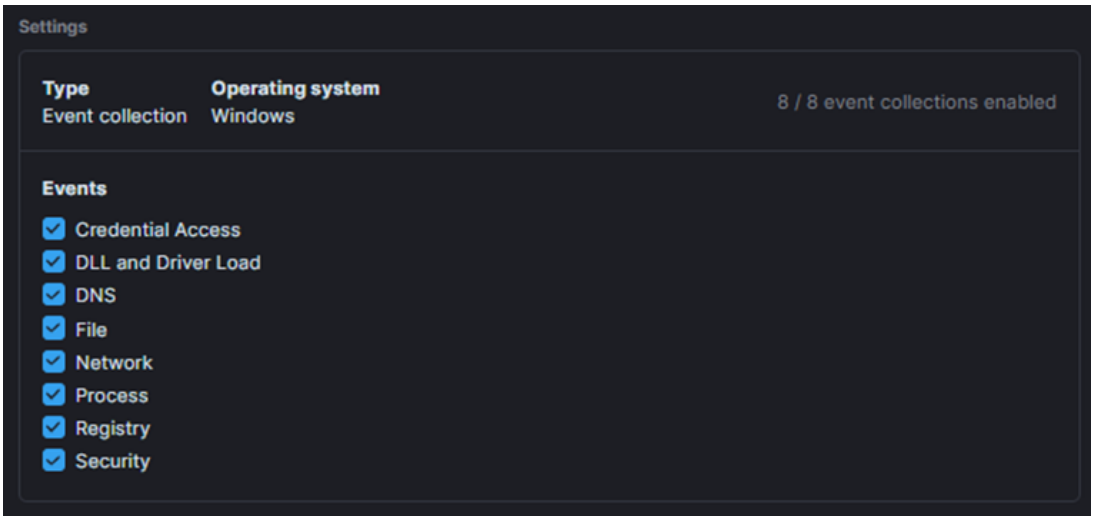


Imagen 6.7: Instalación Elastic Defend (III)

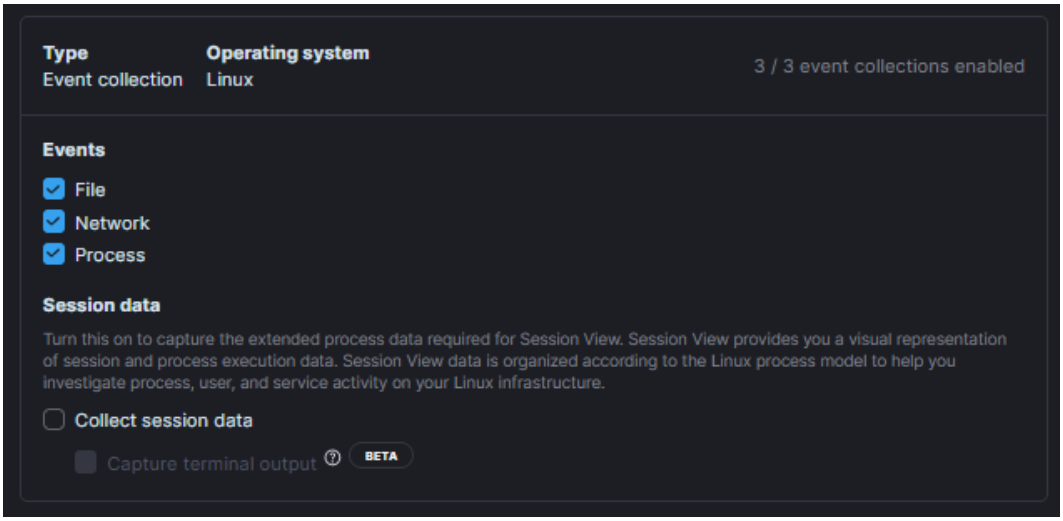


Imagen 6.8: Instalación Elastic Defend (IV)

Una vez configurada la política de la integración, es necesario activar el panel de Elastic Security en Kibana para poder monitorizar los datos que ofrece Elastic Defend y gestionar sus reglas de detección. Para ello hay que ir a Kibana → Stack Management → Spaces → modificar el espacio por defecto habilitando Elastic Security.

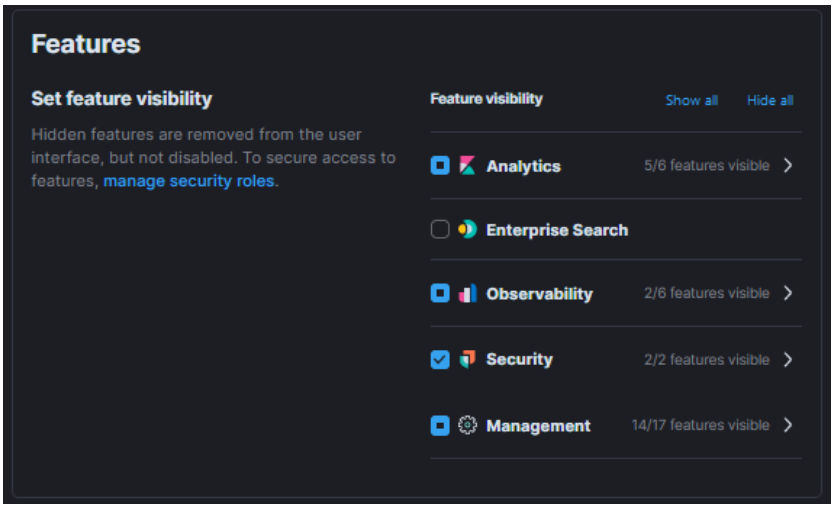


Imagen 6.9: Instalación Elastic Defend (V)

Una vez habilitado el panel Security hay que ir a Kibana → Security → Alerts → Manage Rules y activar las reglas correspondientes a Windows.

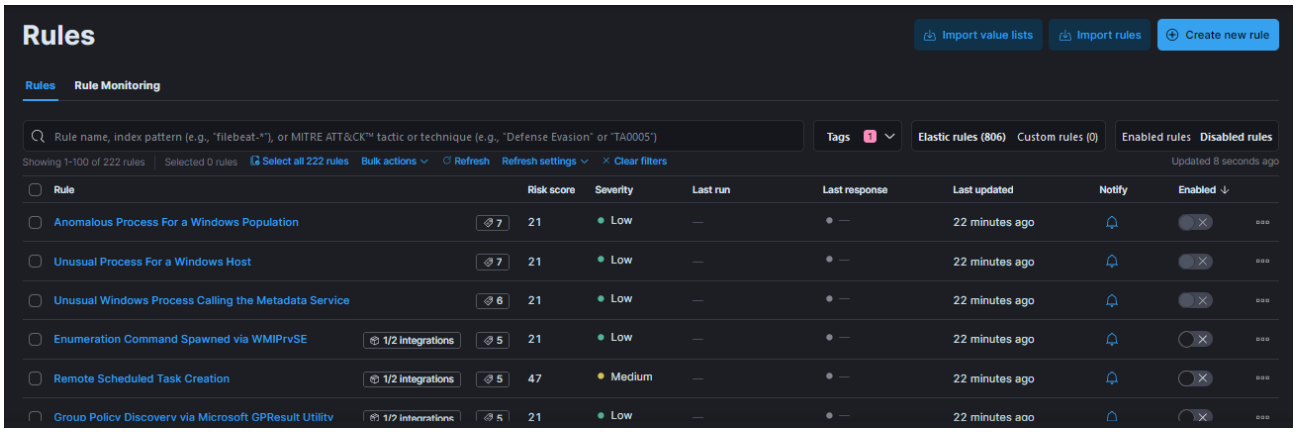


Imagen 6.10: Instalación Elastic Defend (VI)

Para verificar el correcto funcionamiento hay que ir a Kibana → Security → Alerts y ver que aparecen alertas a la hora de realizar alguna acción indebida.

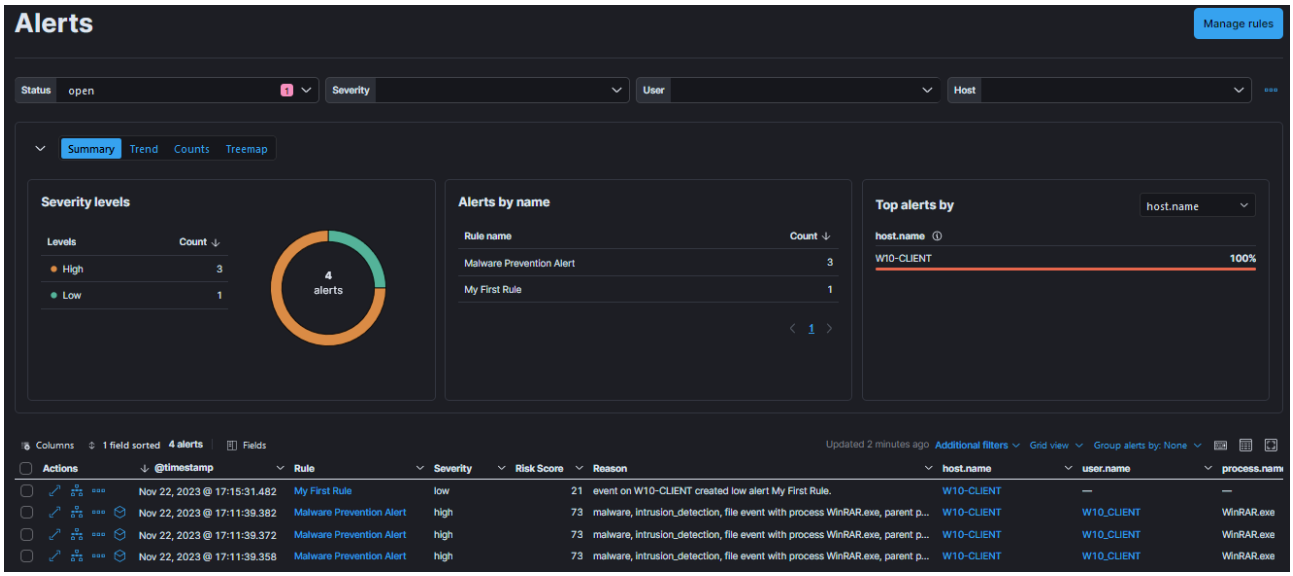


Imagen 6.11: Instalación Elastic Defend (VII)

6.1.3 Syslog de electrónica de red

Elastic Agent cuenta con diferentes integraciones para recibir syslog entre las cuales destacan las integraciones para sistemas específicos como pfSense o Fortinet. En este caso la integración se va a realizar para recopilar los logs del firewall virtual implementado mediante la máquina virtual de pfSense.

En este caso, el agente que va a recibir los logs de syslog es el que esta desplegado en el nodo manager-search. Para activar la integración hay que añadirla en la política de Elastic Fleet.

Desde Kibana → Fleet → Agent policies → so-grid-nodes_general → Add integration → pfSense → Add pfSense.

Durante el proceso de configuración de la política hay que especificar la IP de la interfaz que va a recibir los logs y el puerto que se va a utilizar que en este caso es UDP 9001.
Una vez configurada la integración hay que abrir el puerto de firewall de SO para aceptar tráfico UDP en el puerto 9001:

- Administration -> Configuration -> Firewall
- Activar las opciones avanzadas desde Options -> Interruptor
  - firewall -> hostgroups -> customhostgroup1 -> añadir IP de pfSense
  - firewall -> portgroups -> customportgroup1 -> añadir puerto 9001
  - firewall -> role -> managersearch -> chain -> DOCKER-USER -> hostgroups -> customhostgroup0 -> portgroups -> añadir customportgroup1

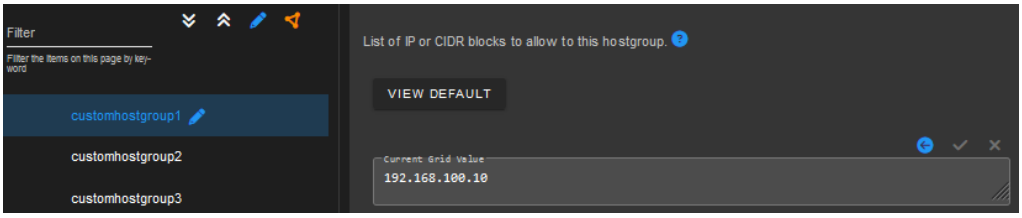


Imagen 6.12: Activación Syslog Firewall (I)

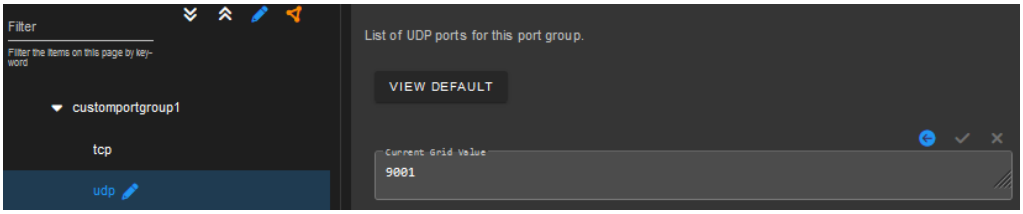


Imagen 6.13: Activación Syslog Firewall (II)

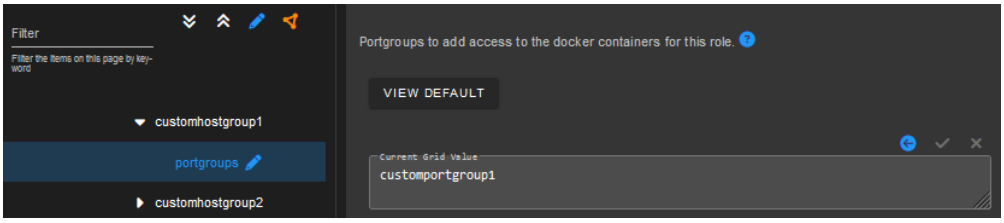


Imagen 6.14: Activación Syslog Firewall (III)

Una vez configurado el firewall hay que activar el envío de logs en el propio pfSense. Para ello desde la interfaz web de pfSense hay que ir a: Status → System Logs → Settings → Enable Remote Logging.

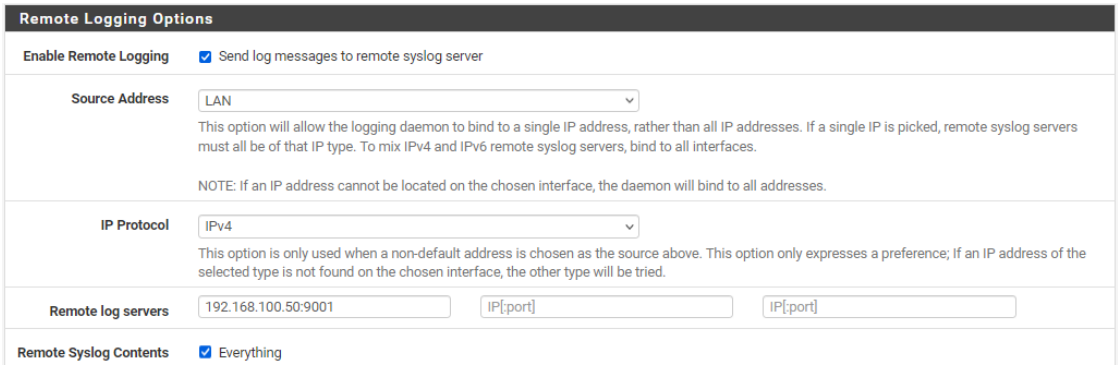


Imagen 6.15: Activación Syslog Firewall (IV)

Para finalizar la integración y poder ver los logs, es necesario crear la visualización específica para estos. Hay que ir a Stack Management -> Kibana (Data Viewes) -> Create Data View y crear una visualización con el nombre “pfSense” y el patrón “logs-pfsense.log-default”.

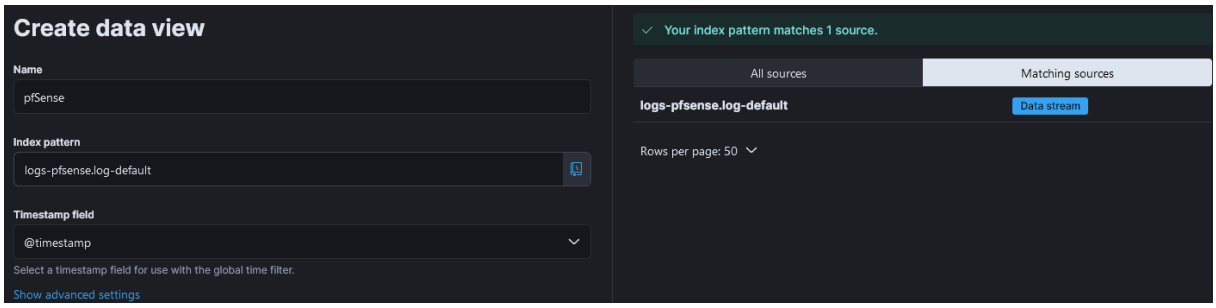


Imagen 6.16: Activación Syslog Firewall (V)

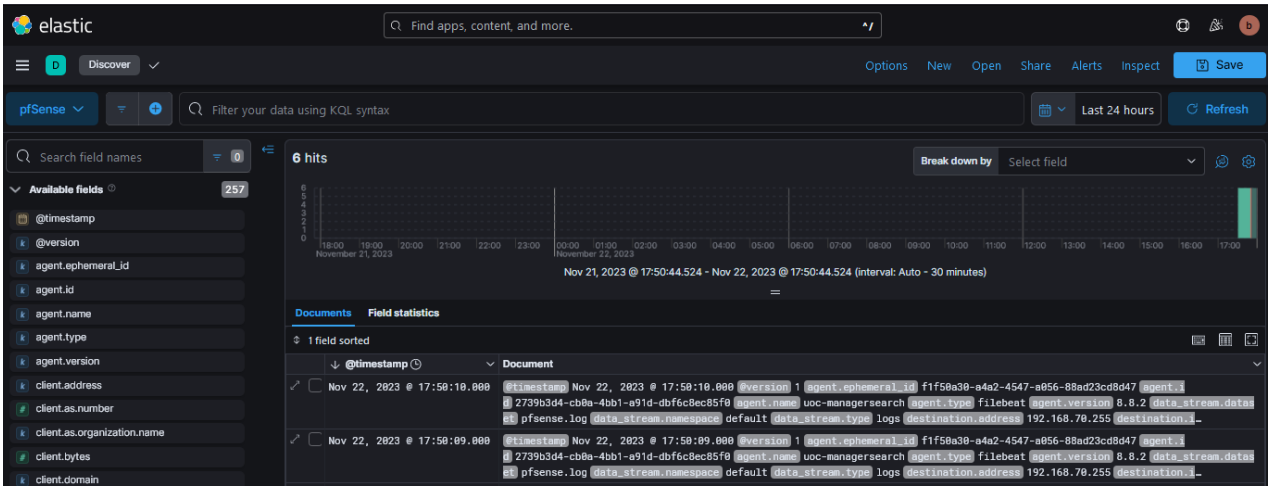


Imagen 6.17: Activación Syslog Firewall (VI)

6.2 Verificación consumo de los recursos del sistema.

Una vez desplegado el sistema de monitorización al completo incluidas las integraciones, es necesario verificar que el sistema esta correctamente dimensionado a nivel de recursos de hardware. En este caso al tratarse de un entorno de laboratorio se va a comprobar si los recursos definidos para las máquinas virtuales son suficiente para cubrir las pruebas de este trabajo.

Para poder ver el estado del sistema y el consumo de recursos, Security Onion dispone de la herramienta Grafana que se encarga de mostrar de forma gráfica el uso de recursos que hace cada nodo del sistema.

-Nodo manager-search:

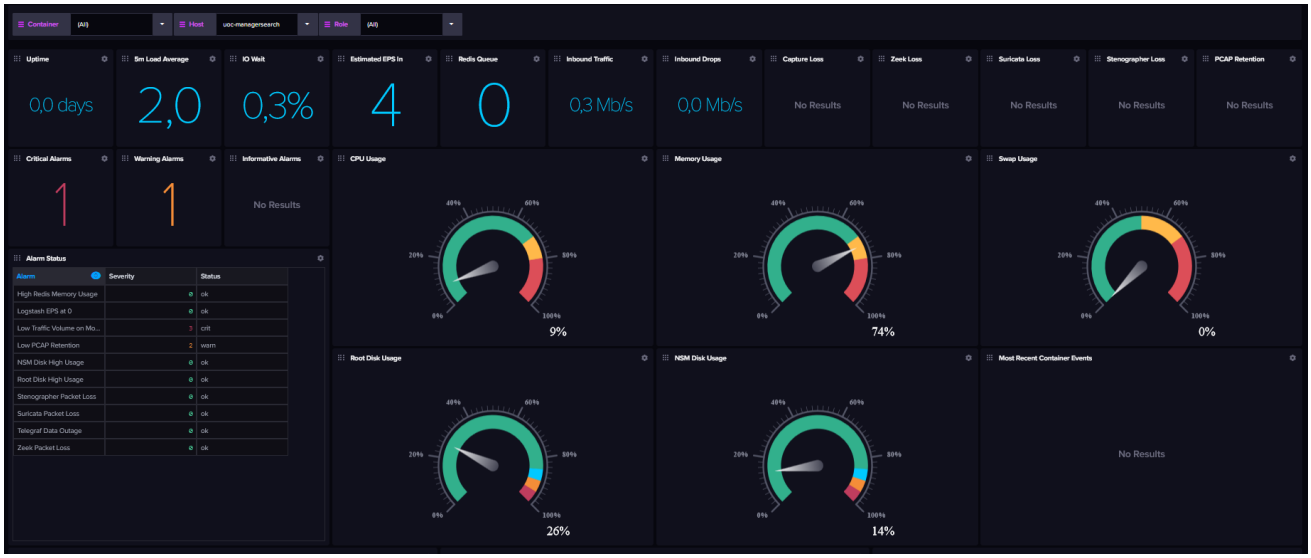


Imagen 6.18: Recursos nodo manager-search

A simple vista se puede ver que los recursos asignados al nodo manager-search son suficientes y el sistema cuenta con un buen margen de reserva. La única medida que tiene un menor margen de reserva es la memoria RAM ya que se trata de 16GB, que son suficientes para el ámbito de este trabajo, pero sería recomendable aumentar este valor hasta 20GB.

-Nodo forward:

Imagen 6.19: Recursos nodo forward

En caso del nodo-forward la asignación de recursos es la idónea ya que ninguna medida sobrepasa el 70% de uso y hay suficiente margen de reserva para los casos de sobrecarga del sistema a la hora de llevar a cabo diferentes pruebas.

7 Pruebas

En este apartado se va a realizar una serie de pruebas para verificar el correcto funcionamiento de las herramientas detección que componen el sistema de monitorización desplegado.

7.1 Análisis de logs y datos recopilados en condiciones normales y estudio de alertas generadas

Debido a que se trata de un entorno de laboratorio y que únicamente se dispone de 2 clientes (Windows y Ubuntu), el intervalo de tiempo escogido para el análisis es de 2 horas. Durante este tiempo se han ejecutado tareas de uso cotidiano de un equipo cliente dentro de una red domestica o corporativa. Entre estas tareas se encuentra actualización del sistema operativo, navegación, consulta de correo electrónico, uso de almacenamiento en la nube, descarga de archivos, etc.

7.1.1 Logs generados

Los logs generados por el sistema se pueden consultar desde el Dashboard de Kibana, en concreto desde Security Onion – Home. Durante el periodo de tiempo escogido, el sistema ha generado 322.313 logs de los cuales 48.852 corresponden a la actividad de la red (navegación, correo y descargas) y el resto son debidos a la operación normal de los equipos cliente (ejecución de aplicaciones, servicios, manejo de información) y los propios servidores de monitorización.

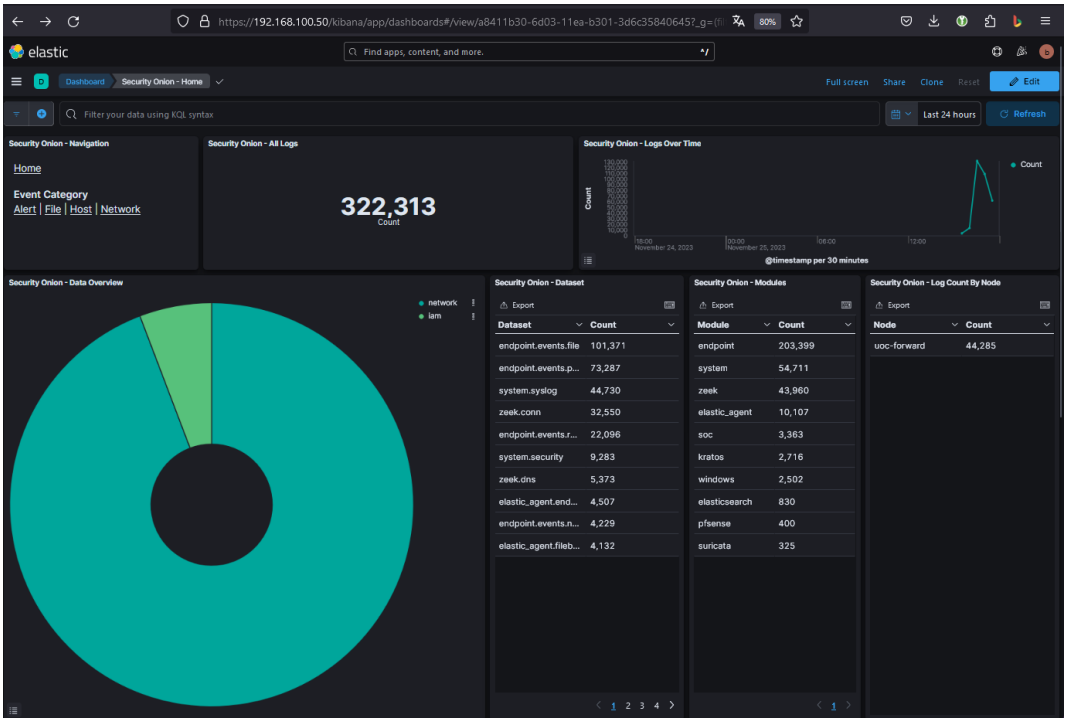


Imagen 7.1: Logs totales

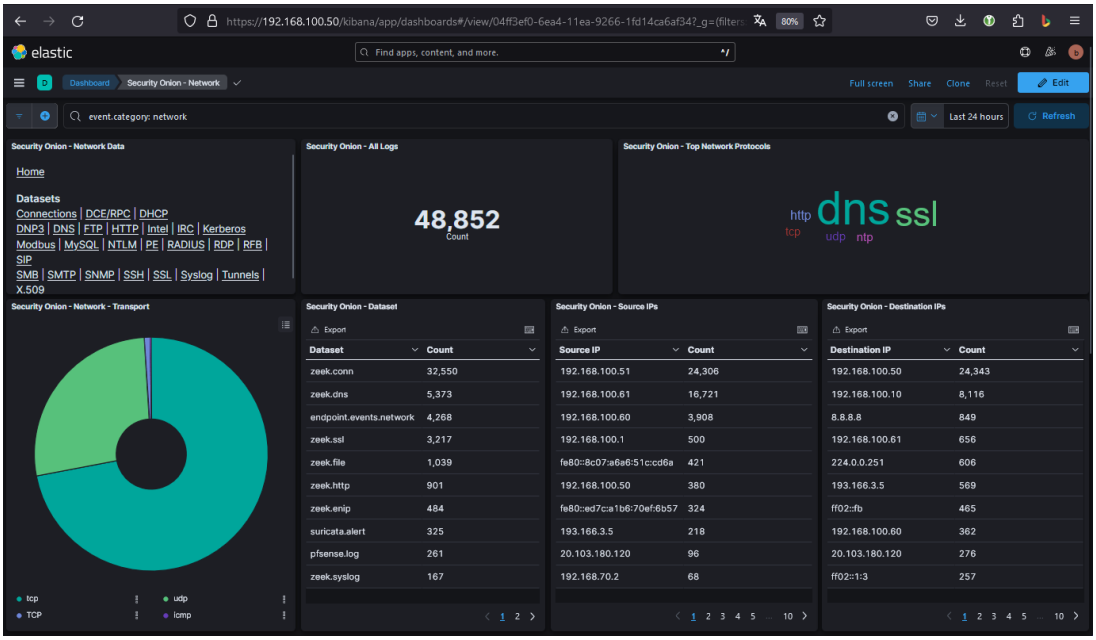


Imagen 7.2: Logs de red

Respecto a los logs generados en los clientes estos pueden consultarse desde el panel Security de Kibana.

Imagen 7.3: Logs de host

En cuanto a los logs generados por cada herramienta incluida en el sistema tenemos siguientes cifras.

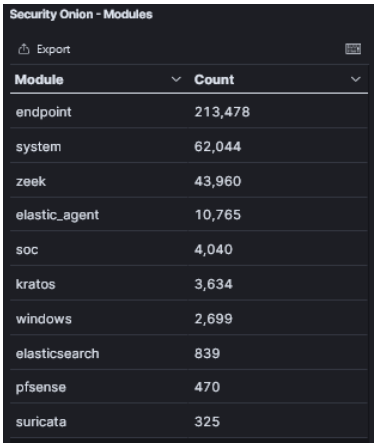


Imagen 7.4: Logs por herramienta

Otra forma de ver los logs es a través de los dashboards que ofrece SOC.

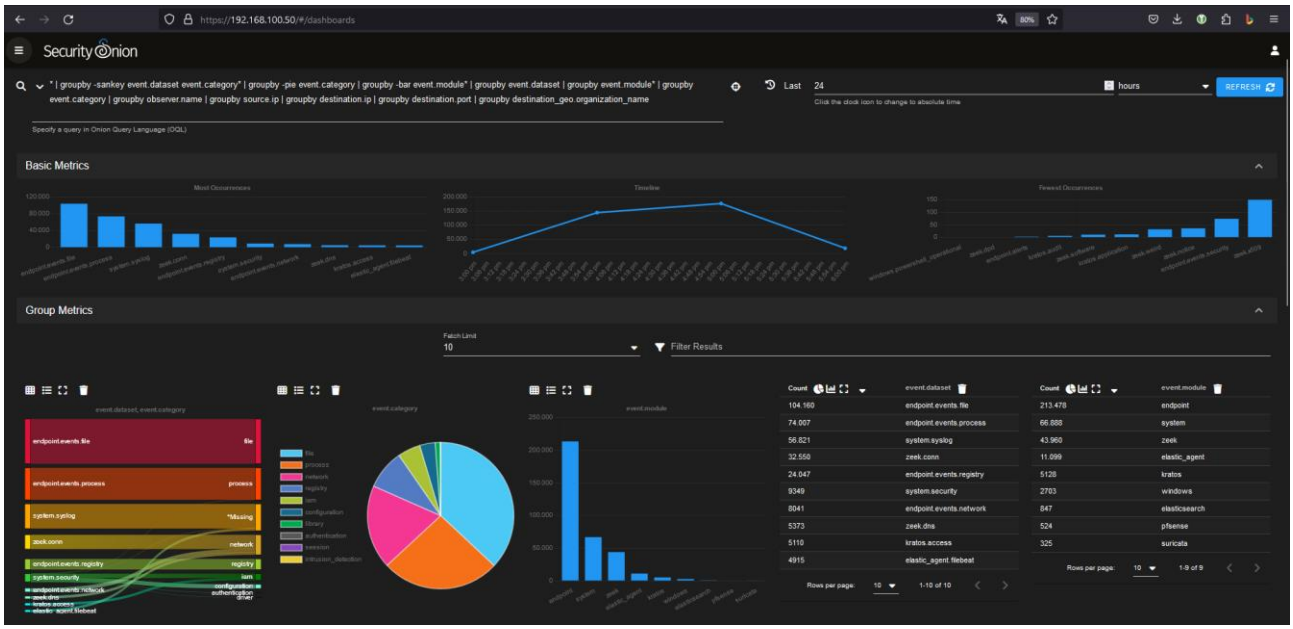


Imagen 7.5: SOC Dashboard

7.1.2 Estructura de logs

Los logs obtenidos se procesan y se guardan en el servidor para poder ser consultados. El formato habitual en el que se guardan es JSON. Cada log independientemente de la herramienta que lo haya generado se divide en diferentes campos de los que unos son comunes a todos los logs y otros varían según la herramienta empleada.

Los campos comunes son:

- Identificador del log (cadena alfanumérica única)
- Índice
- Versión
- Grupo fecha-hora
- Nodo que genera el log
- Herramienta que genera el log

Los campos variables en caso de logs de red son:

- Dirección IP y puerto de origen
- Dirección IP y puerto de destino
- Contenido
- Protocolo de red
- Flags
- Nº de paquetes enviados

Los campos variables en caso de logs de host son:

- Tipo de evento
- Usuario involucrado
- Directorio involucrado
- Datos del sistema operativo donde se produce (direcciones IP y MAC, nombre, etc.)

Si se trata de logs que muestran alertas, en este caso aparecen campos adicionales como:

- Severidad de la alerta (baja, media, alta)
- Regla que genera la alerta (nombre y contenido)
- Categoría de la alerta

7.1.3 Alertas generadas

Durante el periodo de tiempo escogido se han generado 325 alertas a nivel de red. De las cuales 300 son del supuesto tráfico no sospechoso, 16 del tráfico potencialmente malicioso y 9 de actividades varias sin categoría.

	Count	rule.name	event.module	event.severity_label
	2	ET DNS Query to a *.top domain - Likely Hostile	suricata	medium
	2	ET DNS Query for .cc TLD	suricata	medium
	12	ET INFO Observed DNS Query to .biz TLD	suricata	medium
	1	ET INFO Windows OS Submitting USB Metadata to Microsoft	suricata	low
	4	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	suricata	low
	4	ET INFO Observed DNS Query to Filesharing Service (mega .co .nz)	suricata	low
	300	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	suricata	low

Imagen 7.6: Alertas en el dashboard de SOC

Ninguna de estas alertas es crítica ya que su nivel de severidad es medio o bajo y son meramente informativas (etiqueta INFO en la descripción).

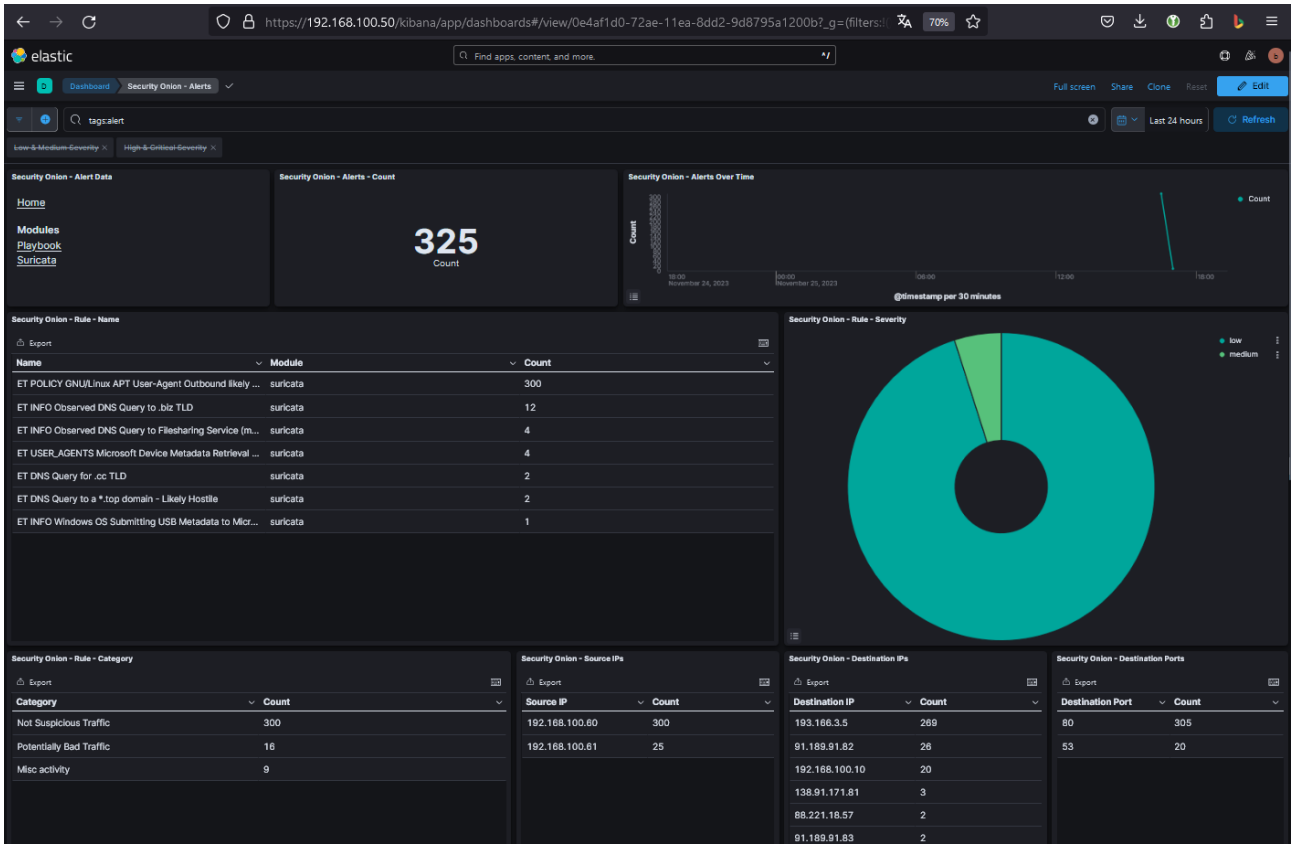


Imagen 7.7: Alertas de red

A nivel de host se han generado 50 alertas, de las cuales 3 se deben a la detección y prevención de un malware debido a la descarga de software sospechoso para activación de Windows 10, en este caso KMS Pico. El resto de las alertas no tienen mayor importancia ya que son falsos positivos que hay que ir filtrando con el tiempo y creando excepciones para eventos que son legítimos.

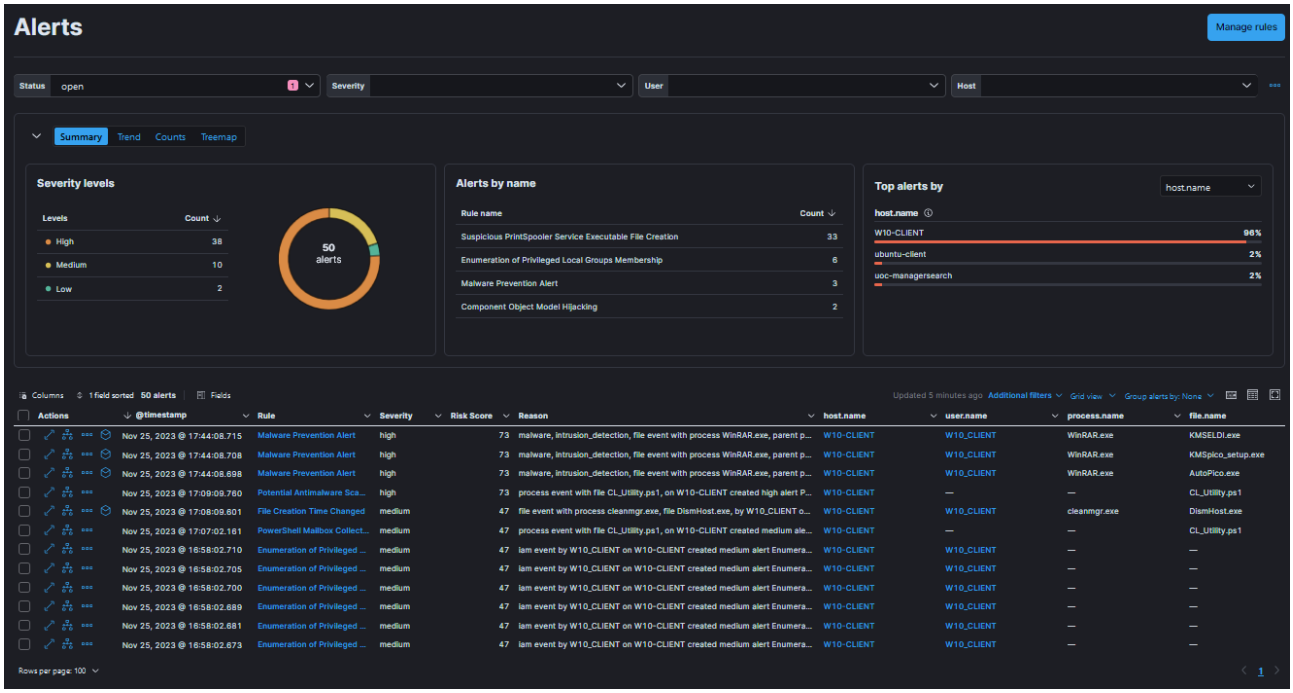


Imagen 7.8: Alertas de host

7.2 Ejecución de ataques básicos y análisis de alertas

Tras la monitorización del entorno en condiciones normales y el análisis de los datos obtenidos se va a realizar una serie de ataques con las herramientas que ofrece Kali Linux. Para ello se va a desplegar la máquina virtual con Kali Linux siguiendo el anexo X y se va a definir un conjunto de reglas para la detección de los ataques de prueba.

Para añadir las reglas personalizadas al sistema, es necesario ir a la consola web de SO. En concreto a Administration → Configuration → idstools → rules → Local Rules → escribir una regla por línea.

7.2.1 Detección de intentos de navegación hacia dominios maliciosos

En muchas ocasiones el ransomware intenta obtener las direcciones IP de sus servidores de mando y control mediante resoluciones de nombres de dominios maliciosos. En este caso, se va a definir una regla para la detección de cualquier petición de resolución de nombres a cualquier dominio .ru.

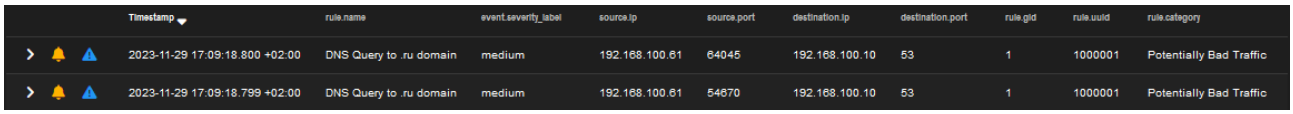
Por ejemplo, esta regla puede resultar muy útil para detectar la actividad de un gusano, del grupo de hackers ruso, conocido como “Little Drifter”. Los servidores a los que intenta conectarse ese gusano, todos residen en dominios rusos.

alert dns $HOME_NET any -> any any (msg:"DNS Query to .ru domain"; dns.query; content:".ru"; endswith; fast_pattern; classtype:bad-unknown; sid:1000001;)

Los campos que componen la regla son los siguientes:

- alert → indica que se debe generar una alerta cuando se cumple la condición.
- dns → especifica que la regla está relacionada con el tráfico DNS.
- $HOME_NET any → especifica que el origen de las consultas es nuestra red y el puerto de salida es cualquiera.
- any any → indica que la dirección IP y el puerto destino pueden ser cualesquiera.
- msg → es el mensaje que se registrará cuando se active la regla.
- dns_query → es el modificador de contenido que especifica que la regla debe coincidir con consultas DNS.
- content:".ru"; endwith; fast_pattern → comprueba la presencia de ".ru" al final de las consultas DNS y fuerza que la coincidencia se debe buscar rápidamente.
- classtype:bad-unknown → asigna una clasificación a la alerta, en este caso, "bad-unknown" que indica una actividad potencialmente maliciosa pero sin una clasificación específica.
- sid:1000001→ es el identificador único de la regla.

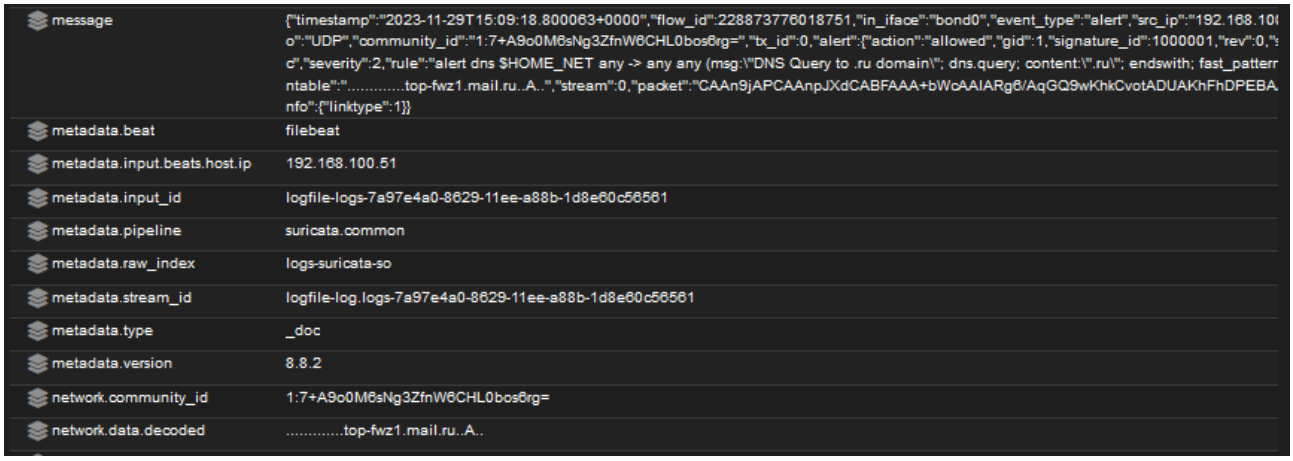
Para comprobar el funcionamiento de la regla se ha realizado navegación hacia paginas rusas aleatorias desde el cliente con Windows 10 y el resultado ha sido el siguiente.



	Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uuid	rule.category
>	2023-11-29 17:09:18.800 +02:00	DNS Query to .ru domain	medium	192.168.100.61	64045	192.168.100.10	53	1	1000001	Potentially Bad Traffic
>	2023-11-29 17:09:18.799 +02:00	DNS Query to .ru domain	medium	192.168.100.61	54670	192.168.100.10	53	1	1000001	Potentially Bad Traffic

Imagen 7.9: Navegación a dominios maliciosos (I)

Se puede observar que se ha generado la alerta correspondiente pudiendo identificar claramente el origen y el destino de la información. Para poder ver más datos al respecto y la propia consulta DNS es necesario desplegar la alerta.



message	{"timestamp":"2023-11-29T15:09:18.800063+0000","flow_id":228873776018751,"in_iface":"bond0","event_type":"alert","src_ip":"192.168.10(o":"UDP","community_id":"1:7+A9o0M6sNg3ZfnW6CHL0bos6rg=","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":1000001,"rev":0,"s c","severity":2,"rule":"alert dns $HOME_NET any -> any any (msg:\"DNS Query to .ru domain\"; dns.query; content:\".ru\"; endswith; fast_patterr ntable":".....top-fwz1.mail.ru..A..","stream":0,"packet":"CAAn9jAPCAAnpJXdCABFAAA+bWoAAIARg6/AqGQ9wKhkCvotADUAKhFhDPEBA nfo":{"linktype":1}}
metadata.beat	filebeat
metadata.input.beats.host.ip	192.168.100.51
metadata.input_id	logfile-logs-7a97e4a0-8629-11ee-a88b-1d8e60c56561
metadata.pipeline	suricata.common
metadata.raw_index	logs-suricata-so
metadata.stream_id	logfile-log.logs-7a97e4a0-8629-11ee-a88b-1d8e60c56561
metadata.type	_doc
metadata.version	8.8.2
network.community_id	1:7+A9o0M6sNg3ZfnW6CHL0bos6rg=
network.data.decoded	.....top-fwz1.mail.ru..A..

Imagen 7.10: Navegación a dominios maliciosos (II)

En el campo de “network.data.decoded” es posible identificar cual ha sido la consulta DNS realizada.

Otra forma de ver la misma información es a través de la interfaz web de Arkime.

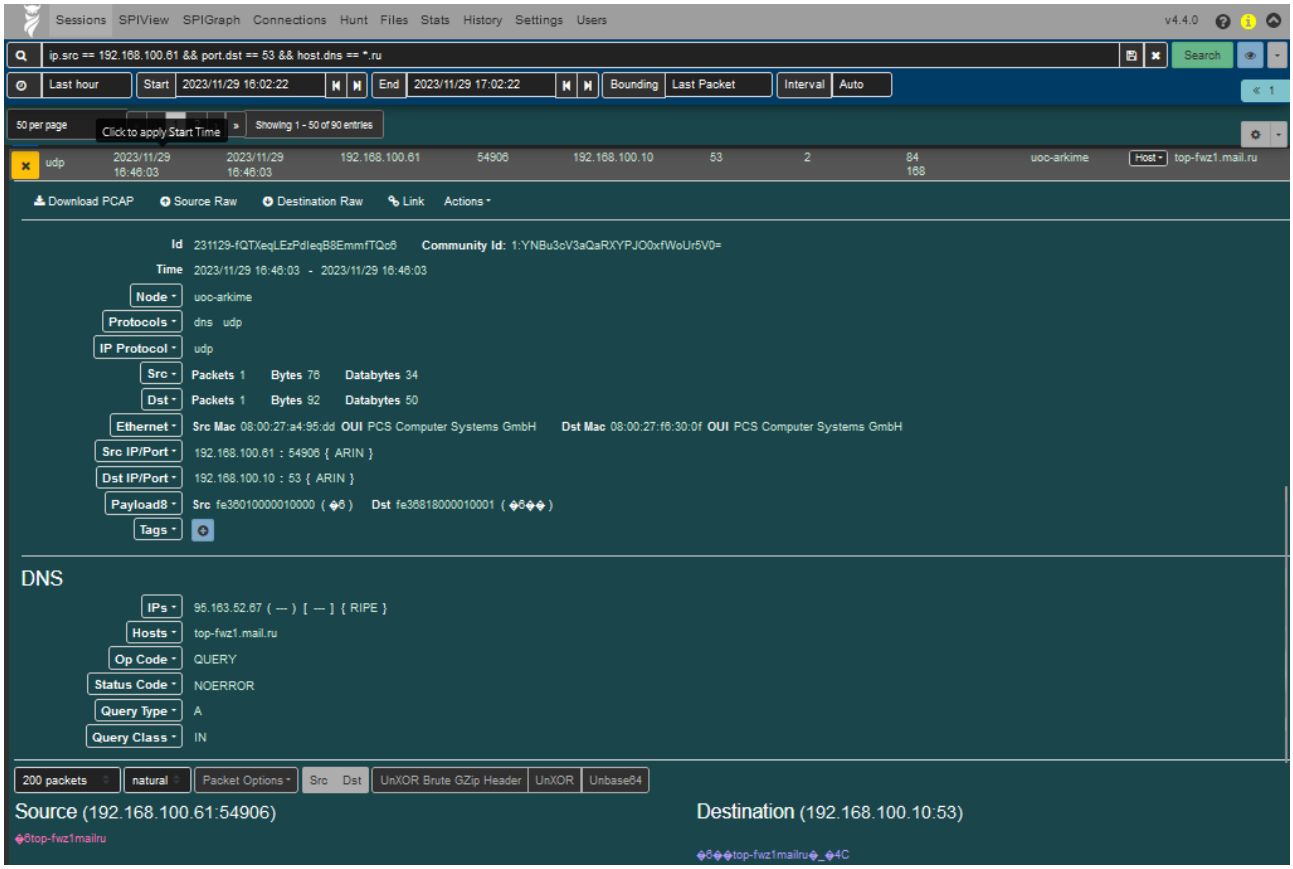


Imagen 7.11: Navegación a dominios maliciosos (III)

7.2.2 Detección de escaneo TCP con NMAP

Una de las técnicas que realizan los agentes maliciosos antes de atacar la red es el reconocimiento de la misma. Para ello se ejecutan diferentes escaneos de red con la herramienta NMAP incluida en la distribución de Kali Linux. En este caso, el escaneo que se va a realizar será enviando paquetes TCP con el flag SYN activo a diferentes puertos de aplicaciones bien conocidas. El comando a utilizar es:

nmap 192.168.100.0/24 -Pn -sS

Según la respuesta que reciba NMAP existen 3 estados de puerto:

- Si se recibe el paquete SYN/ACK, el puerto está abierto.
- Si se recibe un paquete RST, el puerto está cerrado.
- Si no se recibe respuesta, el puerto está filtrado.

La regla para la detección tendrá la siguiente sintaxis:

alert tcp any any -> $HOME_NET any (msg:"NMAP TCP Syn Scan"; flags:S,12; dsize :0; detection_filter: track by_src, count 20, seconds 60; classtype:attempted-recon; sid :10000002;)

Los campos que componen la regla son los siguientes:

- alert → indica que se debe generar una alerta cuando se cumple la condición.
- tcp → especifica que la regla está relacionada con el tráfico TCP.

- $EXTERNAL_NET any → especifica que el origen de las consultas es una red externa y el puerto origen es cualquiera.
- $HOME_NET any → indica que el destino es nuestra red y el puerto destino pueden ser cualquiera.
- msg → es el mensaje que se registrará cuando se active la regla.
- dsize:0 → verifica que el tamaño de la carga útil sea cero.
- flags:S,12 → verifica que se establezca la flag SYN y el valor de la flag TCP sea 12. El valor 12 representa que tanto la bandera SYN como la ACK están establecidas. Este es un patrón común visto en exploraciones TCP SYN.
- ack:0 → verifica que el número de acuse de recibo (ACK) en el encabezado TCP sea cero. En una exploración TCP SYN, la bandera ACK suele establecerse en cero.
- detection_filter: track by_src, count 20, seconds 60 → condición de umbral que ayuda a reducir falsos positivos. Especifica que, si ocurren 20 eventos que coinciden con esta regla dentro de una ventana de 60 segundos y comparten la misma dirección IP de origen, se activará una alerta.
- classtype:attempted-recon → es un tipo de clasificación que indica intento de reconocimiento.
- sid:1000002→ es el identificador único de la regla.

Para comprobar el funcionamiento de la regla se va a realizar un escaneo desde Kali Linux hacia toda la red del laboratorio.

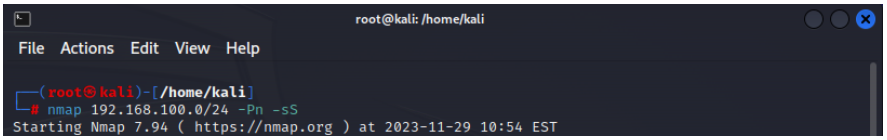


Imagen 7.12: Escaneo TCP con Nmap (I)

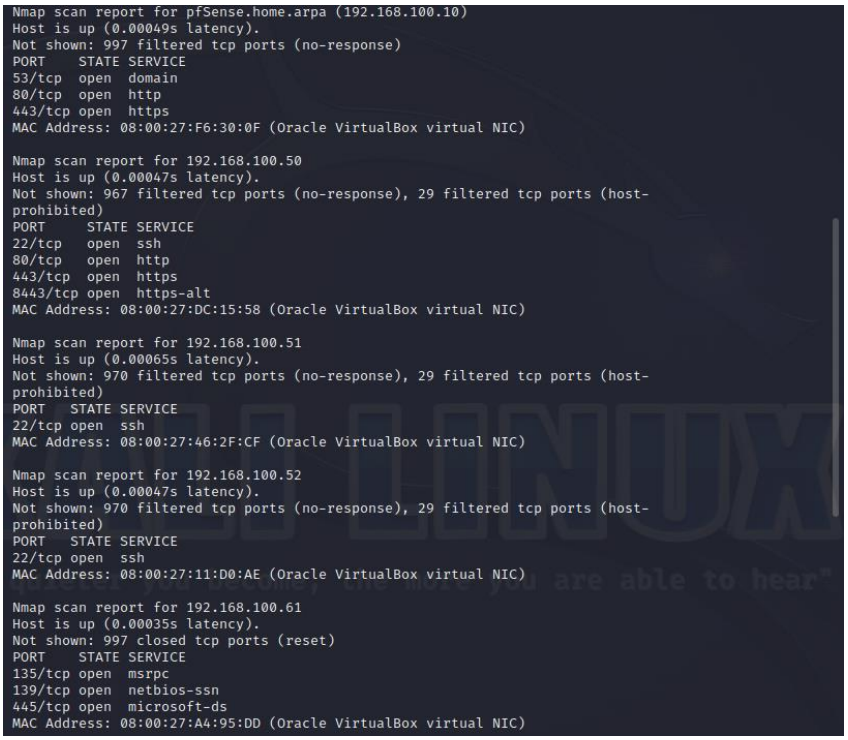


Imagen 7.13: Escaneo TCP con Nmap (II)

Se puede observar que se ha generado la alerta correspondiente pudiendo identificar claramente el origen y el destino del escaneo.

Imagen 7.14: Escaneo TCP con Nmap (III)

Al desplegar la alerta vemos cada transacción que se ha producido a diferentes puertos destino.

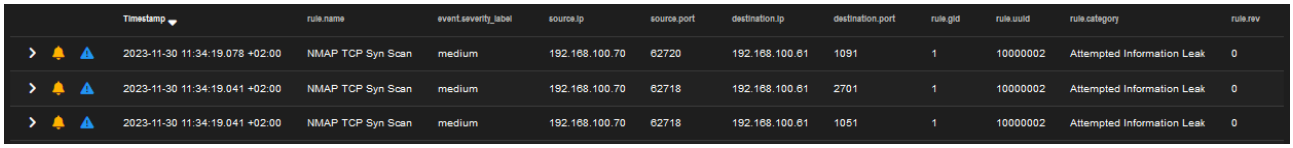


Imagen 7.15: Escaneo TCP con Nmap (IV)

En el detalle de cada consulta podemos ver que se trata flujo TCP.

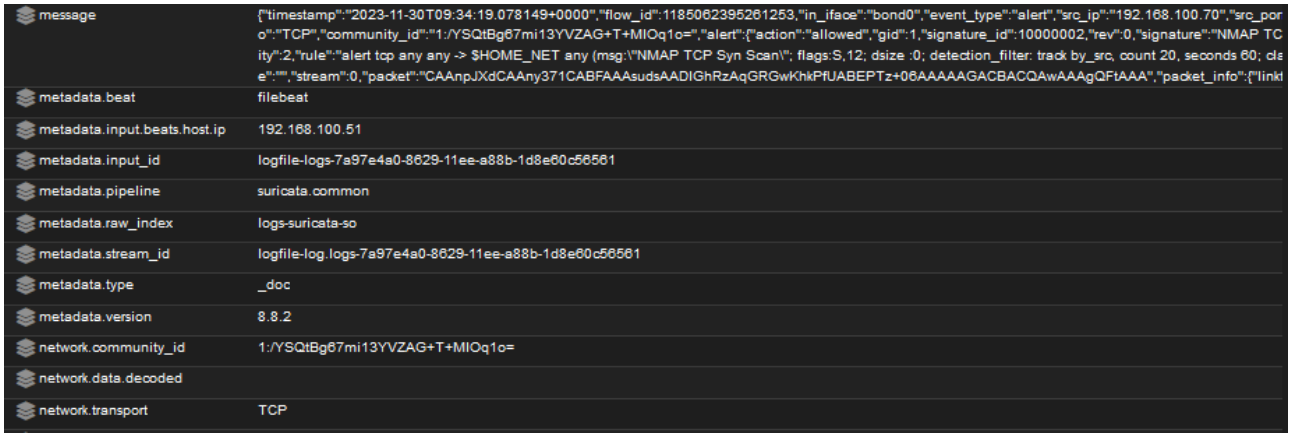


Imagen 7.16: Escaneo TCP con Nmap (V)

Finalmente, mediante Arkime se puede comprobar que efectivamente se trata de tráfico TCP sin carga útil y con el flag SYN activado.

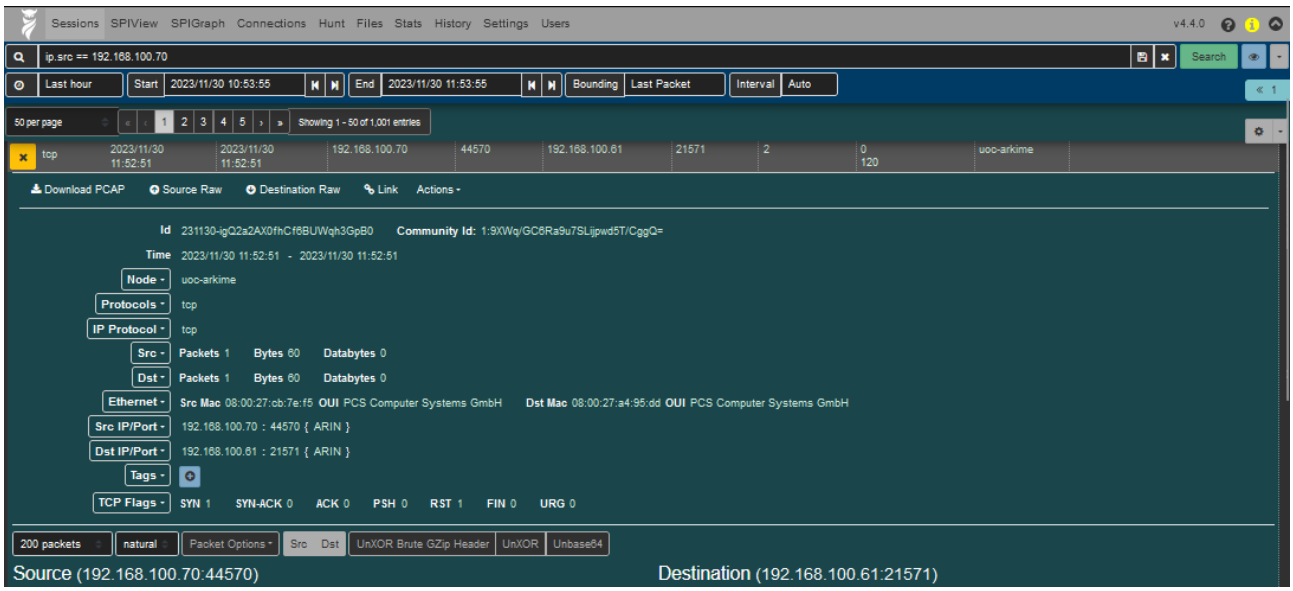


Imagen 7.17: Escaneo TCP con Nmap (VI)

7.2.3 Detección de fuerza bruta por SSH

Otro de los ataques muy comunes a los sistemas informáticos consiste en ganar acceso a los dispositivos por SSH mediante fuerza bruta. Kali Linux dispone de la herramienta HYDRA que permite usar listas de usuarios y contraseñas para realizar ataques de fuerza bruta hacia determinados equipos. Para detectar estos ataques se va a crear la siguiente regla de detección.

alert tcp any any -> $HOME_NET 22 (msg:"Possible SSH brute forcing!"; flags: S+; threshold: type both, track by_src, count 5, seconds 30; sid:10000001; rev: 1;)

Los campos que componen la regla son los siguientes:

- alert → indica que se debe generar una alerta cuando se cumple la condición.
- tcp → especifica que la regla está relacionada con el tráfico TCP.
- any any -> $HOME_NET 22 → se aplica a cualquier dirección IP de origen y cualquier puerto de origen, con destino al puerto 22 (SSH) en la red interna.
- msg → el mensaje que se registrará cuando se active la regla.
- flags: S+ → Verifica que se establezca la bandera SYN en el encabezado TCP (S+ indica SYN).
- threshold: type both, track by_src, count 5, seconds 30 → condición de umbral que ayuda a reducir falsos positivos. Indica que si hay 5 eventos que coinciden con esta regla dentro de una ventana de 30 segundos y comparten la misma dirección IP de origen, se activará una alerta.
- sid:10000003 → identificador único de la regla.

Para verificar el funcionamiento se realiza el ataque con Hydra al nodo manager-search usando el comando:

hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz 192.168.100.50 ssh -t 4

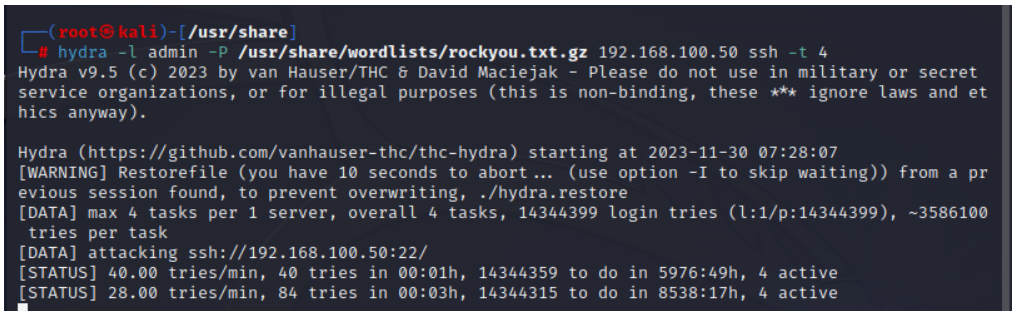


Imagen 7.18: Fuerza bruta vía SSH (I)

Al ejecutar el ataque se genera alerta en el Security Onion, indicando direcciones IP involucradas y los puertos.

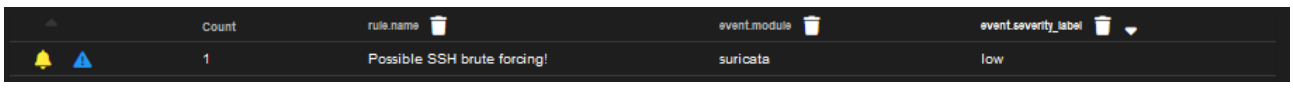


Imagen 7.19: Fuerza bruta vía SSH (II)

Imagen 7.20: Fuerza bruta vía SSH (III)

En este caso, Arkime ofrece información complementaria como los flags activados o la versión de SSH.

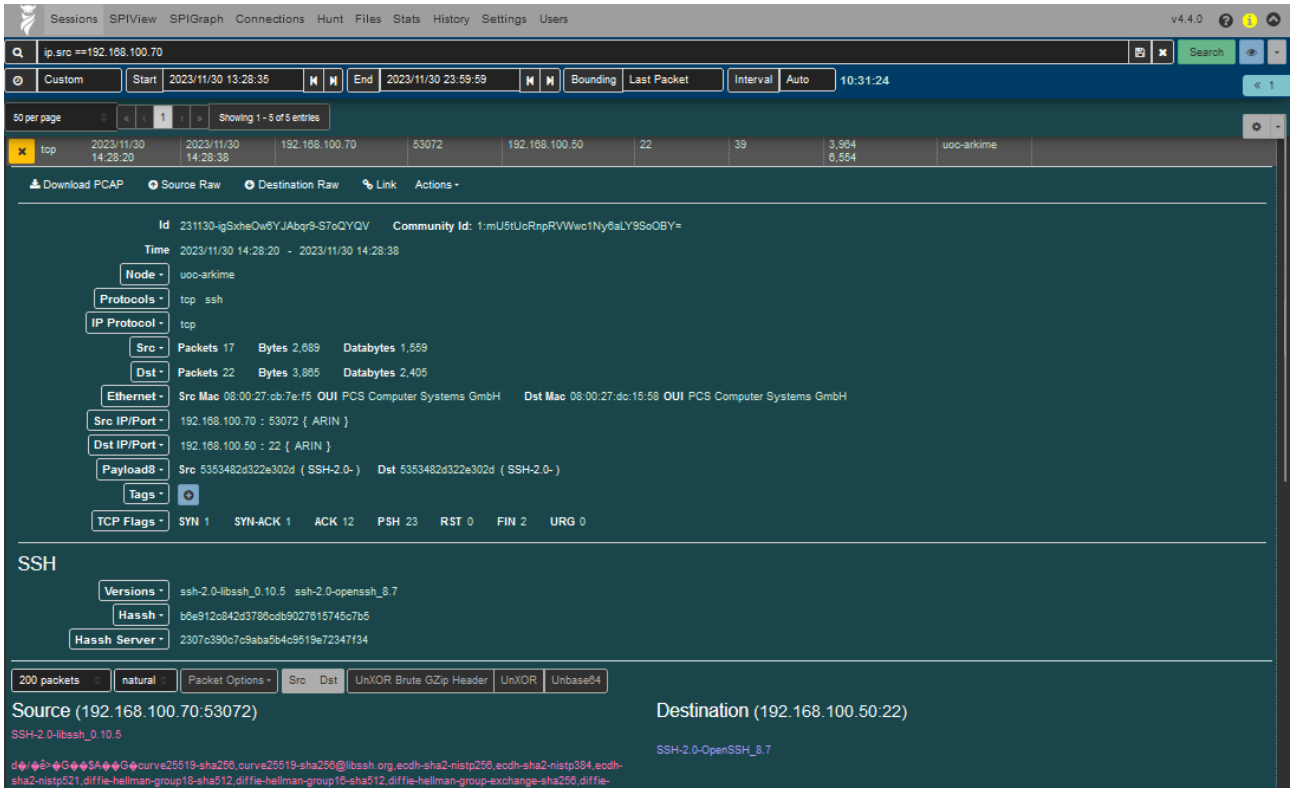


Imagen 7.21: Fuerza bruta vía SSH (IV)

7.2.4 Detección de un intento de denegación de servicio mediante paquetes SYN

Tal y como se ha explicado al principio de este trabajo, los ataques DoS y DDoS son muy frecuentes para interrumpir el funcionamiento de los servicios de una empresa con el fin de generar pérdidas económicas o de confianza. Estos ataques normalmente consisten en inundación de un determinado servidor con paquetes TCP o UDP. Para llevar a cabo este ataque se usará la herramienta Hping3 también disponible en Kali Linux. En cuanto a la detección de un ataque de este tipo se define la siguiente regla.

alert tcp any any -> $HOME_NET any (msg:"DoS via TCP SYN"; flags:S; dsize:0; detection_filter:track by_dst , count 500, seconds 5; classtype:attempted-dos; sid:1000004;)

Los campos que componen la regla son los siguientes:

- alert → indica que se debe generar una alerta cuando se cumple la condición.
- tcp → especifica que la regla está relacionada con el tráfico TCP.
- any any -> $HOME_NET any → se aplica a cualquier dirección IP de origen y cualquier puerto de origen, con destino a cualquier puerto en la red interna.
- msg → el mensaje que se registrará cuando se active la regla.
- flags: S → verifica que se establezca la bandera SYN en el encabezado TCP.
- dsize :0 → indica el tamaño de la carga útil.
- detection_filter:track by_dst , count 500, seconds 5 → condición de umbral que ayuda a reducir falsos positivos. Indica que, si hay 500 eventos que coinciden con esta regla dentro de una ventana de 5 segundos y comparten la misma dirección IP de destino, se activará una alerta.
- sid:10000004 → identificador único de la regla.

Para verificar el funcionamiento se realiza el ataque con HYDRA al nodo manager-search usando el comando:

hping3 --rand-source -S --flood 192.168.100.61

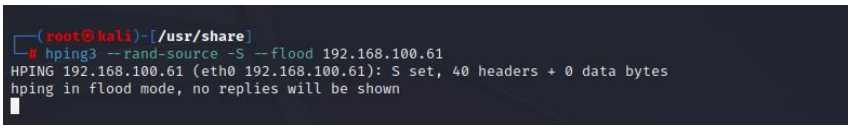


Imagen 7.22: Denegación de servicio (I)

Al ejecutar el ataque se generan alertas en el Security Onion, indicando direcciones IP involucradas y los puertos. Se ve que el ataque simula diferentes direcciones IP de origen que hacen peticiones a la única dirección IP objetivo.

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid
2023-11-30 16:02:40.494 +02:00	DoS via TCP SYN	medium	254.105.118.129	24652	192.168.100.61	0	1
2023-11-30 16:02:40.494 +02:00	DoS via TCP SYN	medium	225.93.76.175	24651	192.168.100.61	0	1
2023-11-30 16:02:40.494 +02:00	DoS via TCP SYN	medium	217.39.12.237	24650	192.168.100.61	0	1
2023-11-30 16:02:40.493 +02:00	DoS via TCP SYN	medium	7.148.90.243	24649	192.168.100.61	0	1
2023-11-30 16:02:40.493 +02:00	DoS via TCP SYN	medium	67.127.217.19	24648	192.168.100.61	0	1
2023-11-30 16:02:40.493 +02:00	DoS via TCP SYN	medium	147.102.226.84	24647	192.168.100.61	0	1

Imagen 7.23: Denegación de servicio (II)

Quedando agrupadas en único aviso en el panel para su mejor visualización.

Count	rule.name	event.module	event.severity_label
24.764	DoS via TCP SYN	suricata	medium

Imagen 7.24: Denegación de servicio (III)

A su vez Arkime muestra un considerable aumento de tráfico en el momento de ejecución del ataque.

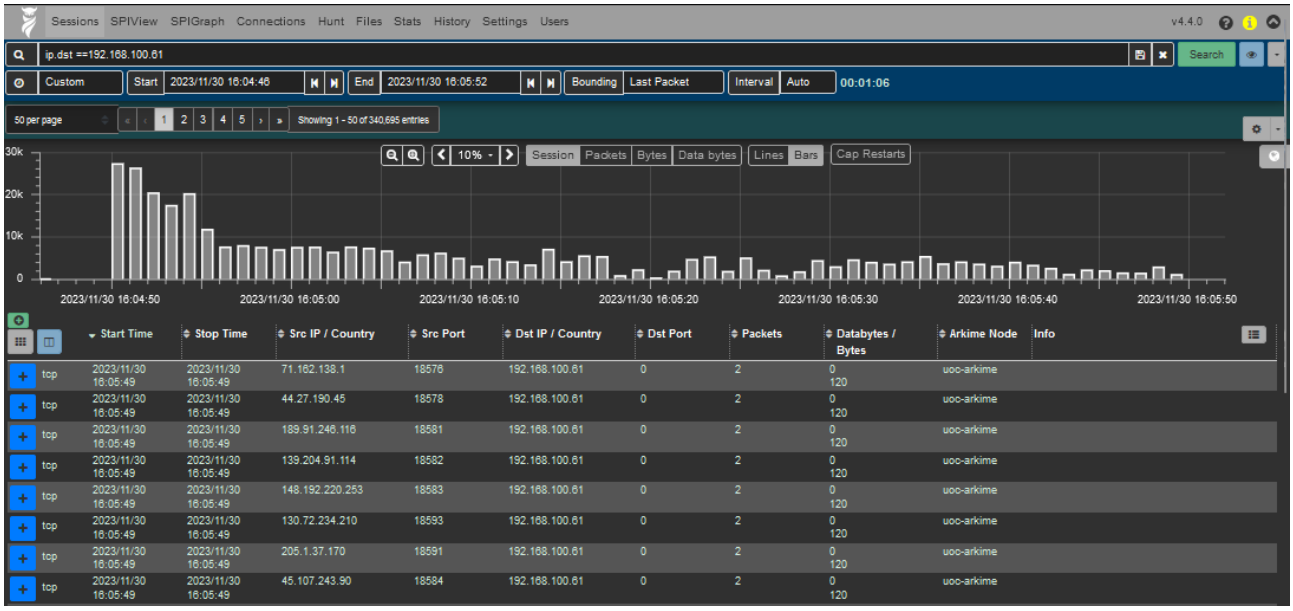


Imagen 7.25: Denegación de servicio (IV)

7.2.5 Detección de ejecución de malware en un host

En este caso el incidente se debe a la ejecución de un archivo .exe malicioso descargado desde una página web. El archivo es generado mediante el módulo Msfvenom de la herramienta Metasploit disponible en Kali Linux. El objetivo del ejecutable es pasar por un archivo de actualización de un videojuego y al ejecutarse abrir una “reverse shell” hacia el equipo atacante. Para poder llevar a cabo las pruebas han sido desactivados tanto el firewall como el antivirus del Windows 10 ya que en caso contrario el archivo seria eliminado antes de la ejecución.

Antes de la ejecución se activa el playbook nº 246 del módulo Playbook de SO. Para ello hay que dirigirse desde la consola web de SO a Playbook, en la interfaz de Playbook hay que localizar el “play” relacionado con Metaspoit y activarlo. De esta manera cuando se detecte el uso de Metasploit, se generará una alerta mediante la herramienta Elastalert.

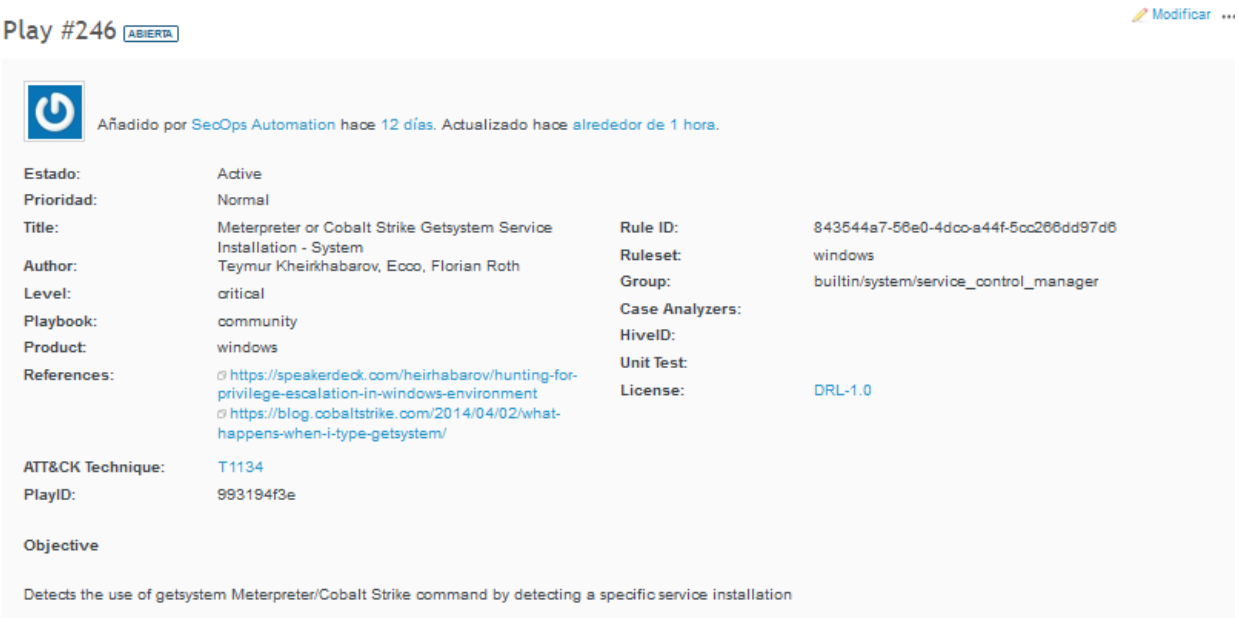


Imagen 7.26: Ejecución de malware (I)

Tras la ejecución del archivo .exe maliciosos en la consola de web de Security Onion se generan las siguientes alertas.

	Count	rule.name	event.module	event.severity_label
	2	ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	suricata	high
	4	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
	2	Meterpreter or Cobalt Strike Getsystem Service Installation - System	playbook	critical
	1	SUSP_Imphash_Mar23_2	strelka	high

Imagen 7.27: Ejecución de malware (II)

La primera alerta indica que se han detectado datos construidos con Metasploit y que el origen de la conexión es la IP de Kali Linux.

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
2023-11-30 17:31:54.299 +02:00	ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	high	192.168.100.70	4444	192.168.100.61	50417
2023-11-30 17:18:40.375 +02:00	ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	high	192.168.100.70	4444	192.168.100.61	49968

Imagen 7.28: Ejecución de malware (III)

Los datos decodificados no aportan ninguna aclaración.

network.data.decoded	V...Y.V.U.Y...t ...t.....u..E..G'....u..E..Gd3.....U...U..".."..V.u.9rtk.....E..;.r.k...M.;.s.9r.u.....3.^].U...E.....].U..VW.}...t..M...t..U...u.3.f...r..j.^.0.....^]...f.>.t....lu...t.+....f....R.f..t.lu.3....u.f.....j"..U...U..M.V..u..u9M.u&3..3..t..E...t...u.3.f.3.f.....[..{.....u..E.3.jPf.TA.X..3.f...p...j".U...E...x!...~...u.....].-<.....].U...$.@...3..E..E.S.....VW.E.3..E.V.E.....}.....E.95.....h....VhP*.....u&.....W.j...VVhP*.....S...hh*..W.....?....P.....}.....t..E...t.P.....9u.t.j.X....9u.t..5.....j.....;.tO9=....tGP..5....E....M..E...t/..t+....t..M.Qj..M.Qj.P.U...t..E..u..}.....0.....t$P....t.....t.....;.t.P....t.V....}..5.....t.W.u..u.V....3..M._^3.[.V....].%(....U..Y.F ;....t.P..].Y.F$;....t.P..].Y.F8;....t.P..].Y.F<;....t.P..].Y.F@.....t.P.p].Y.FD;....t.P.^].Y.FH;....t.P.L].Y.FL;.$...t.P.:].Y^}.U..V.u...tY.;....t.P..].Y.F.;....t.P..].Y.F;....t.P..\.Y.F0;....t.P..\..Y.F4;....t.P..\..Y^}.U..V.u4.Y\...v..Q\...v8.I\...v<.A\....@.v@.6\...vD..\...vH.&\...vL..\...vP..\...vT..\...vX..\...v\..[...v'..[...vd..[...vh..[...vl..[...vp..[...vt..[...vx..[...v|..[....@.....[.....[.....[.....[.....[.....[.....y[.....n[.....q[.....X[.....M[..Z.....Z.....Z.....Z.....Z.....Z.....Z.....Z.....Z.....yZ.....nZ.....cZ.....XZ....@.....JZ.....?Z.....4Z.....]Z.....Z.....Z.....Z...$....Y....(....Y.....Y....0....Y....4....Y....8....Y..Y....\....Y....'....UY....^].U..QQ.@...3..E.SV.u.W.~!.E...I.8.t.@..u.....+.H;..p.|....M$3...u.E....@....E$3.9E{j.j.V.u.....PQ.....M...u.3..q...~Wj.3.X.....rK...A.;.v?.E..E....=....w...<.....t.....P..X....Y..t.....M....\u.VS.u..u.....~Oj.3.X....rC..?.A.;.v9..}....=....w...<.....tg.....P..W....Y..tR.....3....tA.E.WVPS.u..u.....t!3.PP9E u.PP...u .u.WVP.u$.....V.d...YS.]...Y...e._^[.M.3..g.....].U.....u..M...b...u(.E..u$.u .u..u.3...u.E....@....E.W3.9E W.u....u.....PQ.....u.3.....~K....wC...A.;.v9..]...=....w.....t.....P.V...Y..t.....t...PWV._....SV.u..u j..u.....t..u.PV.u.....V....Y...e._^[.M.3.....].U.....u..M..1a...u .E..u..Y].U....$...j...c....t.j.Y.).....5.....=....f.....f.....f.....f.....f.%...f.-.....E.....E.....E.....@.....j.Xk.....j.Xk...@....L..j.X....D....L..h.2.....].U..SVW3.....;.+....jU.4.:...@...t.3.QQQ.u..u..u..u..u..u..]..u..u..u..u..u..u.....YP.....].U..V.u.3...t^.M.SW.}.jA[jZZ+..U...jZZ....f,.rf;.w.....f..r.f:E.w.....Nt f..t.f,.t.....+.[^].$...Vj.^.u.....;.}....$...j.P.....YY..u.j.V.5$.....YY..u.j.X^.3..8.....R.....}..3.^..%6...=D....t..37...5 .....R...% ....Y..8....U..V.u..8....;.r"....w...+.....P.i....N.....Y. .F P..d...^].U...E....}....P.>....E.Y.H.....].E...P..d...].U...E..8....;.r=....w..'....+.....P.a...Y]...
network.transport	TCP
observer.name	uoo-forward
rule.action	allowed
rule.category	A Network Trojan was detected

Imagen 7.29: Ejecución de malware (IV)

La segunda alerta indica que se ha producido la descarga de un archivo ejecutable a través de una página web que trabaja con el protocolo HTTP (puerto 80) lo que resulta sospechoso siendo lo habitual el uso de conexiones HTTPS (puerto 443) cuando se trata de página legitimas.

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uuid
2023-11-30 17:31:37.558 +02:00	ET POLICY PE EXE or DLL Windows file download HTTP	high	192.168.100.70	80	192.168.100.61	50408	1	2018959
2023-11-30 17:18:22.267 +02:00	ET POLICY PE EXE or DLL Windows file download HTTP	high	192.168.100.70	80	192.168.100.61	49962	1	2018959

Imagen 7.30: Ejecución de malware (V)

En este caso, los datos decodificados muestran la respuesta HTTP 200/OK procedente del servidor del atacante hacia la maquina víctima.

network.data.decoded	HTTP/1.1 200 OK Date: Thu, 30 Nov 2023 15:18:21 GMT Server: Apache/2.4.57 (Debian) Last-Modified: Thu, 30 Nov 2023 15:10:08 GMT ETag: "1204a-60b600c21a01d" Accept-Ranges: bytes Content-Length: 73802 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program MZ.....@.....!..L.!This program cannot be run in DOS mode. $.....8...Y...Y...E...Y..TE...Y...F...Y...F...Y...Y...Y..TQ...Y...z...Y..._...Y..Rich.Y.....PE..L.....rJ.....@.....`.....I...x....P..... @.....
network.transport	TCP

Imagen 7.31: Ejecución de malware (VI)

La tercera alerta es generada por el módulo Playbook tal y como estaba planeado. Al establecerse una “reverse Shell” y materializarse la elevación de privilegios se cumplen los criterios de la regla de Elastalert y aparece la notificación correspondiente.

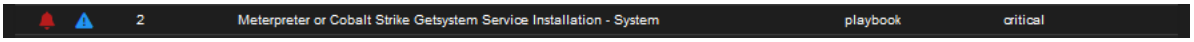


Imagen 7.32: Ejecución de malware (VII)

Imagen 7.33: Ejecución de malware (VIII)

La cuarta alerta es generada por el módulo Strelka. La información que ofrece consiste en el análisis detallado del archivo ejecutable descargado, los diferentes hashes, la entropía, los metadatos, etc. Posteriormente estos datos pueden ser verificados en la plataforma www.virustotal.com.

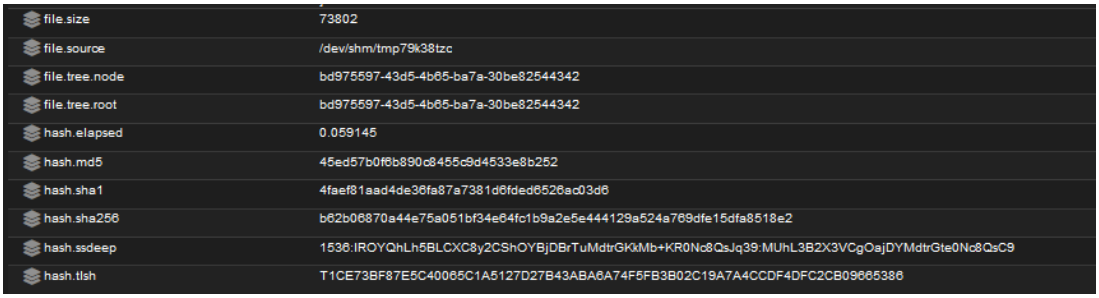


Imagen 7.34: Ejecución de malware (IX)

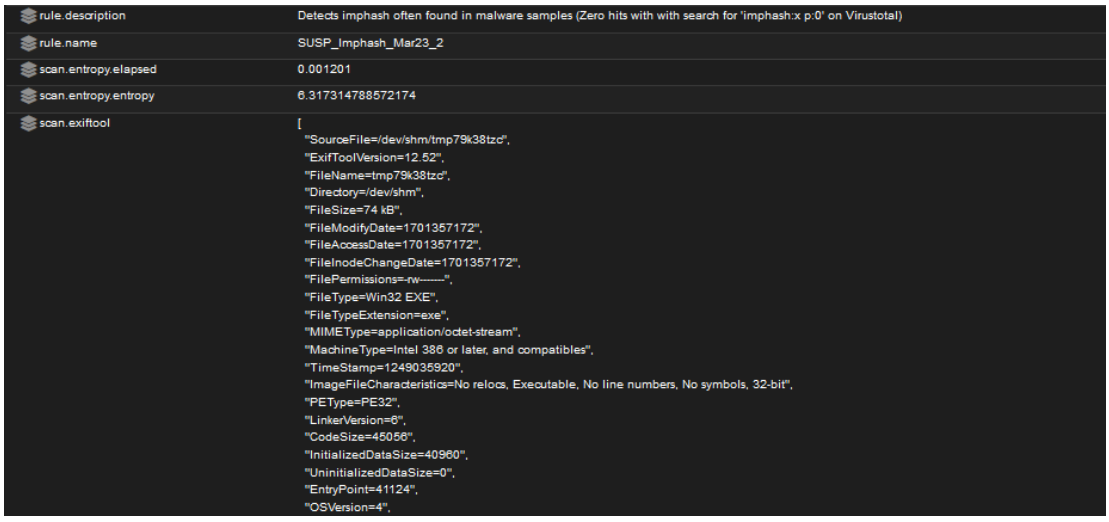


Imagen 7.35: Ejecución de malware (X)

A parte de las 4 alertas generadas a nivel de NIDS, también se ha generado una alerta por parte de HIDS gracias a las reglas de Elastic Defend.

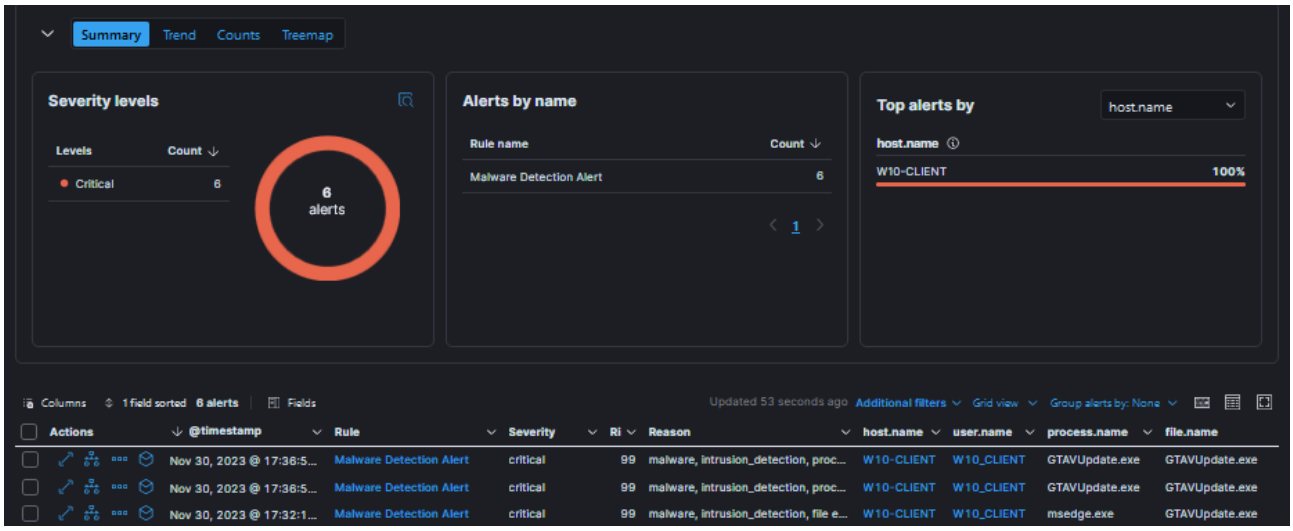


Imagen 7.36: Ejecución de malware (XI)

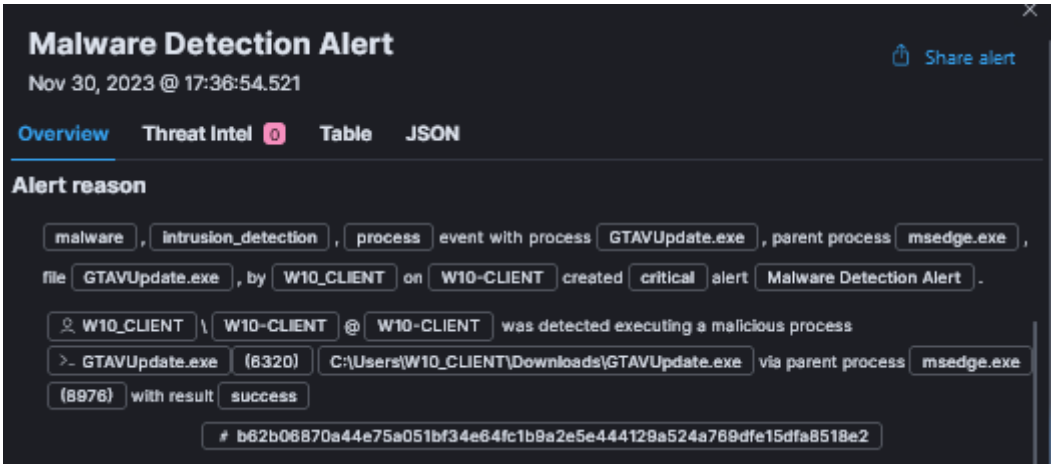


Imagen 7.37: Ejecución de malware (XII)

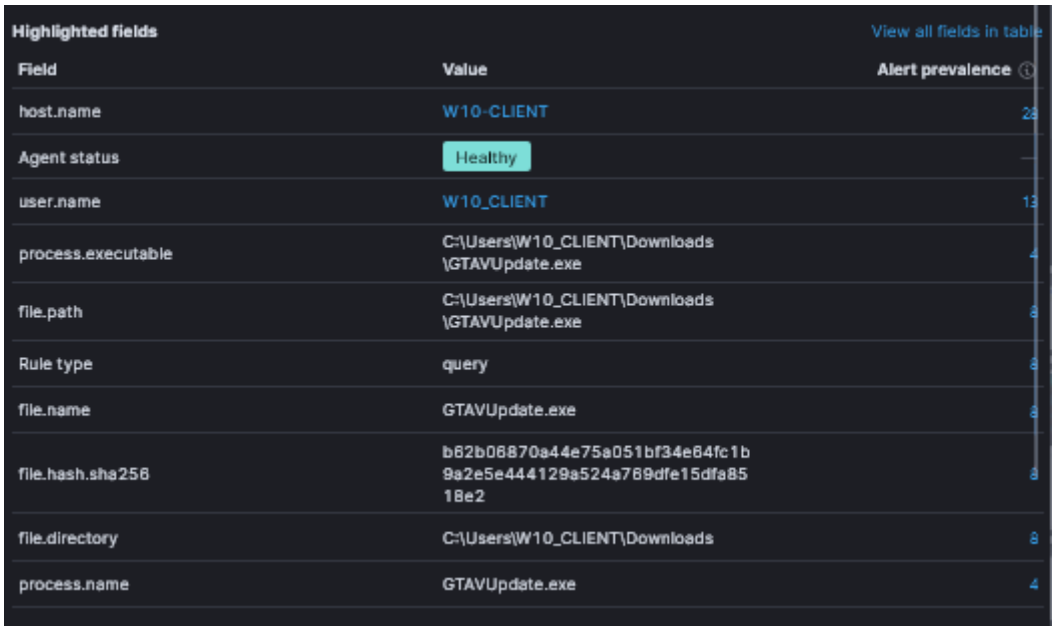


Imagen 7.38: Ejecución de malware (XIII)

Gracias a esta prueba se puede observar claramente la funcionalidad y la redundancia en la detección de malware. Todo ello teniendo en cuenta que el firewall, el antivirus y el módulo de malware prevention de Elastic Defend se encontraban desconectados.

7.2.6 Análisis de malware con PCAPs importados

Otra manera de verificar el correcto funcionamiento de nuestro sistema es hacer uso de las herramientas “so-import-pcap” y “tcpreplay” de SO para reproducir ataques aportando a nuestro sistema archivos de captura de un ataque real.

Los archivos PCAP de prueba se pueden descargar desde la web https://www.malware-traffic-analysis.net. Una vez descargado el archivo de interés, es posible importarlo mediante la interfaz web de SO. Para ello hay que ir a Grid → Seleccionar el nodo forward → Pulsar sobre el icono subida, escoger el archivo y confirmar.

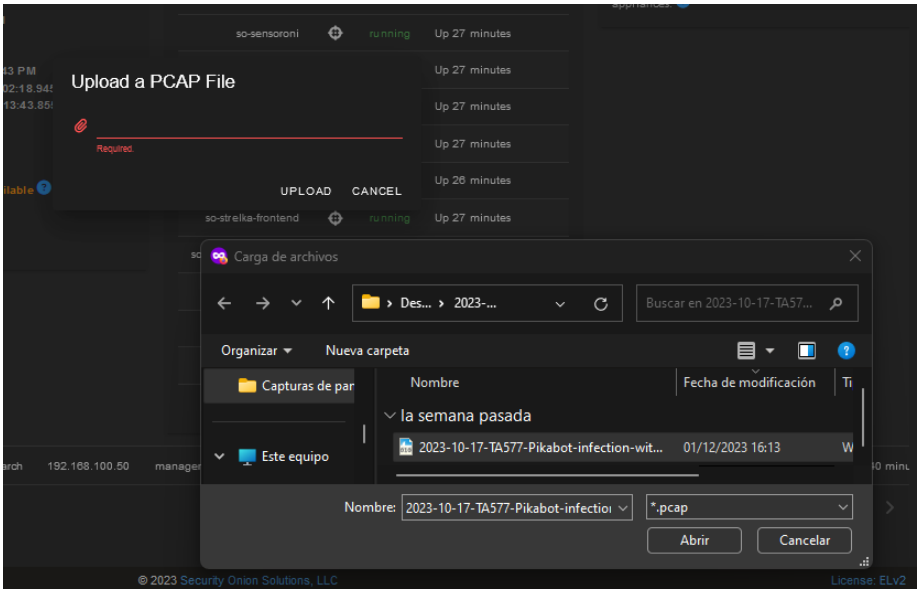


Imagen 7.39: Análisis de PCAP (I)

Otra forma de importar el archivo es a través de la interfaz de línea de comandos.

```
[root@uoc-forward bdavedu]# so-import-pcap 2023-10-17-TA577-Pikabot-infection-with-Cobalt-Strike.pcap
Processing Import: /home/bdavedu/2023-10-17-TA577-Pikabot-infection-with-Cobalt-Strike.pcap
- verifying file
- assigning unique identifier to import: 42094c700ccdfd46d8e8ff176677cb60
- analyzing traffic with Suricata
- analyzing traffic with Zeek
- found PCAP data spanning dates 2023-10-17 through 2023-10-17

Import complete!

Use the following hyperlink to view the imported data. Triple-click to quickly highlight the entire hyperlink and then copy it i
https://192.168.100.50/#/dashboards?q=import.id:42094c700ccdfd46d8e8ff176677cb60%20%7C%20groupby%20-sankey%20event.dataset%20eve
0-bar%20event.module%20%7C%20groupby%20event.dataset%20%7C%20groupby%20event.module%20%7C%20groupby%20event.category%20%7C%20gro
nation.ip%20%7C%20groupby%20destination.port&t=2023%2F10%2F17%2000%3A00%3A00%20AM%20-%202023%2F10%2F18%2000%3A00%3A00%20AM&z=UTC

or, manually set the Time Range to be (in UTC):
From: 2023-10-17    To: 2023-10-18

Note: It can take 30 seconds or more for events to appear in Security Onion Console.
[root@uoc-forward bdavedu]#
```

Imagen 7.40: Análisis de PCAP (II)

Una vez importado el archivo, es necesario entrar al enlace generado para poder visualizar y analizar el tráfico.

En este caso, se trata de “*2023-10-17 (TUESDAY) - TA577 PIKABOT INFECTION WITH COBALT STRIKE*”

En la primera pantalla se muestra una visión general de todas las alertas y logs generados por la reproducción del tráfico de la captura.

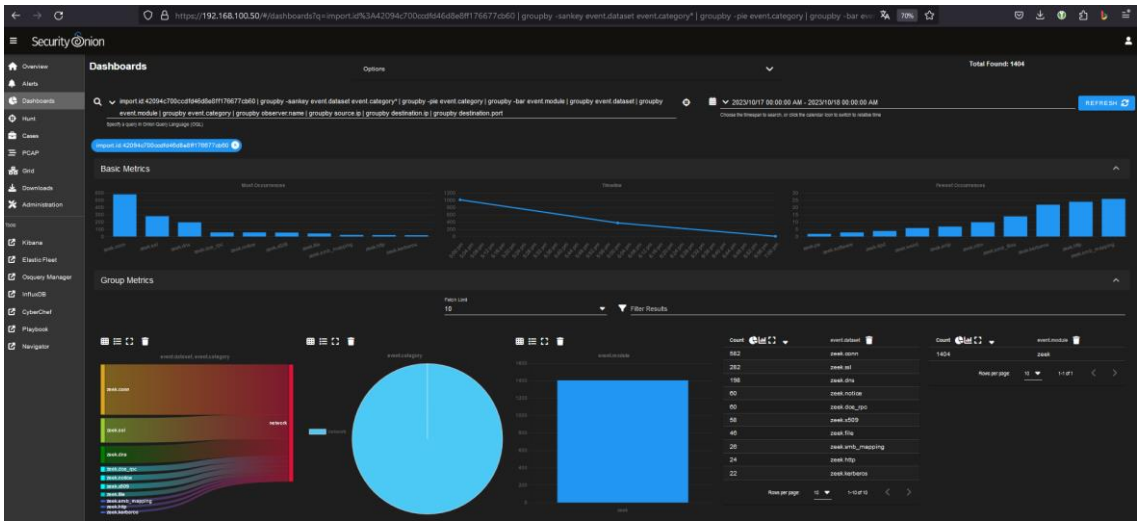
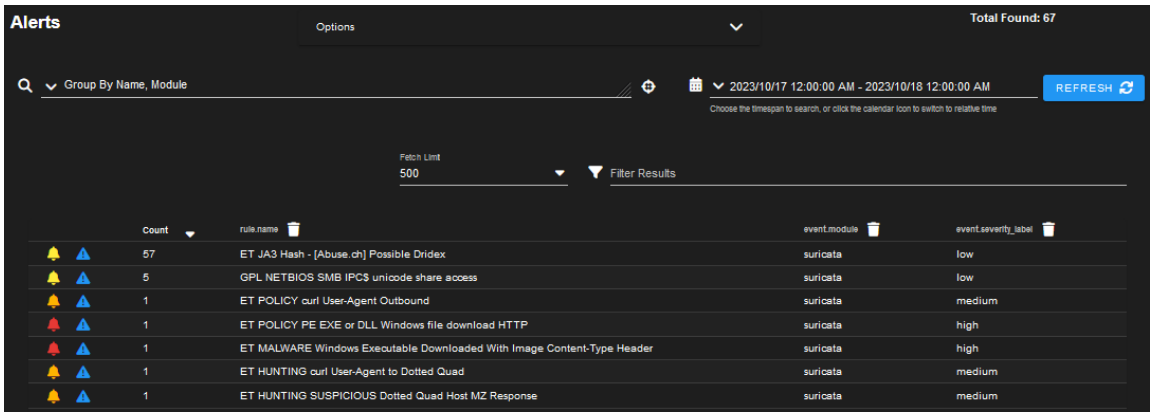


Imagen 7.41: Análisis de PCAP (III)

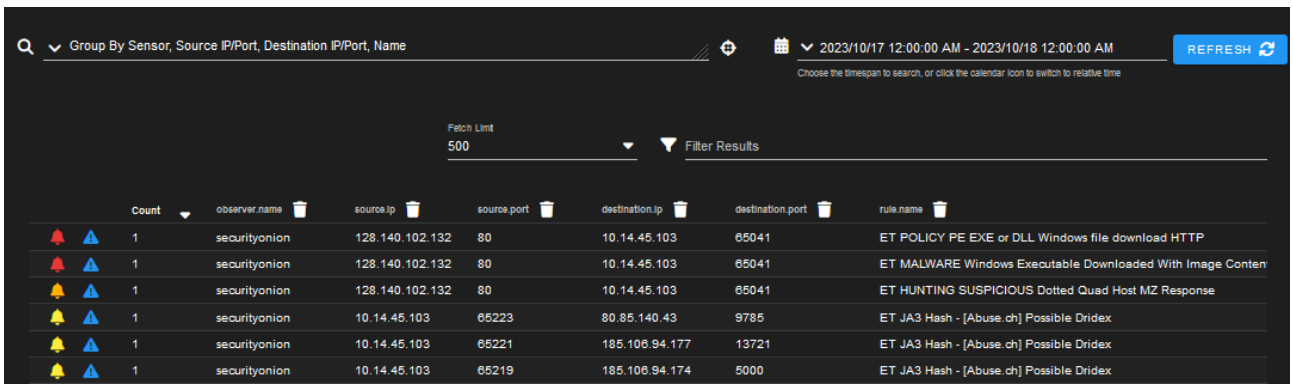
El siguiente paso consiste en ver las alertas generadas haciendo uso del panel “Alerts” de SOC.



Count	rule.name	event.module	event.severity_label
57	ET JA3 Hash - [Abuse.ch] Possible Dridex	suricata	low
5	GPL NETBIOS SMB IPC$ unicode share access	suricata	low
1	ET POLICY curl User-Agent Outbound	suricata	medium
1	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
1	ET MALWARE Windows Executable Downloaded With Image Content-Type Header	suricata	high
1	ET HUNTING curl User-Agent to Dotted Quad	suricata	medium
1	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	suricata	medium

Imagen 7.42: Análisis de PCAP (IV)

Para ver de forma más clara los flujos de datos, es necesario filtrar las alertas eliminando aquellas entradas que no son de interés.



Count	observer.name	source.ip	source.port	destination.ip	destination.port	rule.name
1	securityonion	128.140.102.132	80	10.14.45.103	65041	ET POLICY PE EXE or DLL Windows file download HTTP
1	securityonion	128.140.102.132	80	10.14.45.103	65041	ET MALWARE Windows Executable Downloaded With Image Conten
1	securityonion	128.140.102.132	80	10.14.45.103	65041	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
1	securityonion	10.14.45.103	65223	80.85.140.43	9785	ET JA3 Hash - [Abuse.ch] Possible Dridex
1	securityonion	10.14.45.103	65221	185.106.94.177	13721	ET JA3 Hash - [Abuse.ch] Possible Dridex
1	securityonion	10.14.45.103	65219	185.106.94.174	5000	ET JA3 Hash - [Abuse.ch] Possible Dridex

Imagen 7.43: Análisis de PCAP (V)

Una vez filtrada la información se puede ver que hay un flujo HTTP (puerto 80) interesante que provoca 5 alertas.

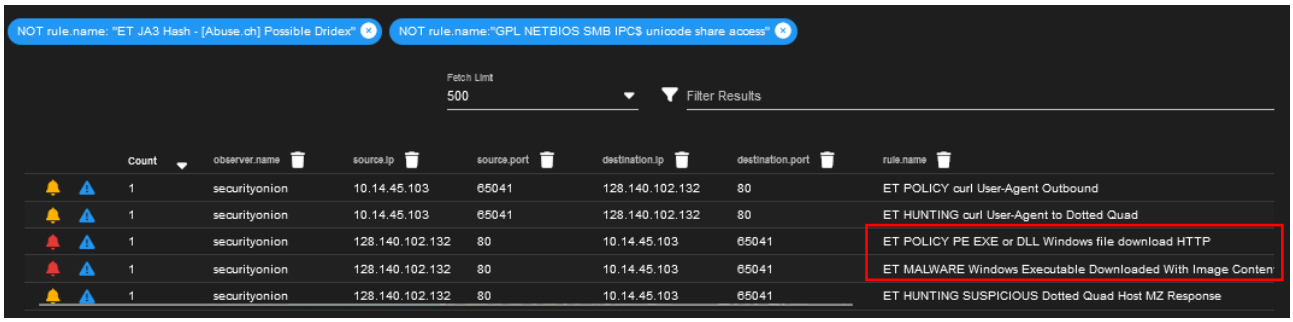


Imagen 7.44: Análisis de PCAP (VI)

Para ver con más detalle este flujo de datos es posible visualizar los datos en forma de paquetes de ida y vuelta. Para ello hay que pulsar sobre la alerta en cuestión y buscar en el desplegable la opción PCAP.

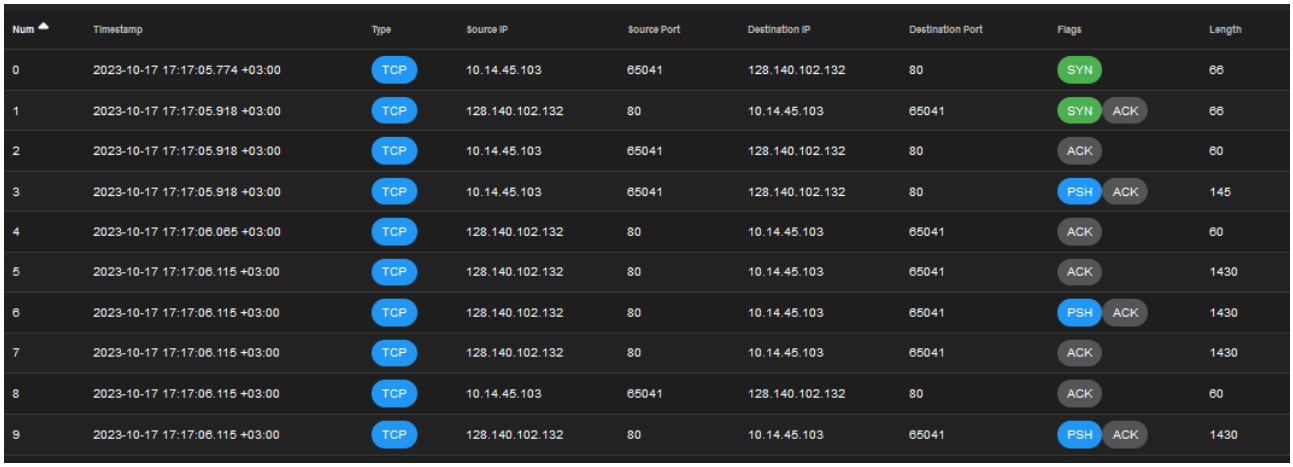


Imagen 7.45: Análisis de PCAP (VII)

Para obtener aún más información, la opción PCAP dispone de visualización en formato ASCII

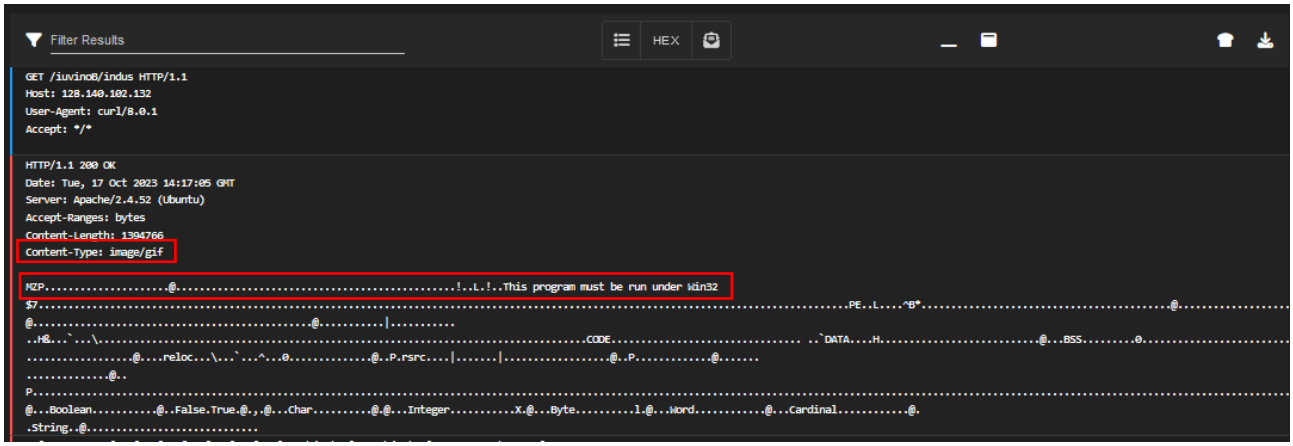


Imagen 7.46: Análisis de PCAP (VIII)

En anterior imagen se ve claramente que se trata de la descarga de un ejecutable como si fuese imagen en formato GIF.

La descarga de este ejecutable también se puede ver volviendo al panel de Dashboard de SOC y filtrando por tráfico HTTP. Además, de la descarga del ejecutable también se puede ver que hay un archivo de tipo ZIP.

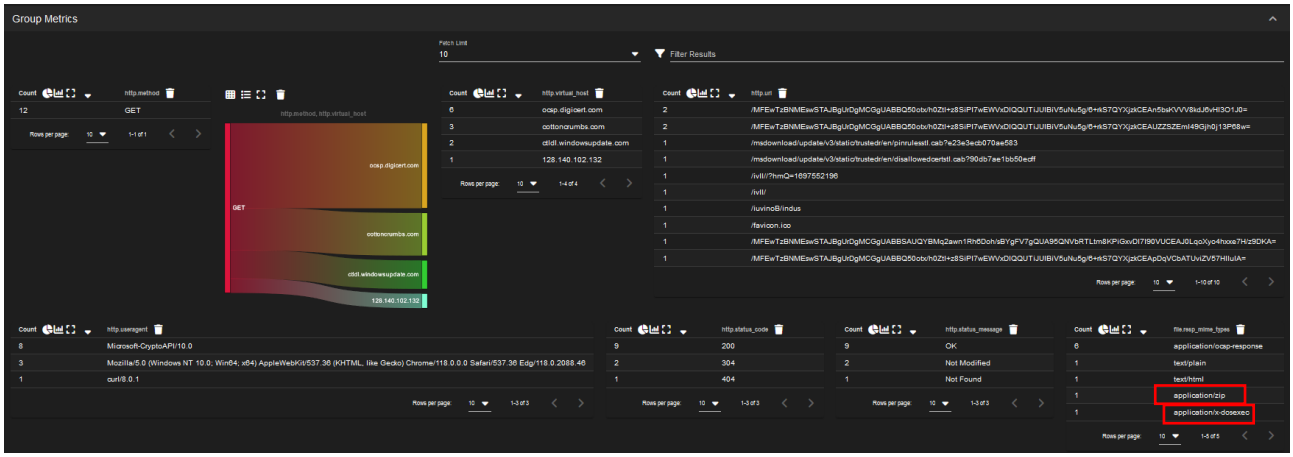


Imagen 7.47: Análisis de PCAP (IX)

A parte de todo lo anterior es posible analizar muchas más cosas como por ejemplo consultas DNS, conexiones TLS/SSL validas e invalidas, etc.

Con esta última prueba queda patente la capacidad del sistema para detectar las amenazas tanto a nivel de red como a nivel host siendo las herramientas “so-import-pcap” y “tcpreplay” útiles tanto para realizar pruebas como a nivel didáctico.

8 Conclusiones

A lo largo del desarrollo de este trabajo fin de grado se han logrado todos los objetivos propuestos. Se ha llevado a cabo de forma satisfactoria la investigación y el estudio de las herramientas NIDS y HIDS basadas en software libre disponibles en la red. De mismo modo se han comprendido por parte del autor los principios de funcionamiento y la arquitectura de despliegue de las diferentes soluciones.

Una vez finalizada la parte teórica del trabajo se han llevado a la práctica los conceptos aprendidos. Se han llegado a definir los requisitos de hardware tanto para un entorno de pruebas como para un despliegue real de un sistema de monitorización en producción. Una vez dimensionado el entorno de laboratorio se ha llevado a cabo la instalación de las diferentes soluciones y la integración de estas unas con otras con el fin de obtener un sistema integral para detección de amenazas. En paralelo con el despliegue del sistema se ha elaborado una guía paso a paso de todo el proceso incluyendo los matices más mínimos.

Finalizada la fase de puesta en marcha del entorno de laboratorio se ha procedido con las pruebas de verificación del correcto funcionamiento del sistema. Se han realizado pruebas de detección de intrusiones tanto a nivel de red como a nivel de host obteniendo resultados más que satisfactorios.

Logrados todos los hitos propuestos se puede concluir que se ha obtenido como resultado un sistema totalmente gratuito que es capaz de cubrir todas las áreas de monitorización como red, electrónica de red y dispositivos finales. En lo que a funcionalidad se refiere, queda patente y demostrado mediante diferentes pruebas que el sistema es capaz de identificar los problemas de seguridad, detectar las intrusiones y responder a las mismas ayudando a mitigar las consecuencias.

A pesar de todos los objetivos logrados en este proyecto aún queda un enorme abanico de mejoras e integraciones que se pueden materializar en trabajos futuros. En otras palabras, se ofrece una solución plenamente funcional, pero con muchas posibilidades en las que se puede profundizar.

9 Retos futuros

En lo que respecta a retos futuros, se pueden destacar los hitos relacionados con la securización de la solución desplegada, la integración del sistema con plataformas de inteligencia de ciberamenazas o el despliegue de plataformas de sistemas trampa para estudio de los modus operandi de los atacantes.

9.1 Securización

El desarrollo de este trabajo se ha centrado únicamente en el diseño e implementación de un sistema de monitorización de eventos de seguridad, dejando en segundo lugar la securización y bastionado del mismo. Esta parte resulta muy importante ya que se trata de otro sistema que puede ser objetivo de ataques. Por ello, se propone como reto futuro la securización del sistema desplegado mediante la aplicación de las guías CCN-STIC a los diferentes subsistemas que componen el conjunto.

9.2 Integraciones con MISP

A parte de las integraciones implementadas tales como Arkime, Elastic Defend o Sysmon también podría ser interesante poder alimentar nuestro sistema con la información de inteligencia compartida en plataformas como OpenCTI o MISP.

El objetivo principal sería el enriquecimiento del sistema y creación de reglas del NIDS personalizadas con la información procedente de los ataques reales guardados en una instancia de MISP, pudiendo ser la instancia de un país, un organismo de seguridad internacional o de la propia empresa.

La forma de implementación seria por medio de conexión de nuestro sistema con MISP mediante su API, proceso que requiere de estudio e investigación.

9.3 Despliegue de nodo Intrusion Detection Honeypot (IDH)

Otra forma de proteger una organización es entender cómo actúan los adversarios. Por ello se propone como reto futuro el despliegue de nodos de tipo IDH con el fin de simular los servicios de red de la organización y exponerlos a los atacantes. De esta manera se podrán obtener datos sobre ataques para su posterior análisis y creación de reglas en base al conocimiento extraído del análisis.

10 Glosario de términos

API: Interfaz de Programación de Aplicaciones (Application Programming Interface) es una pieza de código que permite a diferentes aplicaciones comunicarse entre sí y compartir información y funcionalidades.

ASCII: Es un código de caracteres basado en el alfabeto latino, tal como se usa en inglés moderno.

Benchmark: Es una técnica utilizada para medir el rendimiento de un sistema o uno de sus componentes tanto a nivel funcional como de seguridad.

CIS: (Center for Internet Security) es una plataforma web sin ánimo de lucro que reúne una serie de estándares y herramientas para garantizar la seguridad de los softwares que utilizan las compañías y las personas a diario.

CPU: Unidad Central de Procesamiento (Central Process Unit).

CCN-STIC: Centro Criptológico Nacional-Seguridad de las Tecnologías de la Información y la Comunicación. Son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones.

DDoS: Denegacion de Servicio Distribuida (Distributed Denial-of-Service) es un ataque para inhabilitar el uso de un determinado sistema o infraestructura para que no pueda prestar el servicio para el que está destinado.

DMZ: Zona Desmilitarizada (DeMilitarized Zone) es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

DNS: Sistema de Nombres de Dominio (Domain Name System) es un sistema que traduce los nombres de dominios aptos para lectura humana a direcciones IP.

ELK: (Elasticsearch Logstash Kibana) es la abreviatura del conjunto de herramientas de Elastic Stack.

EPS: Eventos Por Segundo (Events Per Second) es una forma de facturar por servicios de monitorización.

FPC: Captura Completa de Paquetes (Full Packet Capture) es la representación más exhaustiva y completa de los datos de red que se pueden recopilar.

HIDS: Sistema de Detección de Intrusiones en el Host (Host Intrusion Detection System).

HIPAA: (Health Insurance Portability and Accountability Act) es una ley de proteccion de datos de los pacientes.

Hping3: Es una herramienta de red capaz de enviar paquetes ICMP/UDP/TCP personalizados y mostrar respuestas de destino como lo hace ping con las respuestas ICMP. Maneja la fragmentación y el cuerpo y tamaño de paquetes arbitrarios, y puede usarse para transferir archivos bajo protocolos compatibles.

HTTP: Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol) es un protocolo de la capa de aplicación para la transmisión de documentos hipermedia, como

HTML: Lenguaje de Marcas de Hipertexto (HyperText Markup Language)

Hydra: Es un cracker de inicio de sesión en paralelo que admite numerosos protocolos de ataque. Es muy rápido y flexible, y es fácil agregar nuevos módulos.

IPS: Sistema de Proteccion frente a las Intrusiones (Intrusion Protection System).

JSON: (JavaScript Object Notation) es un formato de texto sencillo para el intercambio de datos.

MIME: Extensiones Multipropósito de Correo de Internet (Multipurpose Internet Mail Extensions) son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario.

MISP: Malware Information Sharing Platform es una plataforma de inteligencia contra amenazas especialmente utilizada para la compartición, almacenaje y correlación de indicadores de compromiso, persiguiendo tener una comunidad colaborativa sobre amenazas existentes, cuyo objetivo es ayudar a mejorar las contramedidas utilizadas contra los ataques dirigidos y establecer acciones preventivas y de detección.

Metasploit: Es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

Msfvenom: es una herramienta de línea de comandos que se utiliza para generar payloads personalizados para una amplia variedad de sistemas operativos y arquitecturas.

Network TAP: (Network Test Access Point) es un dispositivo de red que permite separar la entrada de datos de la salida de datos.

NIDS: Sistema de Detección de Intrusiones en la Red (Network Intrusion Detection System).

NIST 800-53: Es un estándar de seguridad de la información que proporciona un catálogo de controles de seguridad y privacidad para todos los sistemas de información federales de EE. UU., excepto aquellos relacionados con la seguridad nacional.

NMAP: Es un programa de código abierto que sirve para efectuar rastreo de puertos

OISF: (Open Information Security Foundation) es una organización sin fines de lucro creada para construir la comunidad y para apoyar tecnologías de seguridad de código abierto como Suricata.

OSINT: Inteligencia de Fuentes Abiertas (Open Source Inteligence) es una metodología multifactorial de recolección, análisis y toma de decisiones sobre datos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia.

OSSIM: (Open-Source Security Information Management).

PCAP: (Packet Capture) es un formato para guardar el tráfico capturado por soluciones FPC.

PCI-DSS: Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard).

ISO/IEC 27001: Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional

PYME: Pequeña y Mediana Empresa.

RAM: Memoria de Acceso Aleatorio (Random Access Memory).

RGPD: Reglamento General de Protección de Datos es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos en la UE y el Espacio Económico Europeo

LOPDGDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales es una ley orgánica aprobada por las Cortes Generales de España que tiene por objetivo adaptar el Derecho interno español al Reglamento General de Protección de Datos

Rootkit: Es un tipo de software malicioso diseñado para darle a un hacker la capacidad de introducirse en un dispositivo y hacerse con el control del mismo.

SIEM: Gestión de Eventos e Información de Seguridad (Security Information and Event Management).

SMTP: Protocolo para Transferencia Simple de Correo (Simple Message Transfer Protocol) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre ordenadores u otros dispositivos

SO: Security Onion.

SPAN: Analizador de Puertos del Switch (Switch Port Analyzer) es una tecnología de capa 2 que permite copiar o más bien hacer el espejo del tráfico que atraviesa un puerto.

SSD: Unidad de Estado Sólido (Solid State Drive) es un dispositivo de almacenamiento, no volátil, fabricado exclusivamente con componentes electrónicos.

SSH: Secure Shell es un protocolo cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada

TCP: Protocolo de Control de Transmisión (Transmission Control Protocol) es un protocolo que define cómo establecer y mantener una comunicacion de red a través de la cual las aplicaciones pueden intercambiar datos.

URI: Identificador de Recursos Uniforme (Uniform Resource Identifier) es una cadena de caracteres que identifica los recursos físicos o abstractos de una red de forma unívoca.

WAP: Punto de Acceso Inalámbrico (Wireless Access Point).

XDR: Detección y Respuesta Extendidas (Extended Detection and Response) es una tecnología de seguridad cibernética que monitorea y mitiga las amenazas de seguridad cibernética.

11 Bibliografía

[1] *Security Information & Event Management: Key Trends, Competitor Leaderboard & Market Forecasts 2022-2027* [en línea] [fecha de consulta: 1 de octubre de 2023]. Disponible en: https://www.juniperresearch.com/researchstore/security-identity/security-information-event-research-report

[2] *¿Qué es la ciberseguridad?* [en línea] [fecha de consulta: 5 de octubre de 2023]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

[3] *La Seguridad de la Información* [en línea] [fecha de consulta: 5 de octubre de 2023]. Disponible en: https://www.tecon.es/la-seguridad-de-la-informacion/

[4] *¿Qué son las licencias de software y qué tipos existen?* [en línea] [fecha de consulta: 8 de octubre de 2023]. Disponible en: https://www.vipnet360.com/blog/que-son-las-licencias-de-software-y-que-tipos-existen

[5] *5 Types of Software Licenses: Definitions, Examples and Tips* [en línea] [fecha de consulta: 8 de octubre de 2023]. Disponible en: https://www.indeed.com/career-advice/career-development/types-of-software-license

[6] *Dispositivos finales* [en línea] [fecha de consulta: 16 de octubre de 2023]. Disponible en: https://www.administracionderedes.com/redes-informaticas/dispositivos-finales/

[7] *Switch de red: ¿cómo facilita las telecomunicaciones en tu hogar?* [en línea] [fecha de consulta: 16 de octubre de 2023]. Disponible en: https://www.movistar.es/blog/router/switch-red-que-es-como-beneficia/

[8] *¿Qué es un router y cuál es su función?* [en línea] [fecha de consulta: 16 de octubre de 2023]. Disponible en: https://www.avg.com/es/signal/what-is-a-router

[9] *¿Qué es un firewall y cómo funciona?* [en línea] [fecha de consulta: 16 de octubre de 2023]. Disponible en: https://www.deltaprotect.com/blog/que-es-un-firewall

[10] *Punto de acceso inalámbrico* [en línea] [fecha de consulta: 17 de octubre de 2023]. Disponible en: https://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico

[11] *IT Explained: Servidor* [en línea] [fecha de consulta: 17 de octubre de 2023]. Disponible en: https://www.paessler.com/es/it-explained/server

[12] *¿Qué es un ataque activo?* [en línea] [fecha de consulta: 19 de octubre de 2023]. Disponible en: https://msmk.university/ciberseguridad/ataque

[13] *Vulnerabilidades y ataques* [en línea] [fecha de consulta: 19 de octubre de 2023]. Disponible en: https://www.uacj.mx/CGTI/CDTE/JPM/Documents/IIT/infseguridad/U2-5.html

[14] *¿Qué es la monitorización en ciberseguridad?* [en línea] [fecha de consulta: 20 de octubre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-la-monitorizacion-en-ciberseguridad/

[15] *¿Qué es la SIEM?* [en línea] [fecha de consulta: 20 de octubre de 2023]. Disponible en: https://www.ibm.com/es-es/topics/siem

[16] *Gestión de información y eventos de seguridad* [en línea] [fecha de consulta: 20 de octubre de 2023]. Disponible en: https://es.wikipedia.org/wiki/Gestión_de_información_y_eventos_de_seguridad

[17] *NIDS - Network Based Intrusion Detection System* [en línea] [fecha de consulta: 21 de octubre de 2023]. Disponible en: https://www.redscan.com/services/nids/

[18] *What is HIDS (Host-Based Intrusion Detection System)?* [en línea] [fecha de consulta: 21 de octubre de 2023]. Disponible en: https://sysdig.com/learn-cloud-native/detection-and-response/what-is-hids/

[19] *AlienVault OSSIM* [en línea] [fecha de consulta: 21 de octubre de 2023]. Disponible en: https://cybersecurity.att.com/products/ossim

[20] *Open Source Security Information Management* [en línea] [fecha de consulta: 22 de octubre de 2023]. Disponible en: https://es.wikipedia.org/wiki/Open_Source_Security_Information_Management

[21] *A comprehensive SIEM solution* [en línea] [fecha de consulta: 22 de octubre de 2023]. Disponible en: https://wazuh.com/platform/siem/

[22] *Getting started with Wazuh* [en línea] [fecha de consulta: 23 de octubre de 2023]. Disponible en: https://documentation.wazuh.com/current/getting-started/index.html

[23] *SELKS 7: Newly Updated Capabilities* [en línea] [fecha de consulta: 23 de octubre de 2023]. Disponible en: https://www.stamus-networks.com/blog/selks-7-newly-updated-capabilities

[24] *What is SELKS?* [en línea] [fecha de consulta: 23 de octubre de 2023]. Disponible en: https://www.stamus-networks.com/selks

[25] *Introduction to SO documentation* [en línea] [fecha de consulta: 24 de octubre de 2023]. Disponible en: https://docs.securityonion.net/en/2.4/introduction.html

[26] *SOS* [en línea] [fecha de consulta: 24 de octubre de 2023]. Disponible en: https://securityonionsolutions.com/

[27] *Suricata. Observe. Protect. Adapt.* [en línea] [fecha de consulta: 24 de octubre de 2023]. Disponible en: https://suricata.io/

[28] *Performance Characterization of Suricata's Thread Models* [en línea] [fecha de consulta: 24 de octubre de 2023]. Disponible en: https://xbu.me/article/performance-characterization-of-suricata-thread-models/

[29] *What is Snort?* [en línea] [fecha de consulta: 25 de octubre de 2023]. Disponible en: https://www.snort.org/

[30] *What Is SNORT?* [en línea] [fecha de consulta: 25 de octubre de 2023]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/snort

[31] *Zeek. An Open Source Network Security Monitoring Tool* [en línea] [fecha de consulta: 25 de octubre de 2023]. Disponible en: https://zeek.org/

[32] *About Zeek* [en línea] [fecha de consulta: 25 de octubre de 2023]. Disponible en: https://docs.zeek.org/en/master/about.html#what-is-zeek

[33] *Server Intrusion Detection for Every Platform* [en línea] [fecha de consulta: 25 de octubre de 2023]. Disponible en: https://www.ossec.net/

[34] *SAMHAIN / BELTANE* [en línea] [fecha de consulta: 26 de octubre de 2023]. Disponible en: https://la-samhna.de/index.html

[35] *Fleet and Elastic Agent overview* [en línea] [fecha de consulta: 26 de octubre de 2023]. Disponible en: https://www.elastic.co/guide/en/fleet/current/fleet-overview.html

[36] *Arkime. Full Packet Capture* [en línea] [fecha de consulta: 26 de octubre de 2023]. Disponible en: https://arkime.com/

[37] *Stenographer* [en línea] [fecha de consulta: 26 de octubre de 2023]. Disponible en: https://github.com/google/stenographer

[38] *CyberChef* [en línea] [fecha de consulta: 27 de octubre de 2023]. Disponible en: https://gchq.github.io/CyberChef/

[39] *Elastic Defend* [en línea] [fecha de consulta: 27 de octubre de 2023]. Disponible en: https://docs.elastic.co/en/integrations/endpoint

[40] *Sysmon* [en línea] [fecha de consulta: 27 de octubre de 2023]. Disponible en: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

[41] *Syslog* [en línea] [fecha de consulta: 28 de octubre de 2023]. Disponible en: https://es.wikipedia.org/wiki/Syslog

[42] *VirtualBox* [en línea] [fecha de consulta: 27 de septiembre de 2023]. Disponible en: https://www.virtualbox.org

[43] *Security Information and Event Management (SIEM) Reviews and Ratings* [en línea] [fecha de consulta: 03 de enero de 2024]. Disponible en: https://www.gartner.com/reviews/market/security-information-event-management

[44] Splunk Enterprise Security: Use Cases, Features, *and Process* [en línea] [fecha de consulta: 03 de enero de 2024]. Disponible en: https://www.bluevoyant.com/knowledge-center/splunk-enterprise-security-use-cases-features-and-process

[45] *Splunk Enterprise Security* [en línea] [fecha de consulta: 03 de enero de 2024]. Disponible en: https://www.splunk.com/en_us/products/enterprise-security.html

[46] *Reduce Risk with SIEM Solutions* [en línea] [fecha de consulta: 03 de enero de 2024]. Disponible en: https://logrhythm.com/solutions/security/siem/

[47] IBM Security QRadar SIEM [en línea] [fecha de consulta: 03 de enero de 2024]. Disponible en: https://www.ibm.com/products/qradar-siem

[48] Security Solutions Product Feature Comparison [en línea] [fecha de consulta: 03 de enero de 2024]. Disponible en: https://logrhythm.com/comparison/logrhythm-vs-splunk/

12 Anexos

12.1 Anexo I – Despliegue y configuración de Security Onion

Para la instalación de los nodos de SO usaremos la ISO disponible en la página de los desarrolladores. Esta ISO tiene incluido tanto el sistema operativo base que es el Oracle Linux 9 como todos los paquetes necesarios para el despliegue de SO. En ambos casos tanto para el nodo manager-search como para el nodo forward los primeros pasos se resumen en la instalación de Oracle Linux 9 y creación del usuario administrador del sistema.

Al arrancar la máquina virtual aparece este menú para la selección de instalación que se va a realizar. En este caso, se va instalar Security Onion 2.4.20 sin interfaz gráfica por lo que la opción escogida es la primera.

Imagen 12.1: Instalación SO (I)

Seguidamente aparece el aviso de que se van a destruir todos los datos en el disco duro debido a la instalación. Al estar de acuerdo con ello hay que confirmar tecleando “yes”.

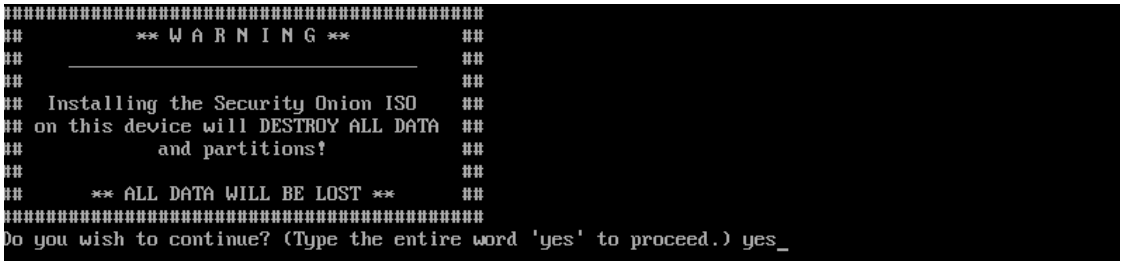


Imagen 12.2: Instalación SO (II)

Seguidamente el proceso solicita las credenciales para el usuario administrador. En este caso el usuario será “bdavedu”. Al confirmar la contraseña dos veces, comienza la instalación del sistema operativo.

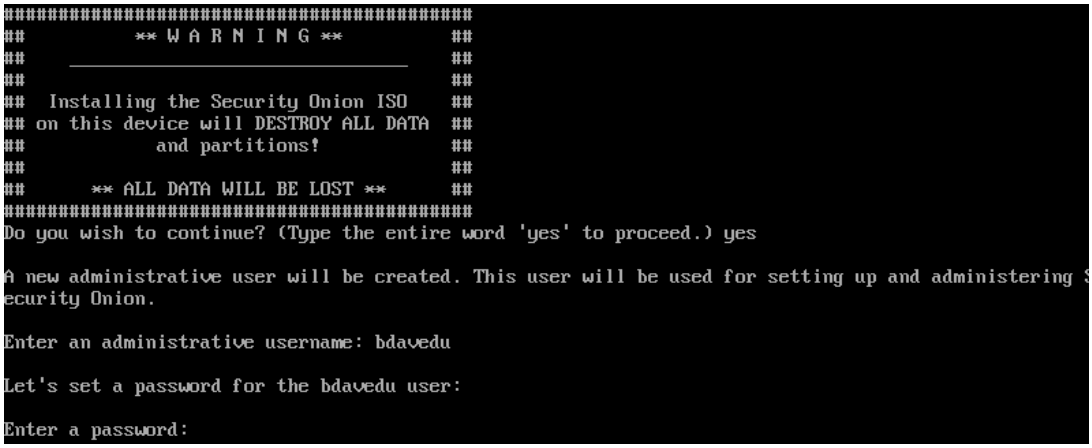


Imagen 12.3: Instalación SO (III)

Al terminar la instalación, es necesario confirmar pulsando “Enter” y esperar a que el sistema se reinicie.

Imagen 12.4: Instalación SO (IV)

Una vez instalado el sistema operativo hay que autenticarse como administrador para seguir con la instalación.

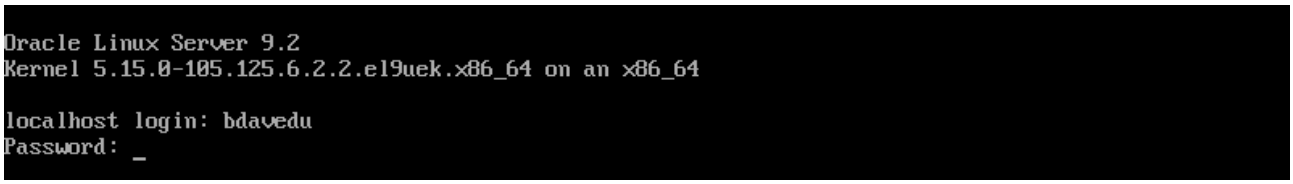


Imagen 12.5: Instalación SO (V)

12.1.1 Instalación nodo Manager-Search

Una vez instalado el sistema operativo y con el usuario de administrador autenticado comienza el proceso de instalación del SO en sí. En la pantalla de bienvenida hay que confirmar con “Yes”.

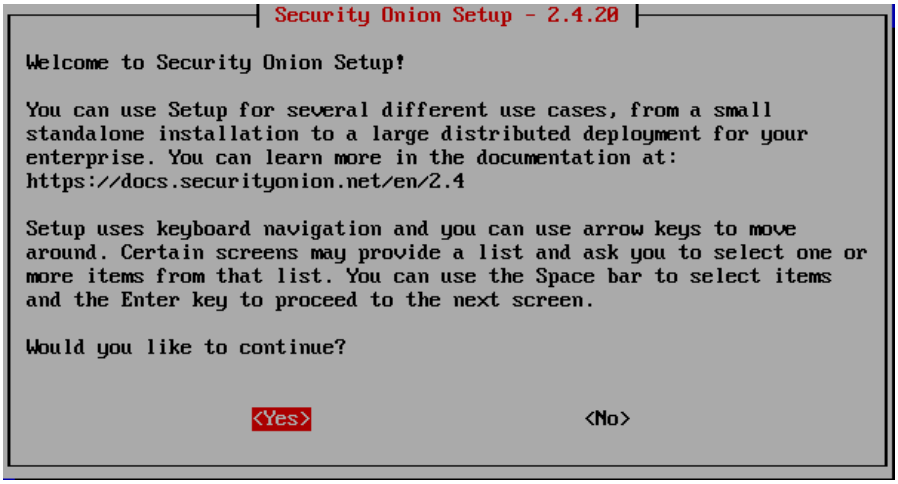


Imagen 12.6: Instalación SO (VI)

Seguidamente hay que se escoger si se van a instalar todos los componentes o únicamente se va a configurar la red. En este caso, la opción es “Install”.

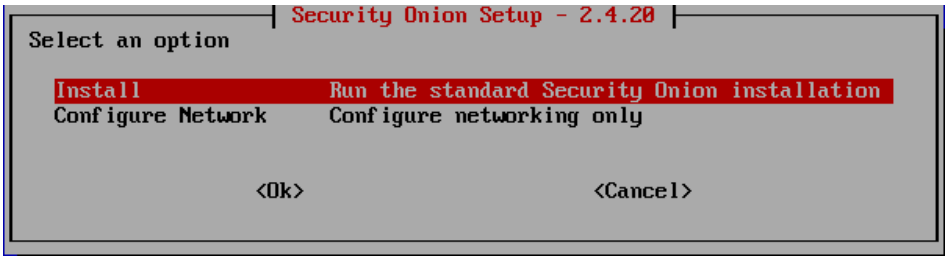


Imagen 12.7: Instalación SO (VII)

En la pantalla siguiente se escoge el tipo de despliegue siendo “DISTRIBUTED” y “New Deployment” en este caso.

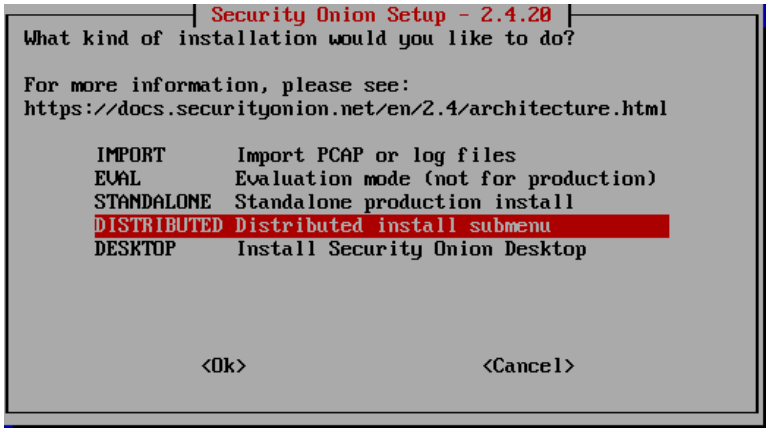


Imagen 12.8: Instalación SO (VIII)

Imagen 12.9: Instalación SO (IX)

En la siguiente pantalla se escoge el tipo de nodo a desplegar, siendo “MANAGERSEARCH” en este caso.

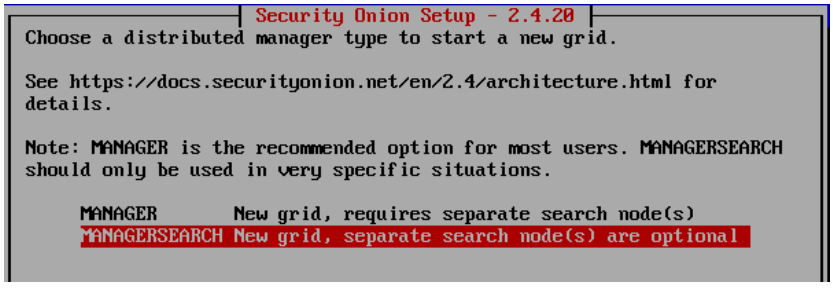


Imagen 12.10: Instalación SO (X)

Una vez seleccionado el nodo, el proceso informa sobre el acuerdo de licencia, el cual hay que aceptar tecleando “AGREE”.

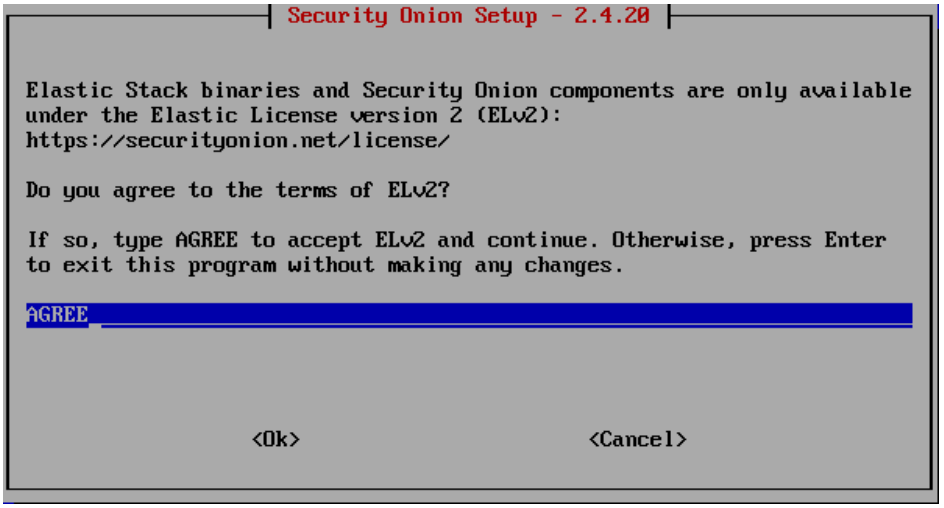


Imagen 12.11: Instalación SO (XI)

En el siguiente paso hay que escoger el tipo de instalación, siendo la opción “Standard” para sistemas con conexión a Internet y la “Airgap” para una instalación sin conexión. En este caso se hará despliegue con conexión.

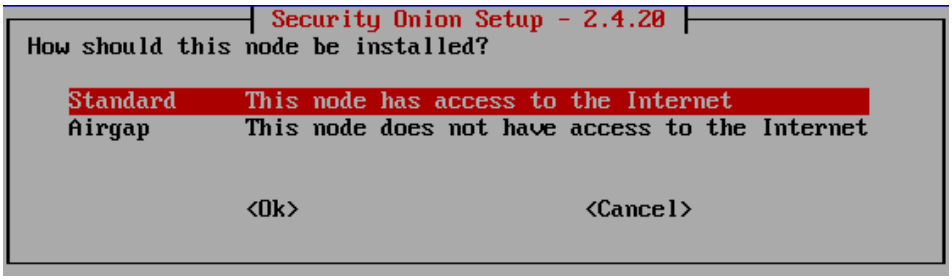


Imagen 12.12: Instalación SO (XII)

Después se define el nombre del nodo que en este caso es “uoc-managersearch” y su descripción.

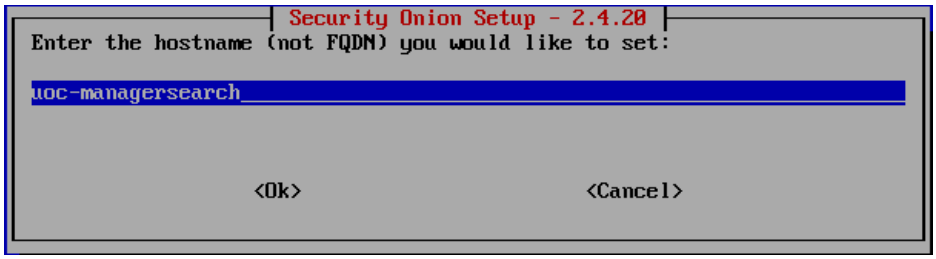


Imagen 12.13: Instalación SO (XIII)

El paso siguiente consiste en escoger y configurar la tarjeta de red administración.

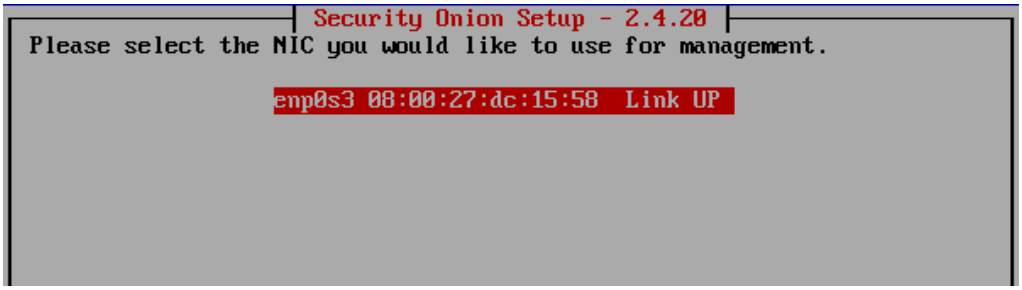


Imagen 12.14: Instalación SO (XIV)

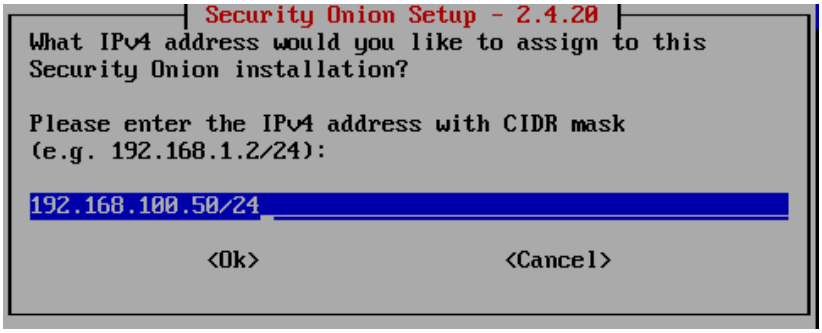


Imagen 12.15: Instalación SO (XV)

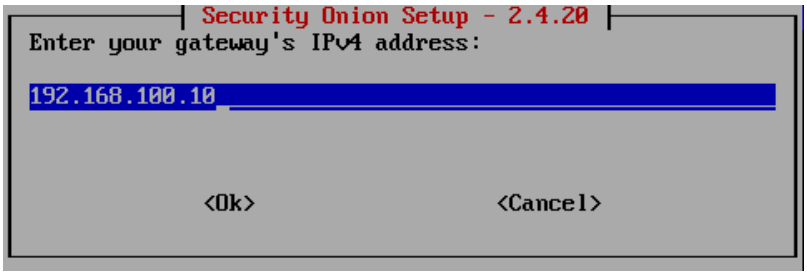


Imagen 12.16: Instalación SO (XVI)

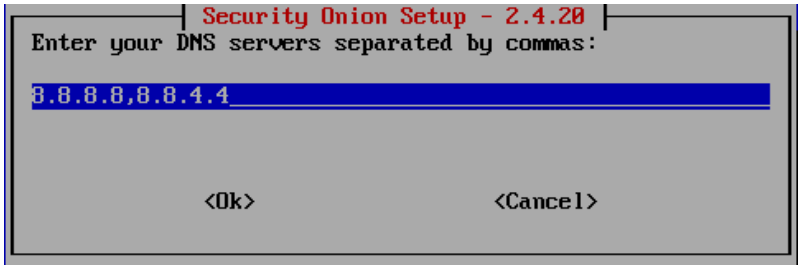


Imagen 12.17: Instalación SO (XVII)

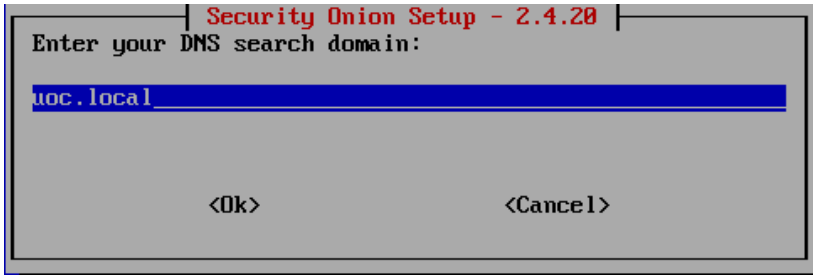


Imagen 12.18: Instalación SO (XVIII)

Una vez configurada la interfaz de red, se pregunta por el tipo de conexión, si es directa o mediante proxy. Para este caso, se trata de una conexión directa hacia Internet.

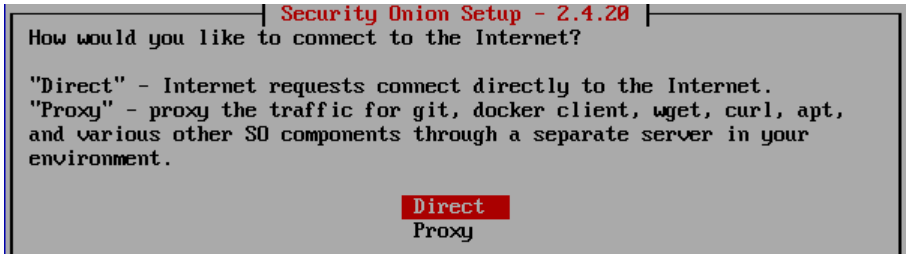


Imagen 12.19: Instalación SO (XIX)

El paso siguiente consiste en definir el usuario administrador de la interfaz web de SO, que en este caso será bdavedu@uoc.edu e indicar como se va a acceder a dicha interfaz y quien podrá acceder a la misma, una IP única o rango de IPs.

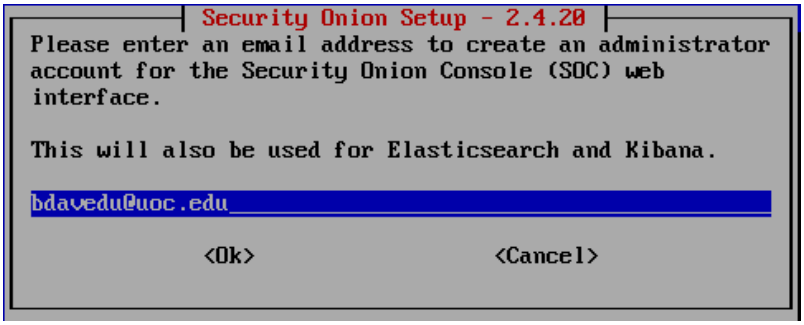


Imagen 12.20: Instalación SO (XX)

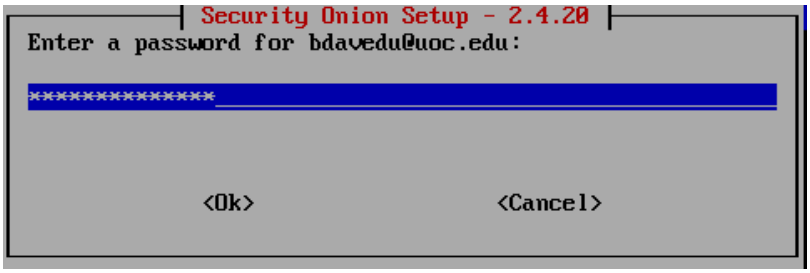


Imagen 12.21: Instalación SO (XXI)

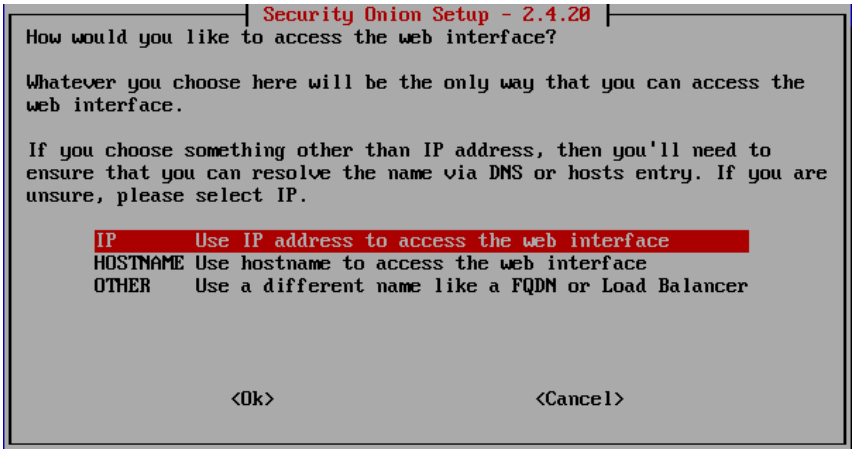


Imagen 12.22: Instalación SO (XXII)

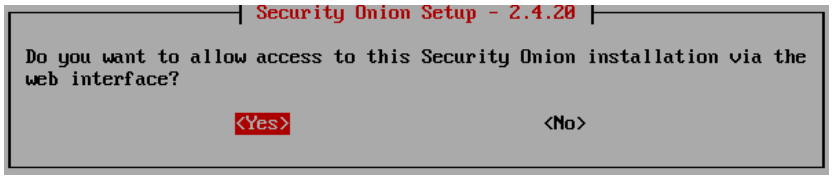


Imagen 12.23: Instalación SO (XXIII)

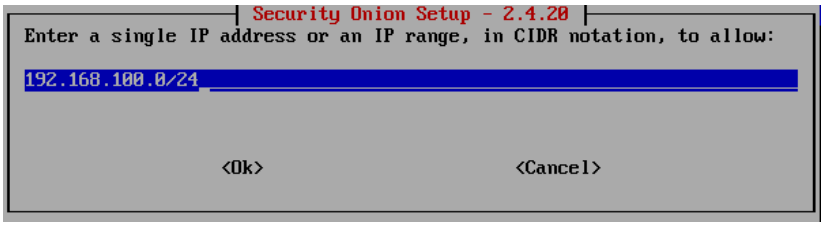


Imagen 12.24: Instalación SO (XXIV)

En este caso se autoriza el acceso a la interfaz web a toda la red. Esta configuración se puede cambiar más adelante desde la propia interfaz o mediante el comando so-firewall.

Para finalizar la configuración se muestra un resumen. En caso de estar todo correcto se debe confirmar con “Yes”.

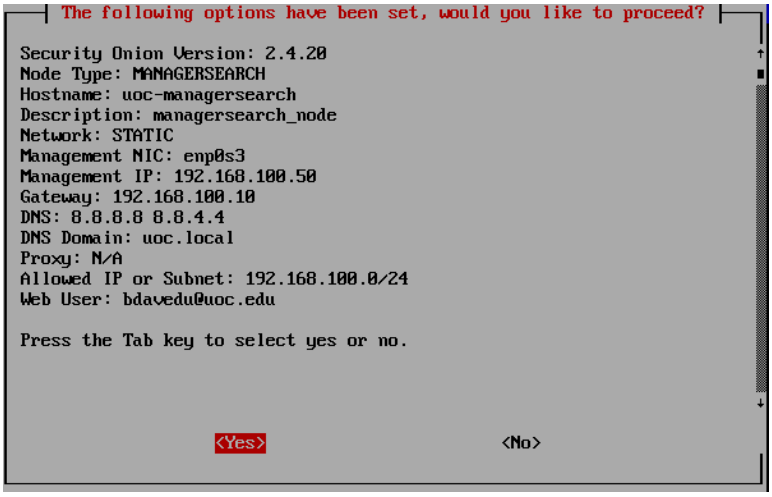


Imagen 12.25: Instalación SO (XXV)

Una vez finalizada la instalación aparece la siguiente ventana de confirmación.

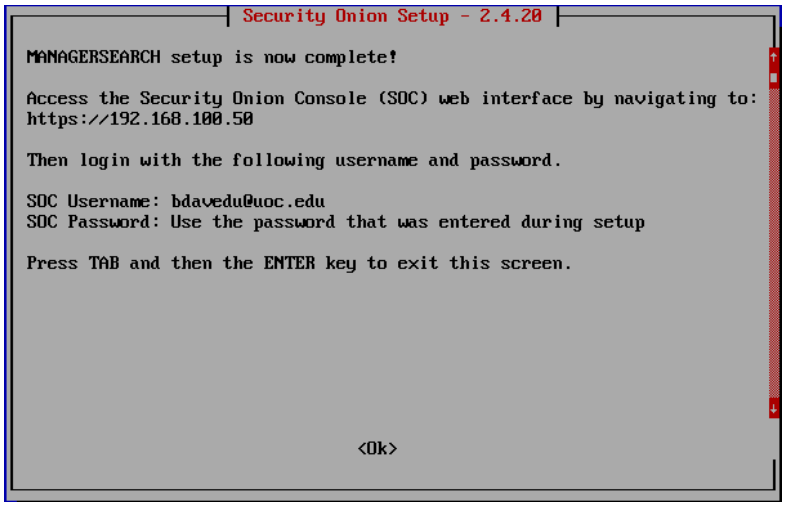


Imagen 12.26: Instalación SO (XXVI)

Para verificar la instalación es necesario entrar en la interfaz web y autenticarse.

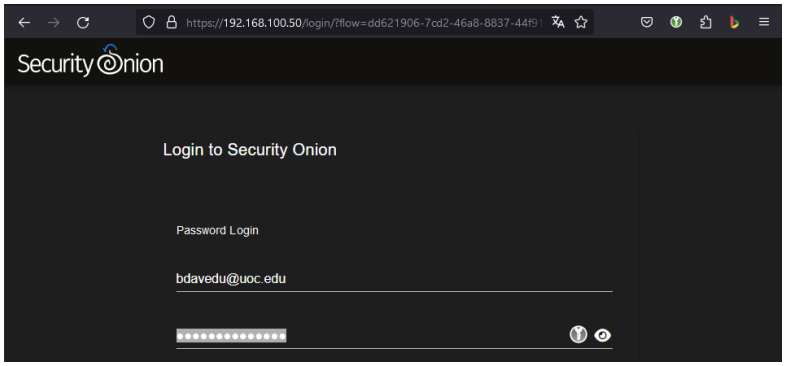


Imagen 12.27: Instalación SO (XXVII)

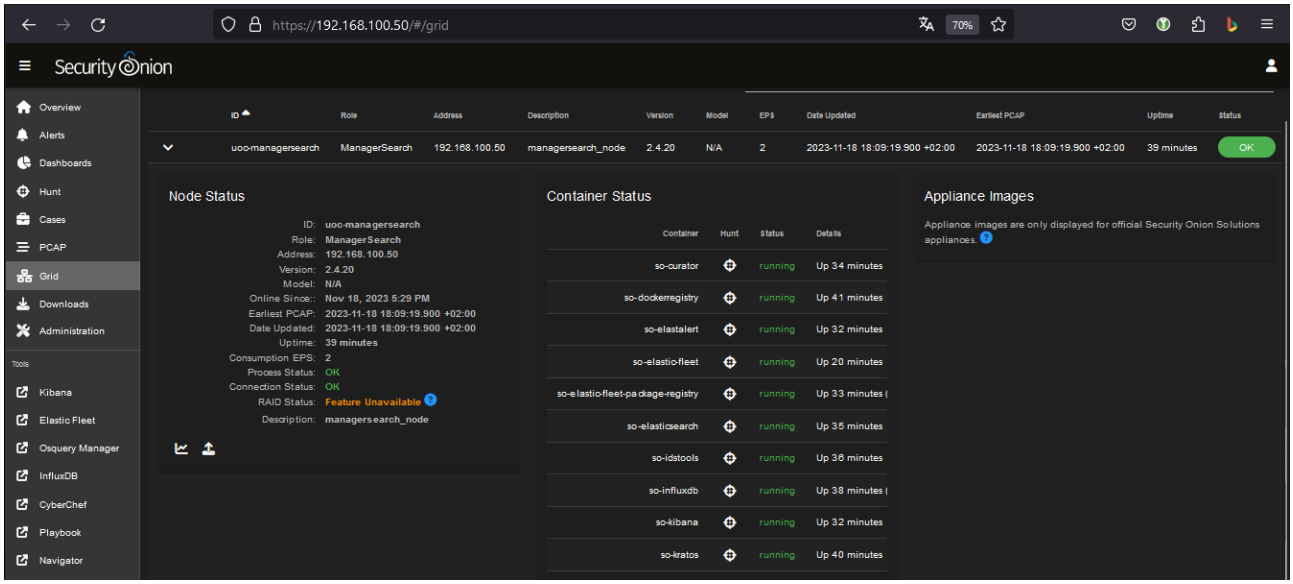


Imagen 12.28: Instalación SO (XXVIII)

12.1.2 Instalación nodo Forward

Al igual que con el nodo manager-search, los pasos iniciales son los mismos hasta llegar a la selección de tipo de instalación. En este caso se escoge “Existing Deployment”.

Imagen 12.29: Instalación SO (XXIX)

El tipo de nodo a escoger es el “SENSOR” al tratarse de nodo forward.

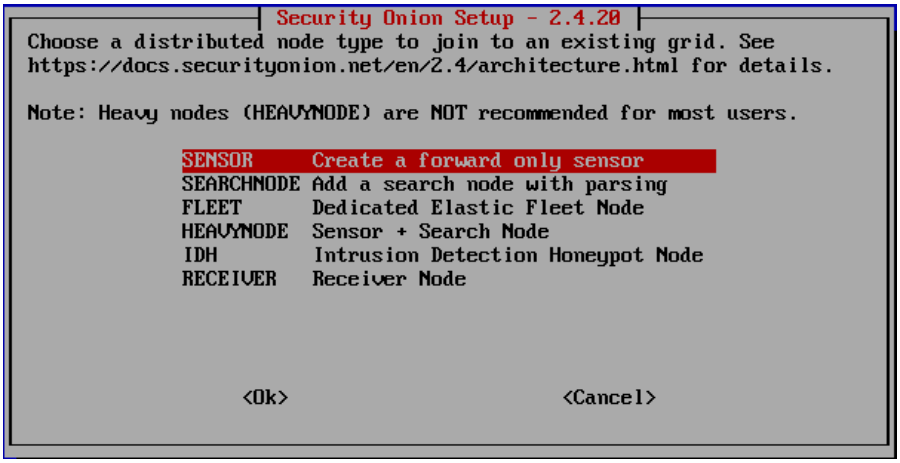


Imagen 12.30: Instalación SO (XXX)

Seguidamente se configura el nombre, la descripción y la interfaz de administración siendo la puerta de enlace predeterminada y los DNS los mismos que para el nodo manager-search.

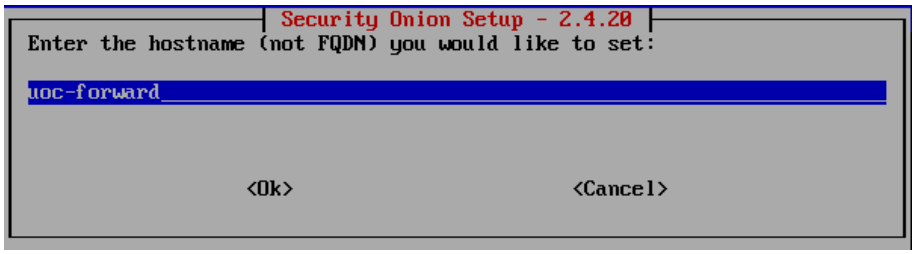


Imagen 12.31: Instalación SO (XXXI)

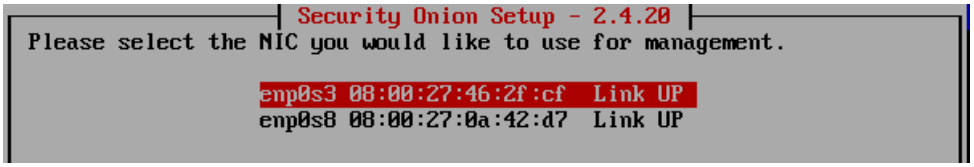


Imagen 12.32: Instalación SO (XXXII)

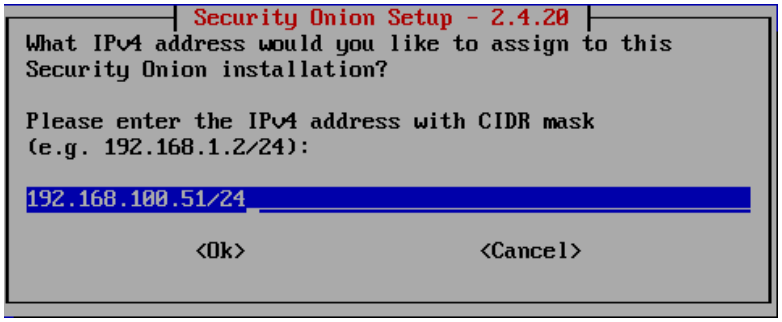


Imagen 12.33: Instalación SO (XXXIII)

Una vez configurada la interfaz de red se debe introducir el nombre del nodo manager-search y su dirección IP.

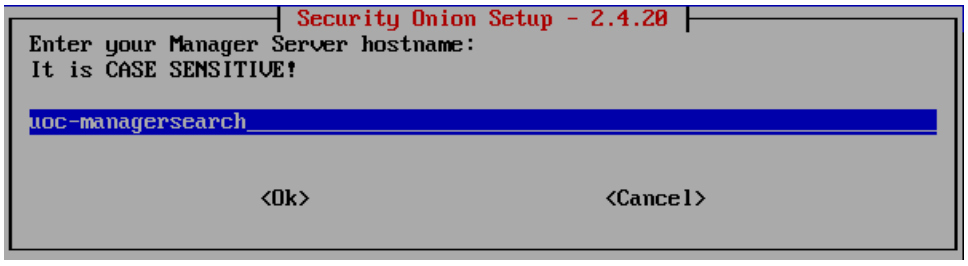


Imagen 12.34: Instalación SO (XXXIV)

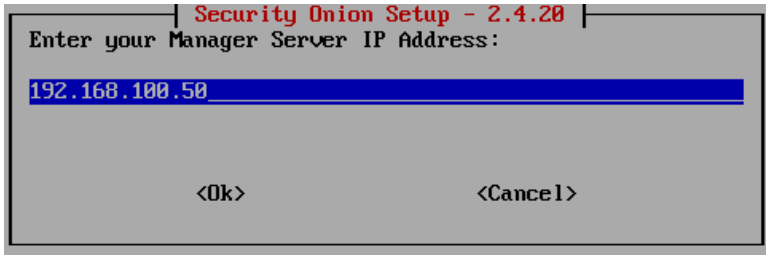


Imagen 12.35: Instalación SO (XXXV)

Para permitir que el nodo forward se conecte al nodo manager-search es necesario habilitar el acceso a través del firewall desde la interfaz web.

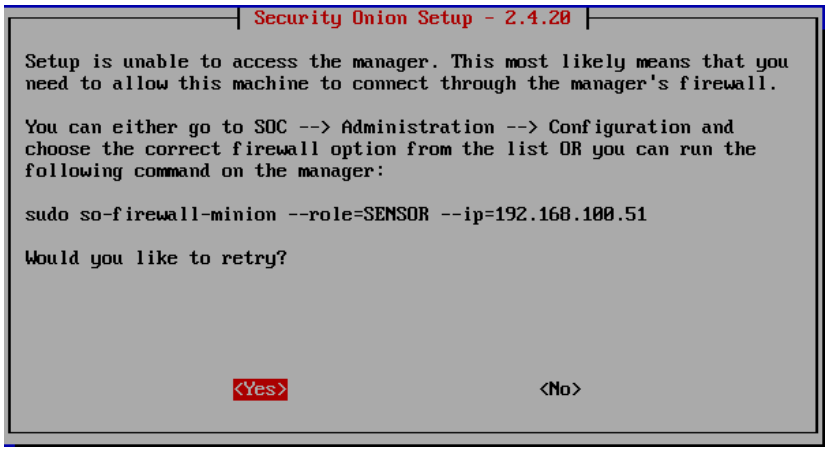


Imagen 12.36: Instalación SO (XXXVI)

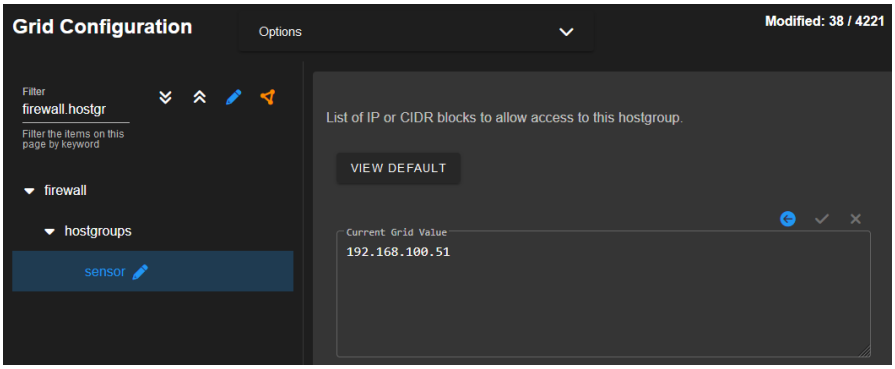


Imagen 12.37: Instalación SO (XXXVII)

A continuación, se escoge la interfaz de red para la monitorización del tráfico de red.

Imagen 12.38: Instalación SO (XXXVIII)

Al igual que con el nodo manager-search hay que aceptar el resumen de la configuración.

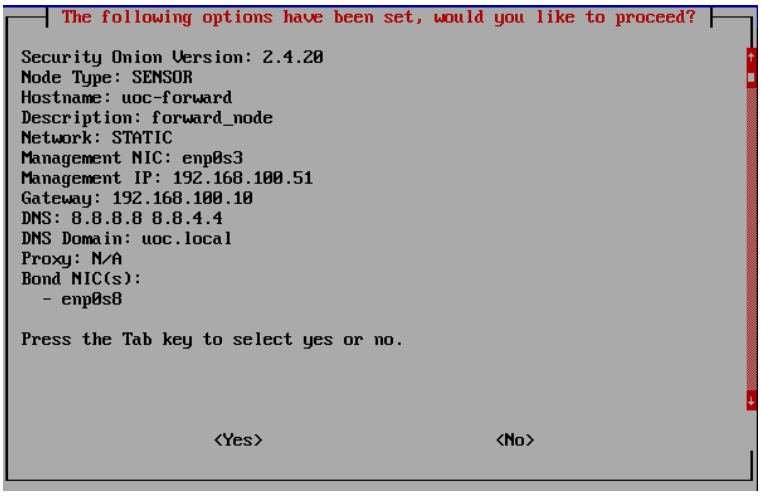


Imagen 12.39: Instalación SO (XXXIX)

Para finalizar la instalación hay que vincular el nodo forward despliegue existente.

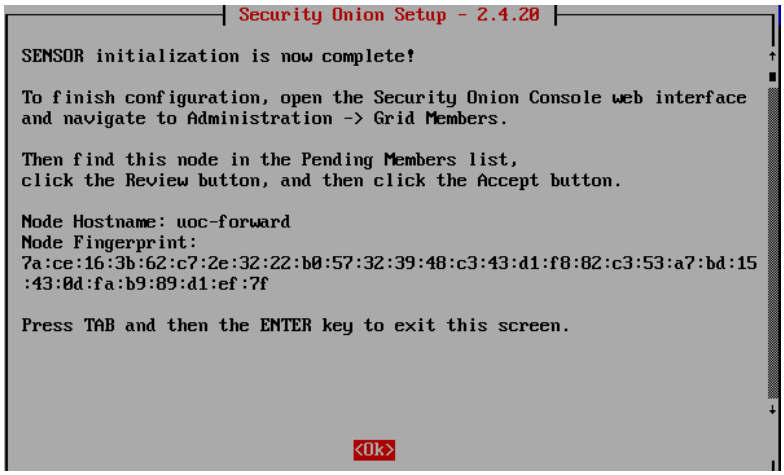


Imagen 12.40: Instalación SO (XL)

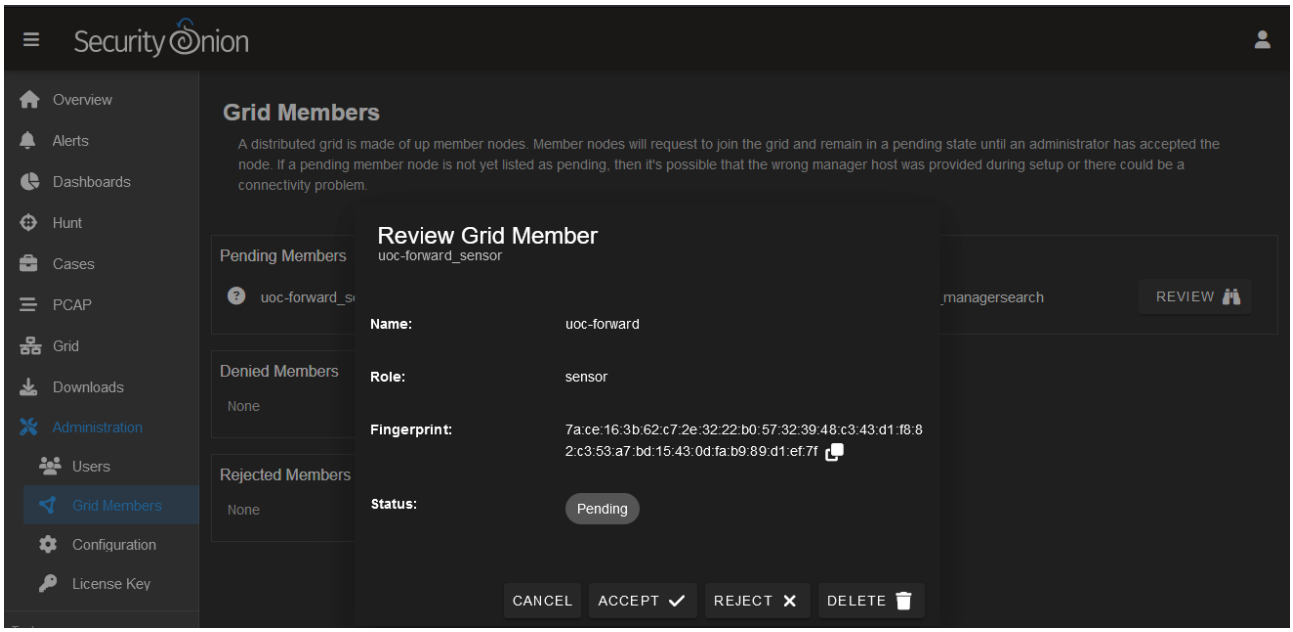


Imagen 12.41: Instalación SO (XLI)

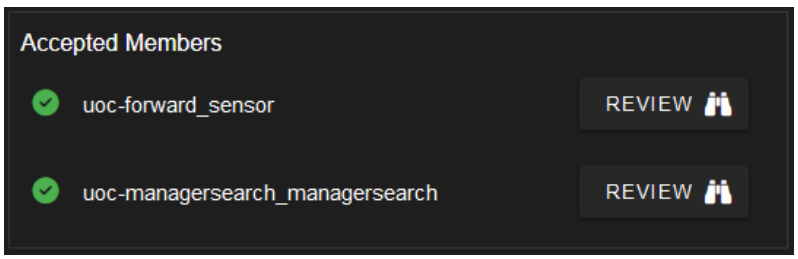


Imagen 12.42: Instalación SO (XLII)

Una vez terminada la instalación, es necesario verificar el correcto funcionamiento del sensor desde la interfaz web.

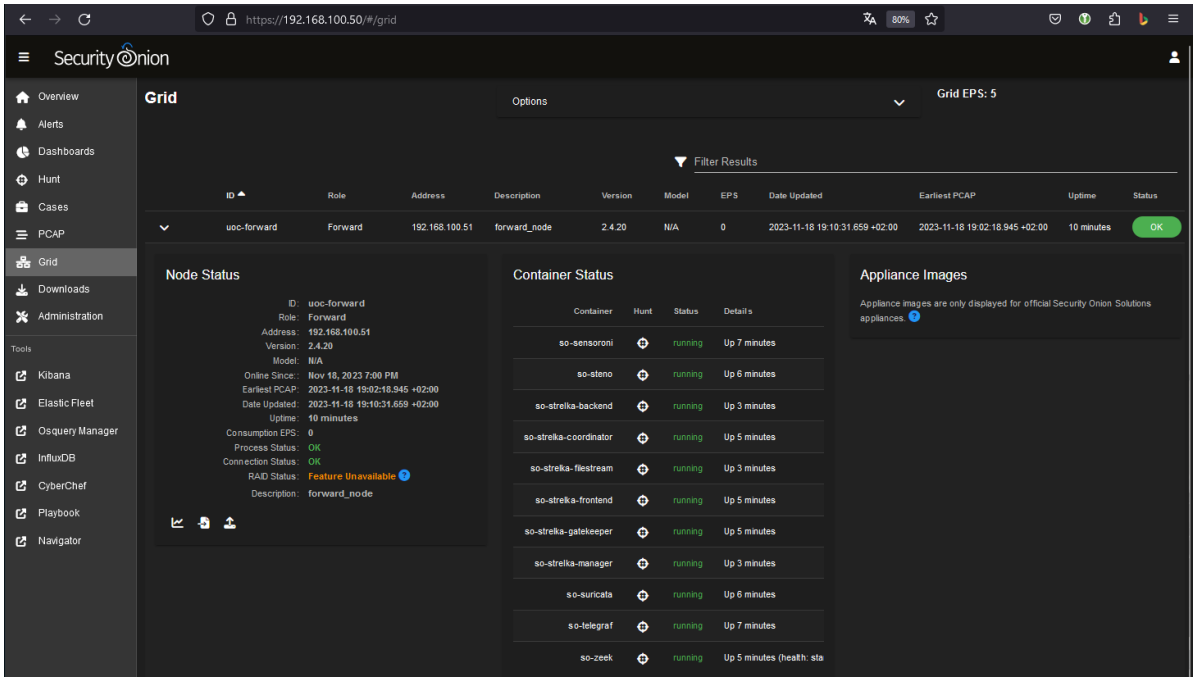


Imagen 12.43: Instalación SO (XLIII)

El último paso es definir las redes propias para el correcto funcionamiento de las reglas del NIDS. En este caso nuestra red privada es 192.168.100.0/24.

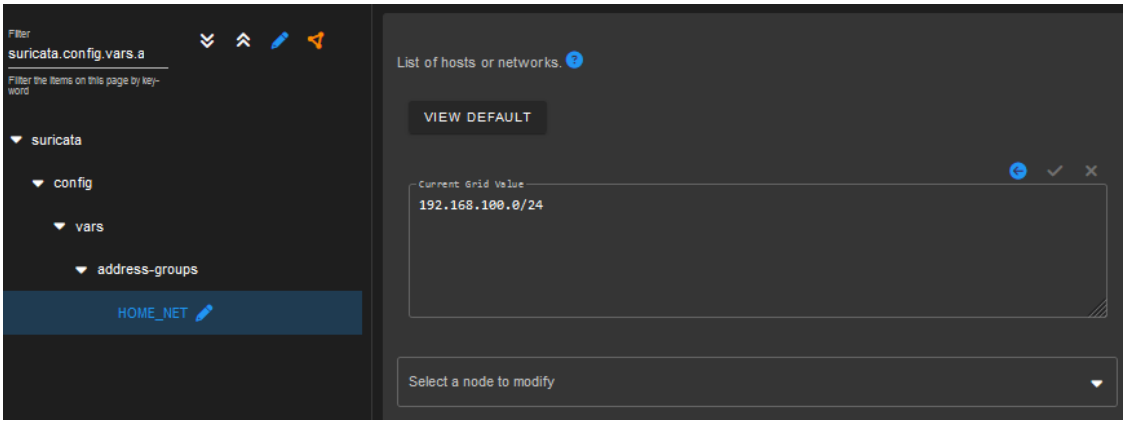


Imagen 12.44: Instalación SO (XLIV)

12.2 Anexo II – Despliegue y configuración de Arkime

El primer paso para el despliegue de Arkime es la instalación del sistema operativo CentOS 7. Este proceso se resume en seguir las indicaciones del instalador como escoger el idioma, nombre de usuario administrador, direccionamiento IP, etc. Estas configuraciones se resumen en las siguientes capturas:

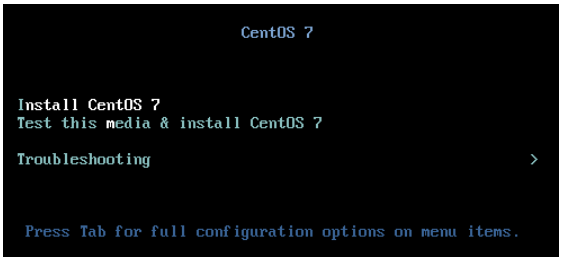


Imagen 12.45: Instalación Arkime (I)

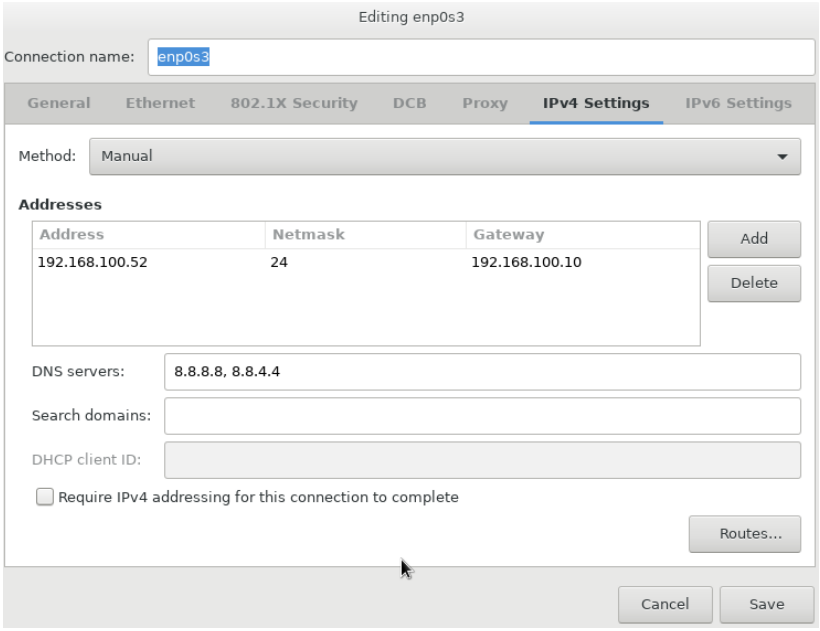


Imagen 12.46: Instalación Arkime (II)

12.2.1 Instalación

Una vez instalado el sistema operativo y realizada la autenticación, es necesario actualizar el sistema e instalar los paquetes “tcpdump” y “wget” con los comandos que se ven a continuación:

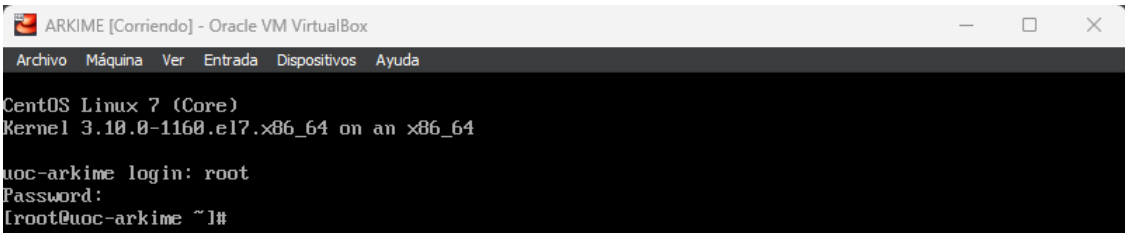


Imagen 12.47: Instalación Arkime (III)

yum upgrade

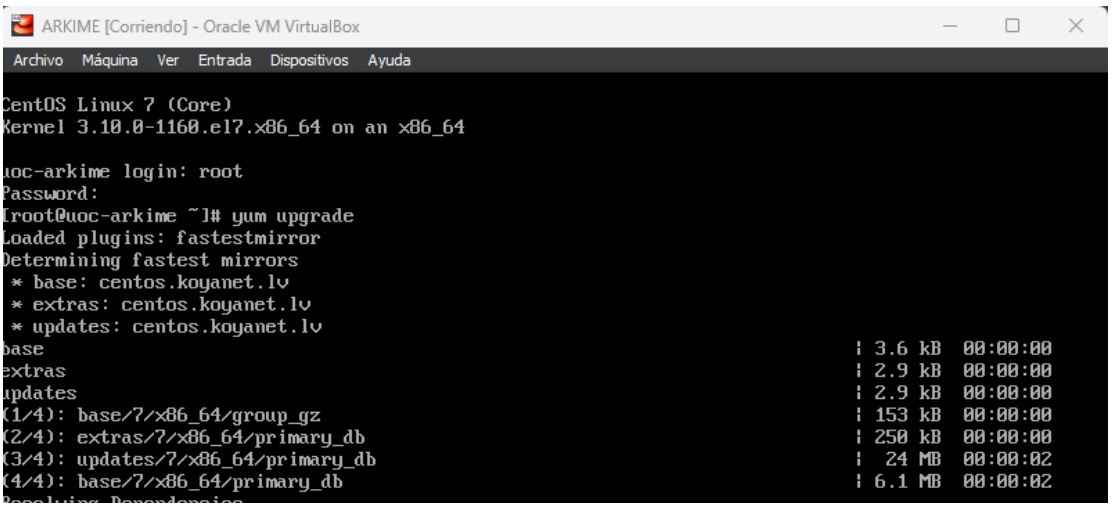


Imagen 12.48: Instalación Arkime (IV)

yum update

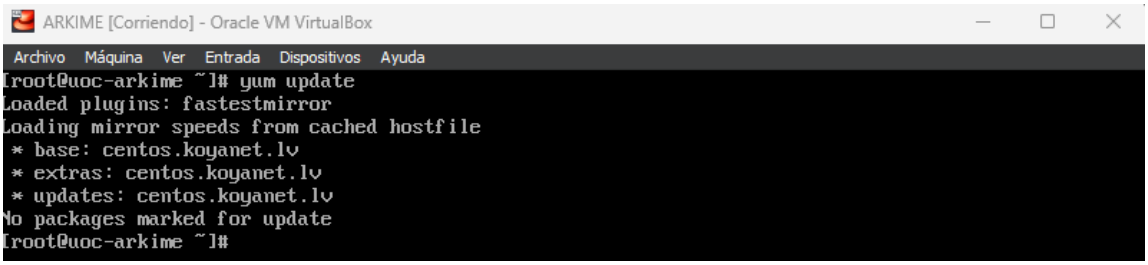


Imagen 12.49: Instalación Arkime (V)

yum install tcpdump

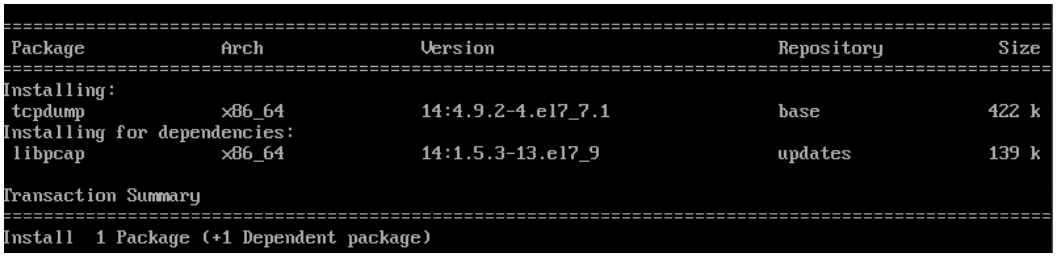


Imagen 12.50: Instalación Arkime (VI)

yum install wget

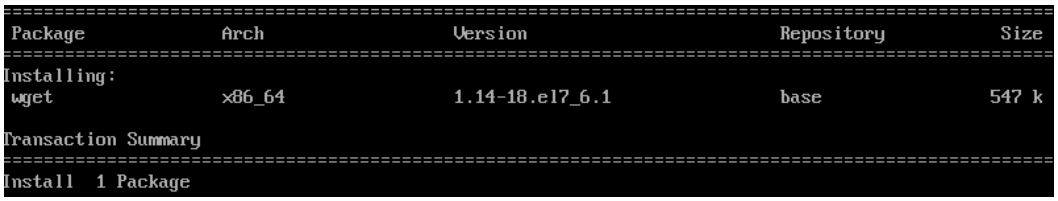


Imagen 12.51: Instalación Arkime (VII)

El siguiente paso consiste en configurar la interfaz de red de captura de tráfico en modo promiscuo usando el siguiente comando:

echo "ip link set ens224 promisc on" >> /etc/rc.d/rc.local && chmod u+x /etc/rc.d/rc.local && systemctl enable rc-local && systemctl start rc-local

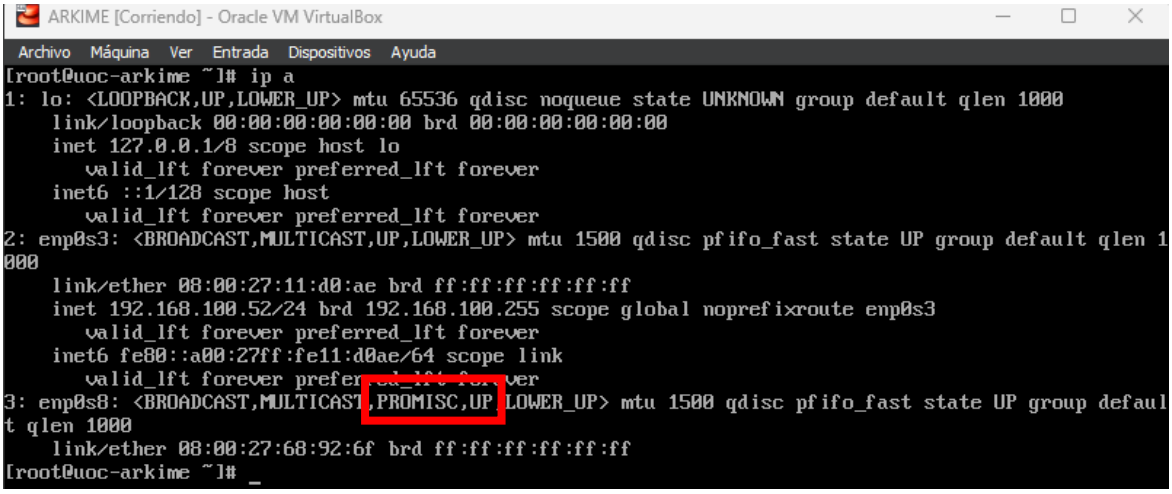


Imagen 12.52: Instalación Arkime (VIII)

A continuación, hay que descargar del repositorio oficial los paquetes de instalación de Arkime haciendo uso de la utilidad “wget” e instalarlos.

wget https://s3.amazonaws.com/files.molo.ch/builds/centos-7/arkime-4.4.0-1.x86_64.rpm

yum install arkime-4.4.0-1.x86_64.rpm

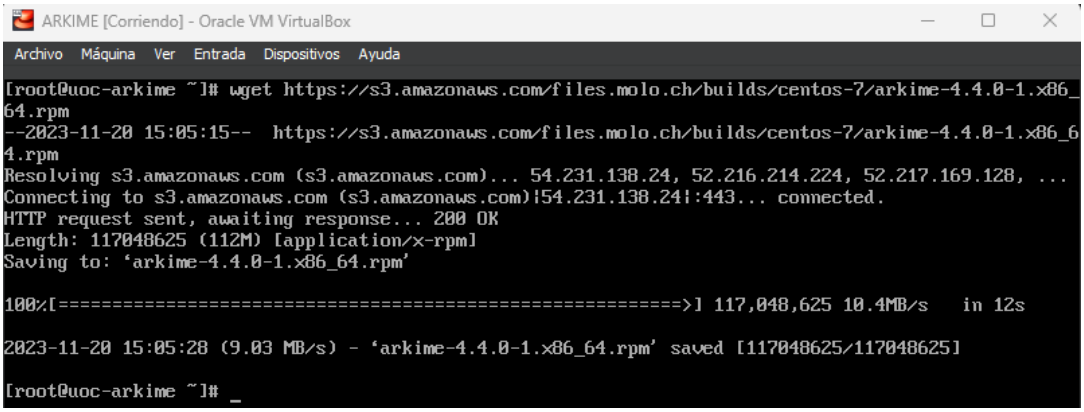


Imagen 12.53: Instalación Arkime (IX)

Una vez instalados los paquetes de Arkime se procede con la conexión del Arkime a la base de datos de Elasticsearch del SO.

12.2.2 Conexión con Security Onion

Para poder conectar Arkime a SO hay que abrir el puerto 9200 en el firewall de SO y crear el usuario de conexión.

Configuración de firewall desde la interfaz web de SO:

- Administration -> Configuration -> Firewall
- Activar las opciones avanzadas desde Options -> Interruptor
  - firewall -> hostgroups -> customhostgroup0 -> añadir IP de arkime
  - firewall -> portgroups -> customportgroup0 -> añadir puerto 9200
  - firewall -> role -> managersearch -> chain -> DOCKER-USER -> hostgroups -> customhostgroup0 -> portgroups -> añadir customportgroup0

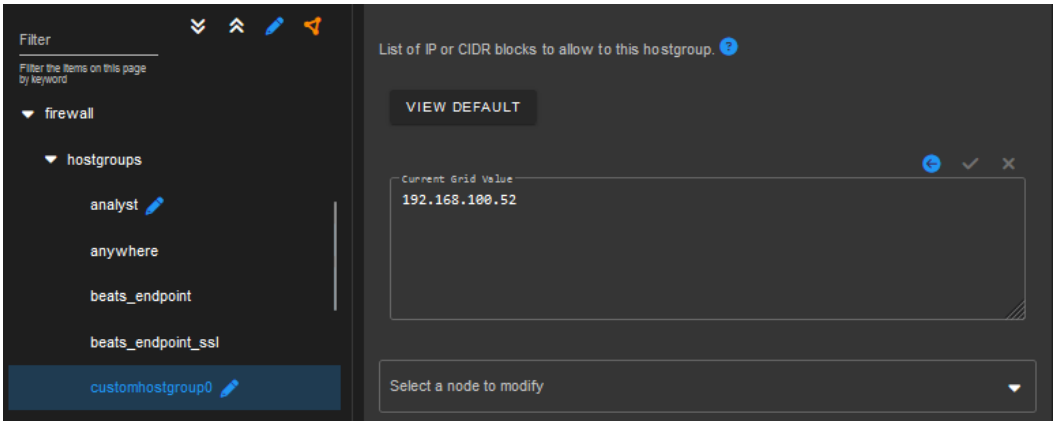


Imagen 12.54: Instalación Arkime (X)

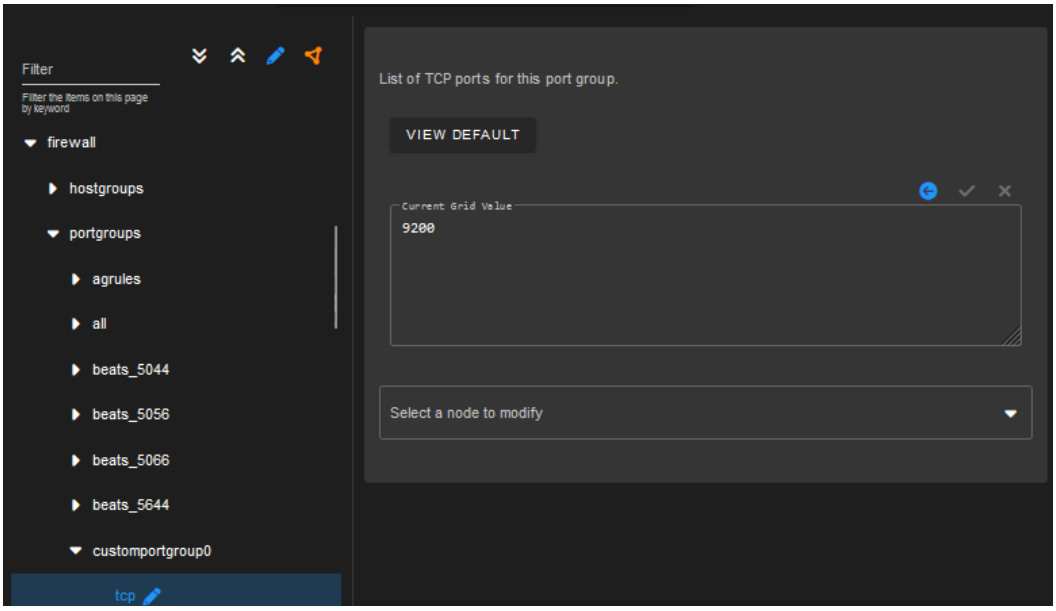


Imagen 12.55: Instalación Arkime (XI)

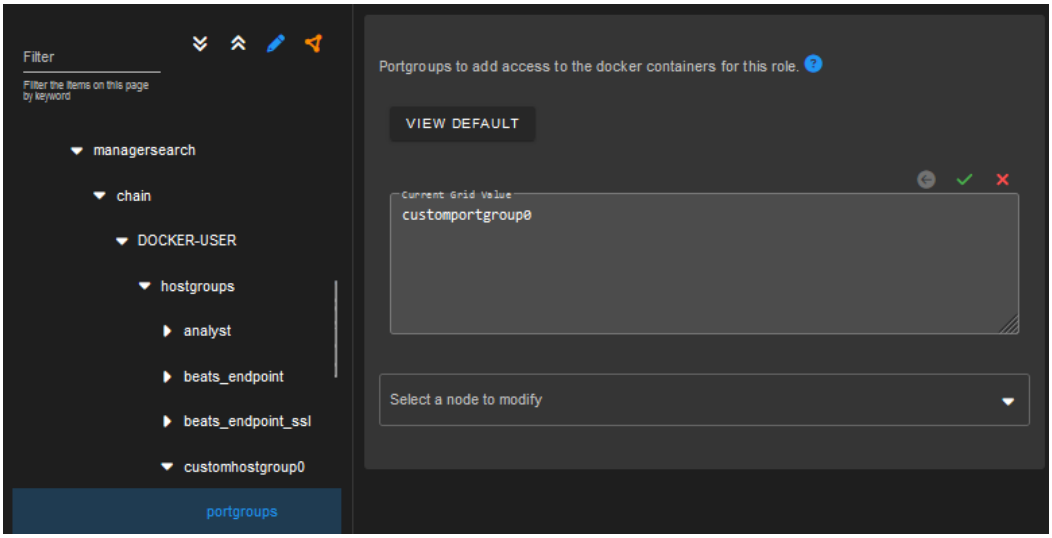


Imagen 12.56: Instalación Arkime (XII)

Creación del usuario de conexión desde interfaz web de Kibana. Hay que ir a Stack Management -> Users -> Create user y poner los siguientes datos, el nombre “arkime”, la contraseña “arkime” y el rol "superuser"

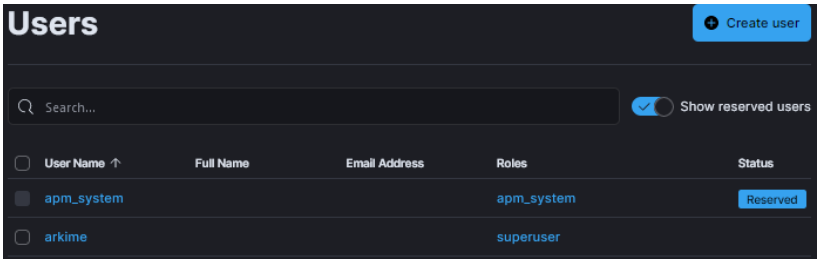


Imagen 12.57: Instalación Arkime (XIII)

Tanto el nombre como la contraseña pueden ser otros a elección del administrador.
Los siguientes pasos se realizan en la máquina virtual de Arkime y consisten en configuración básica, inicialización y configuración de la base de datos, creación del usuario de visualización de PCAPs e inicio de todos los servicios.

Para la configuración básica de Arkime hay que dirigirse al directorio “bin” y ejecutar el binario “Configure”.

cd /opt/arkime/bin/
./Configure
enp0s8
no
https://arkime:arkime 192.168.100.50:9200

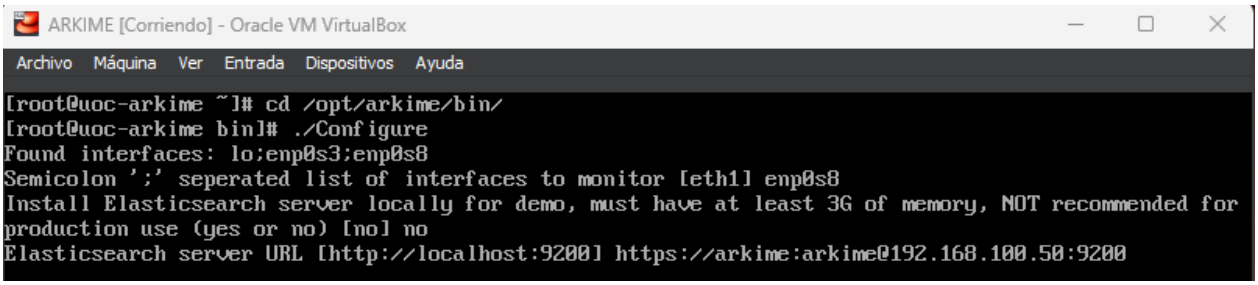


Imagen 12.58: Instalación Arkime (XIV)

El siguiente paso es inicializar y configurar la base de datos. Hay cambiar de directorio a “db” y ejecutar el script “db.pl”.

cd /opt/arkime/db
./db.pl --insecure --esuser arkime:arkime https://192.168.100.50:9200 init

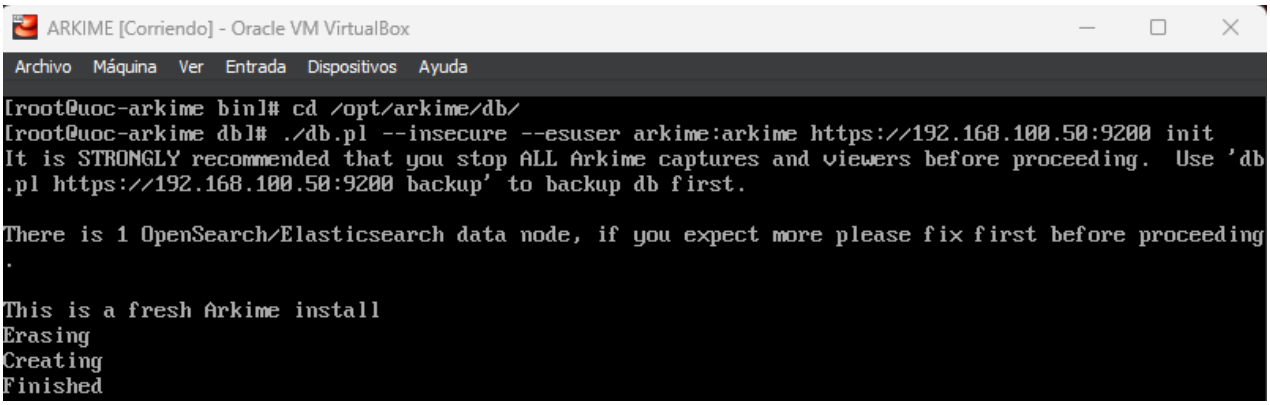


Imagen 12.59: Instalación Arkime (XV)

Una vez inicializada la base de datos hay que ajustar la rotación de indices de Elasticsearch.

./db.pl --insecure --esuser arkime:C1berdefens https://192.168.60.50:9200 ilm 25h 90d --history 30 --replicas 0*

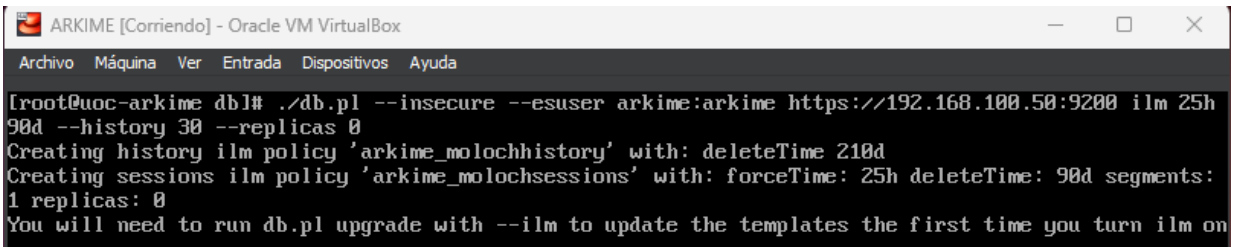


Imagen 12.60: Instalación Arkime (XVI)

./db.pl --insecure --esuser arkime:C1berdefens https://192.168.60.50:9200 upgrade –ilm*

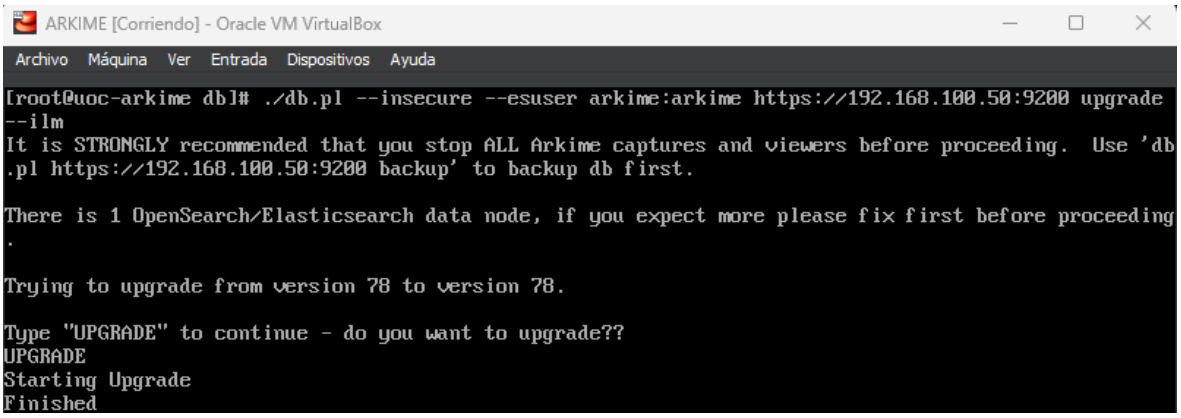


Imagen 12.61: Instalación Arkime (XVII)

Para verificar que la conexión esta activa se utiliza el siguiente comando:

./db.pl --insecure --esuser arkime:C1berdefens https://192.168.60.50:9200 info*

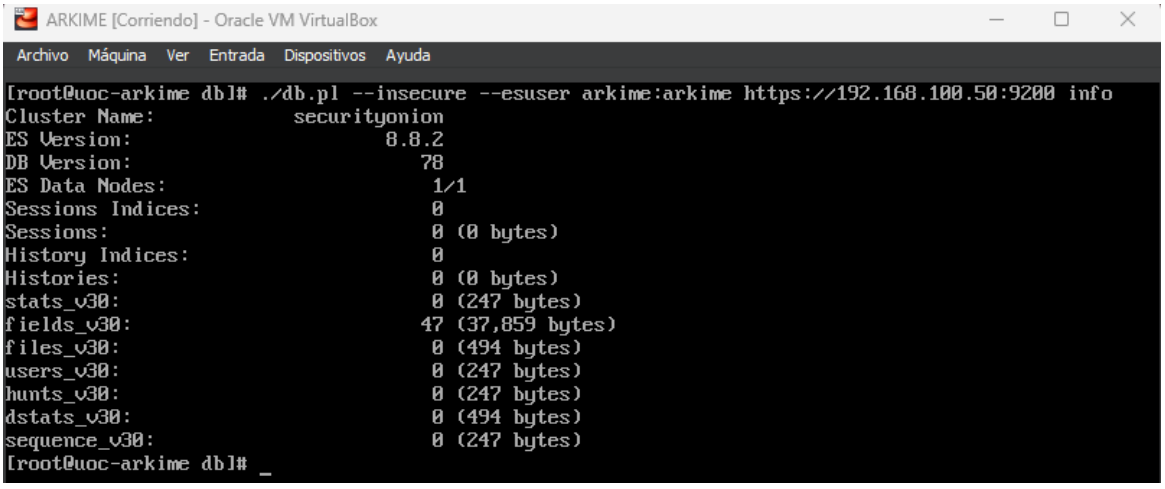


Imagen 12.62: Instalación Arkime (XVIII)

El siguiente paso es crear el usuario de visualizacion. Para ello hay que ir al directorio “bin” y ejecutar el script “arkime_add_user_sh”. El usuario creado es “admin” con contraseña “admin”.

cd /opt/arkime/bin
./arkime_add_user.sh --insecure admin admin admin --admin

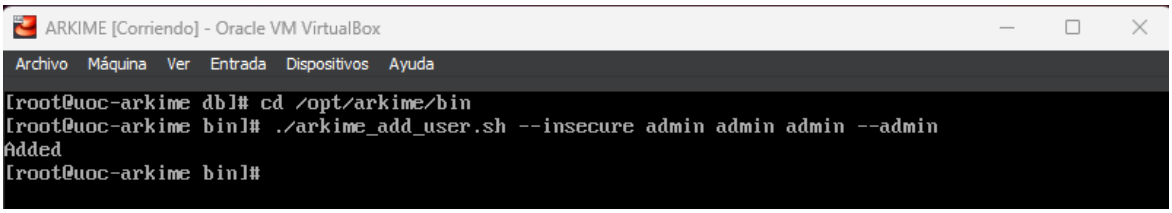


Imagen 12.63: Instalación Arkime (XIX)

Para terminar, es necesario iniciar los servicios y comprobar que funcionan.

systemctl daemon-reload

systemctl enable arkimecapture

systemctl enable arkimeviewer

systemctl start arkimecapture

systemctl start arkimeviewer

systemctl status arkimecapture

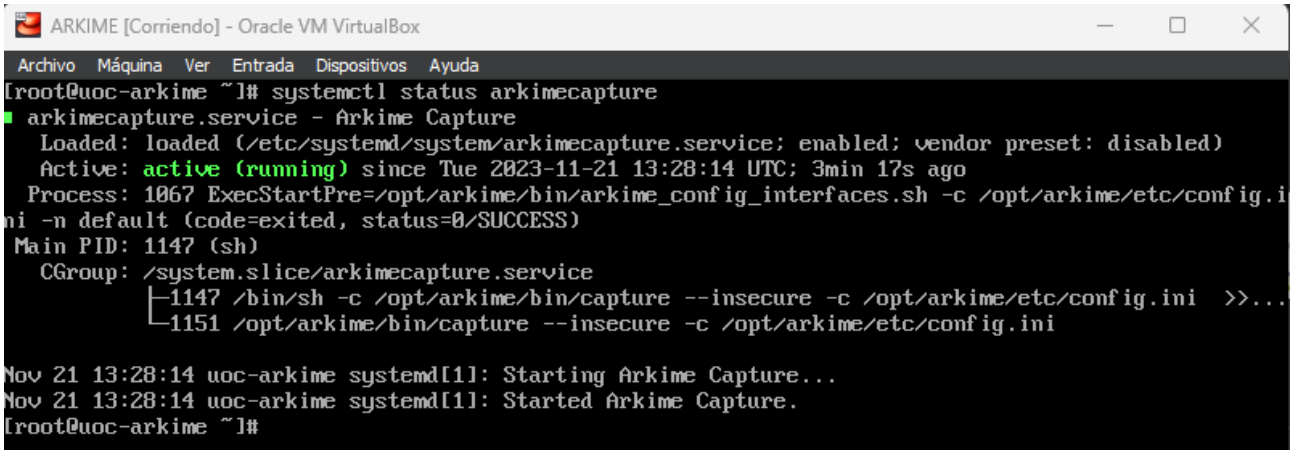


Imagen 12.64: Instalación Arkime (XX)

systemctl status arkimeviewer

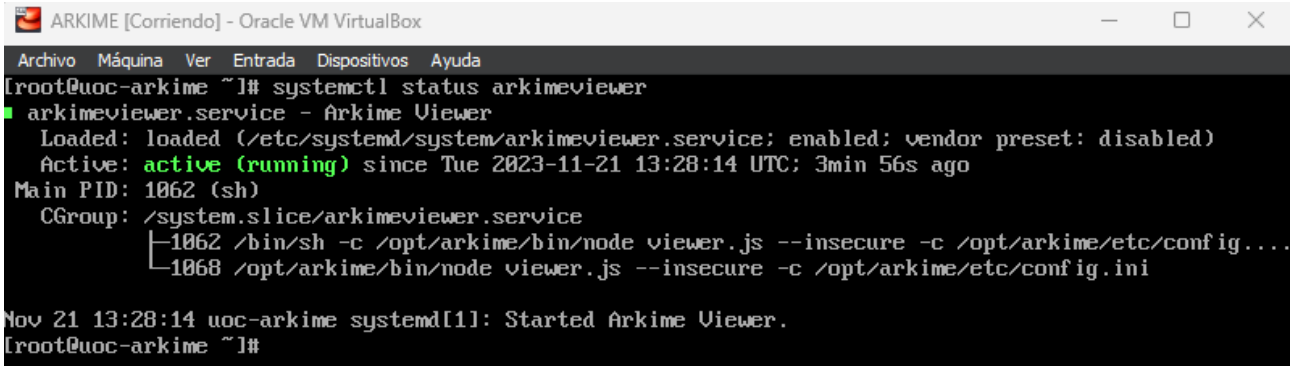


Imagen 12.65: Instalación Arkime (XXI)

El último paso es abrir el puerto 8005 en el firewall de Arkime para permitir el acceso a la interfaz web del mismo.

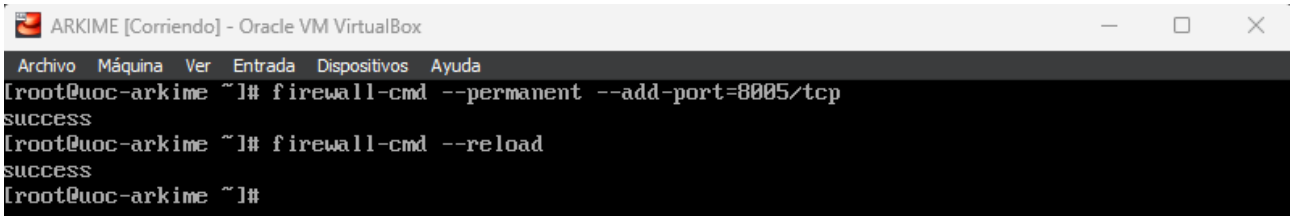


Imagen 12.66: Instalación Arkime (XXII)

Para verificar el funcionamiento del Arkime hay que entrar en la interfaz web usando la IP y el puerto 8005.

http://192.168.100.52:8005

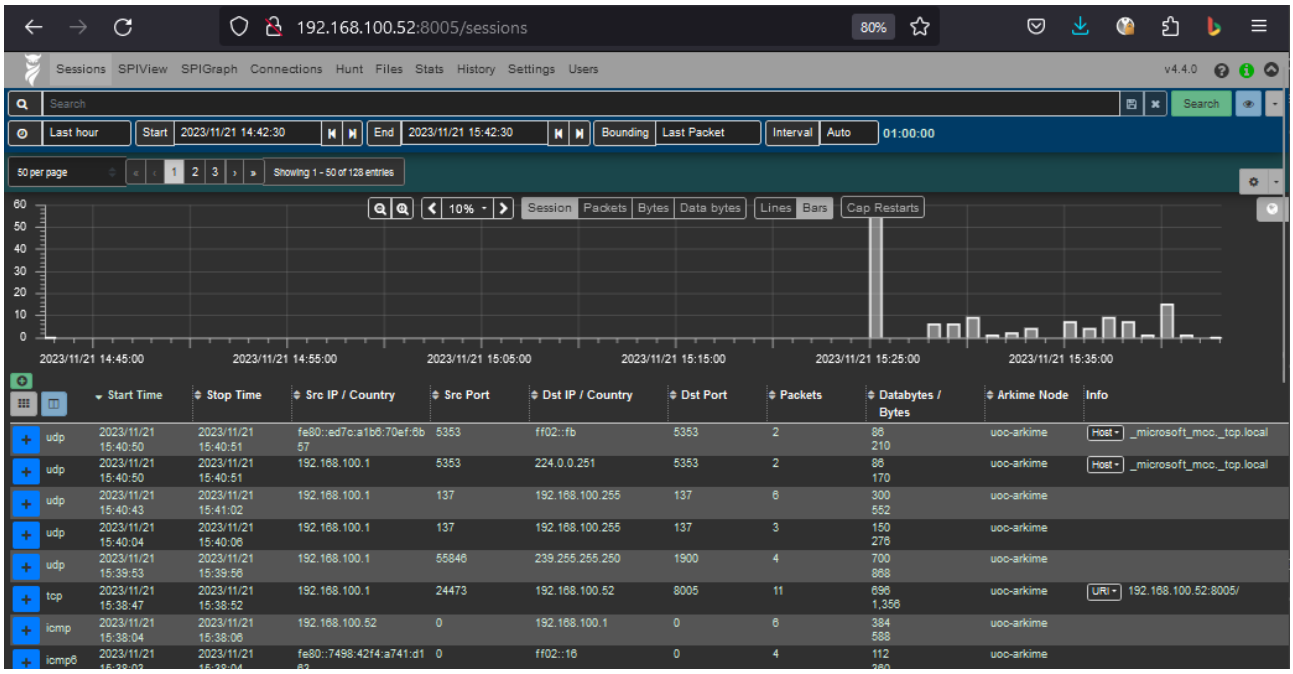


Imagen 12.67: Instalación Arkime (XXIII)

Para verificar la integración de Arkime con Elasticsearch de SO hay que ir a la interfaz web de Kibana y comprobar que se generan los índices de Arkime. Hay que ir a Stack Management -> Kibana (Data Viewes) -> Create Data View y crear una visualizacion con nombre “Arkime” y patron “arkime_sessions3*”.

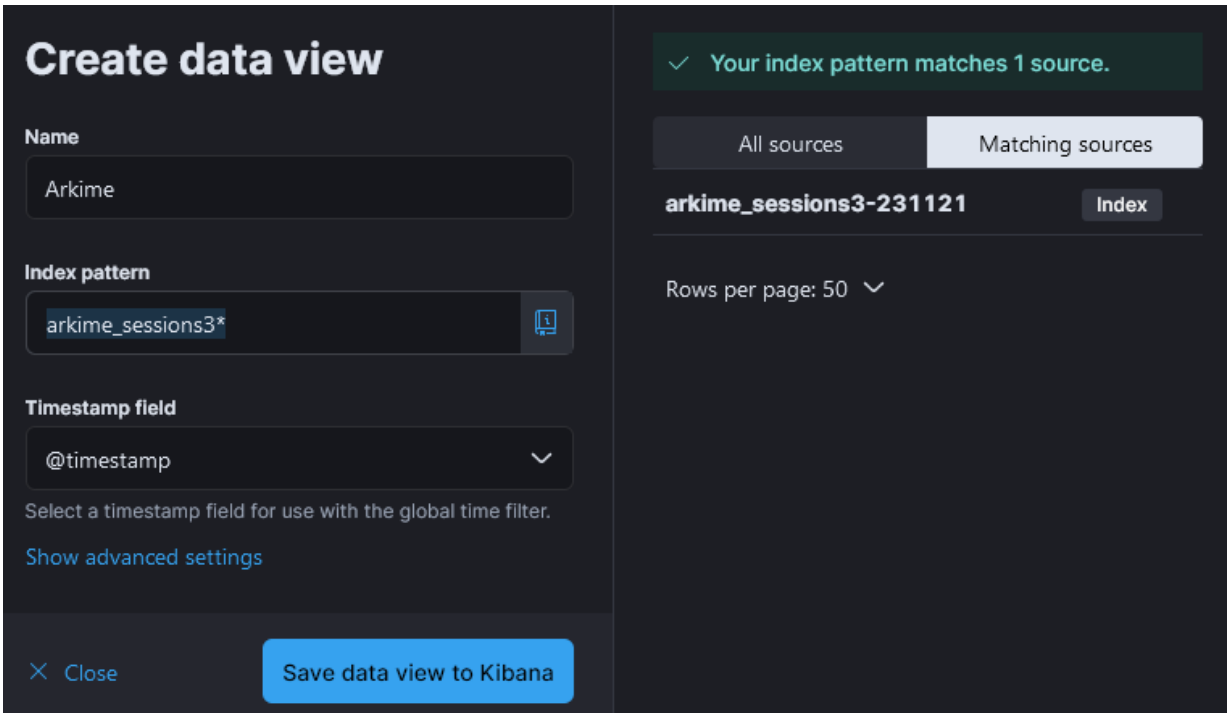


Imagen 12.68: Instalación Arkime (XXIV)

Una vez creada la visualizacion se puede visualizar desde el apartado “Discover” filtrando por “Arkime”.

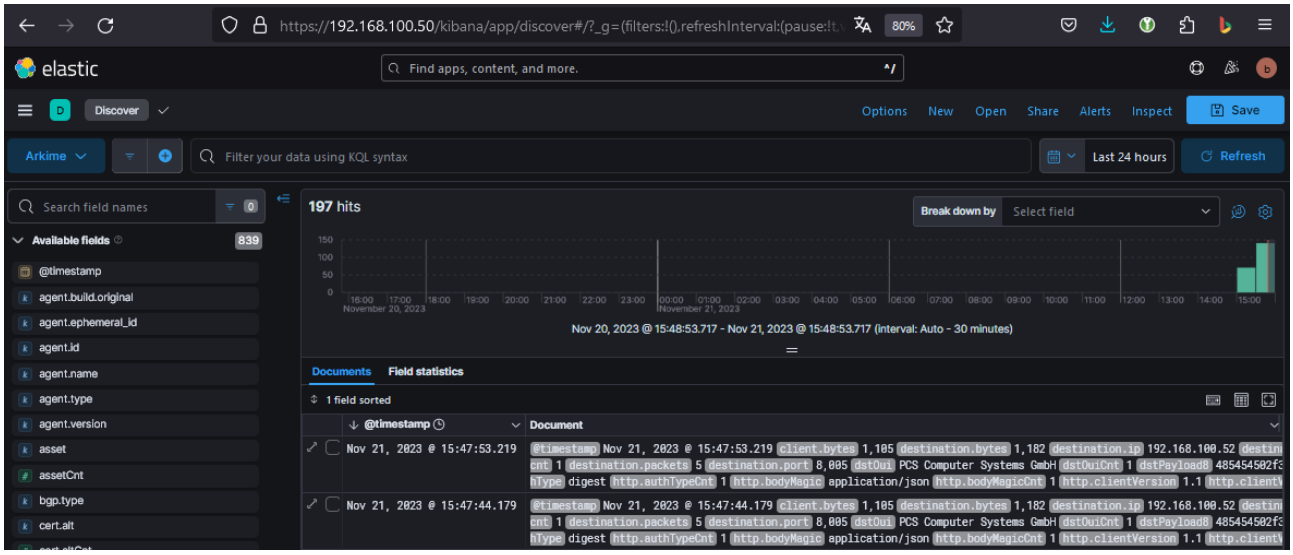


Imagen 12.69: Instalación Arkime (XXV)

12.3 Anexo III – Despliegue y configuración de Elastic Agent

12.3.1 Instalación en el cliente con Windows 10

Previamente a la instalación del agente es necesario permitir que este pueda conectarse al servidor de Elastic Fleet del SO. Para ello, en interfaz web de SO hay que ir a:

- Adminstration -> Configuration -> firewall -> hostgroups -> elastic_agent_endpoint y añadir la IP o la red (X.X.X.X/Y) donde se instalarán los agentes.

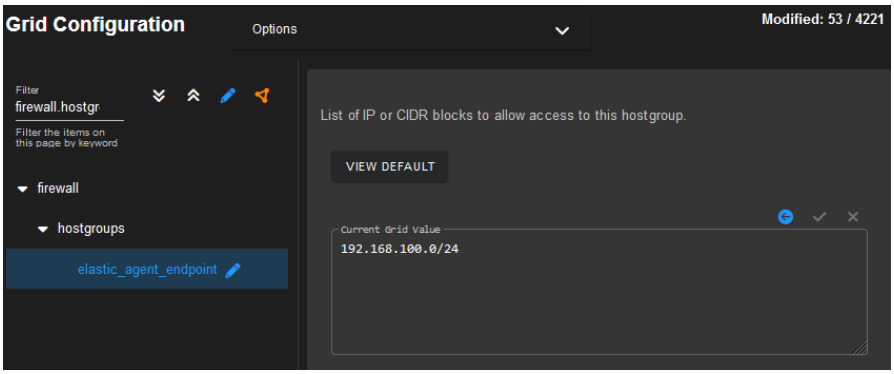


Imagen 12.70: Instalación Elastic Agent (I)

Una vez abierto el firewall hay que ir al apartado “Downloads” de SO y descargar el paquete de instalación de ElasticAgent para Windows.

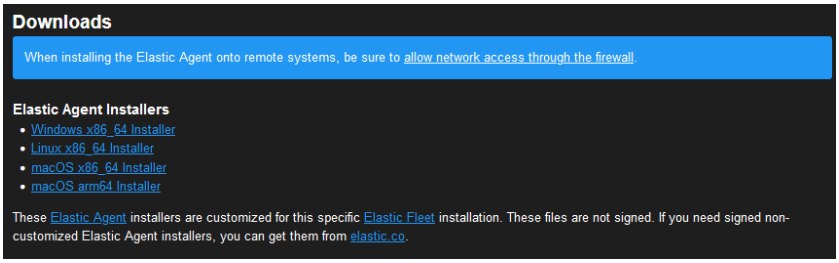


Imagen 12.71: Instalación Elastic Agent (II)

Una vez descargado el instalador del agente, es necesario ejecutarlo con derechos de administrador. Una vez terminada la instalación hay que verificar el log de instalación y comprobar que el agente aparece desplegado en Kibana en el apartado de “Elastic Fleet”.

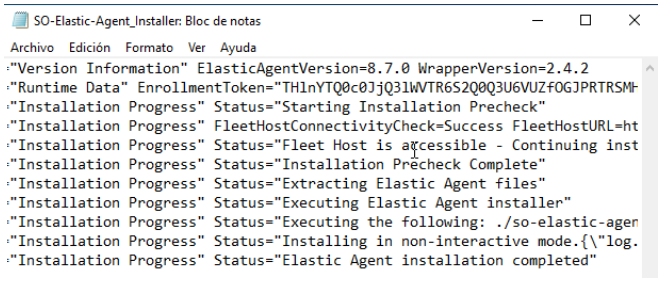


Imagen 12.72: Instalación Elastic Agent (III)

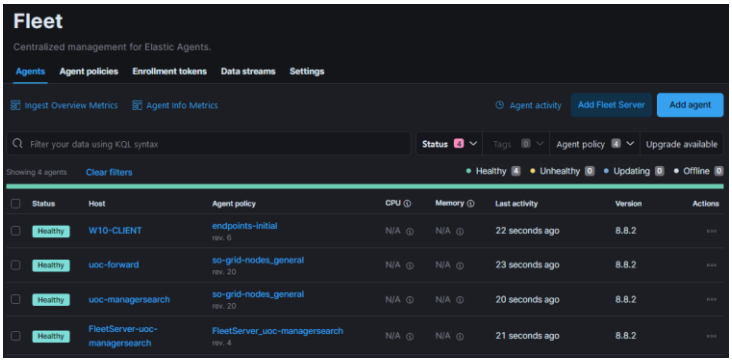


Imagen 12.73: Instalación Elastic Agent (IV)

12.3.2 Instalación en el cliente con Ubuntu

Al igual que con el agente para Windows 10, es necesario abrir el firewall del SO para permitir la comunicación entre el agente y el servidor de Elastic Fleet y descargar el paquete de instalación para Linux desde el apartado de “Downloads” de SO.

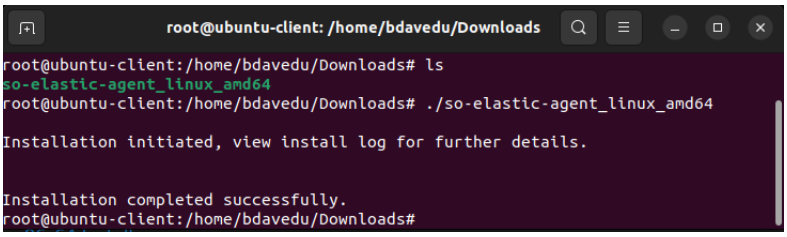


Imagen 12.74: Instalación Elastic Agent (V)

Una vez instalado hay que comprobar que el agente aparece en Elastic Fleet.

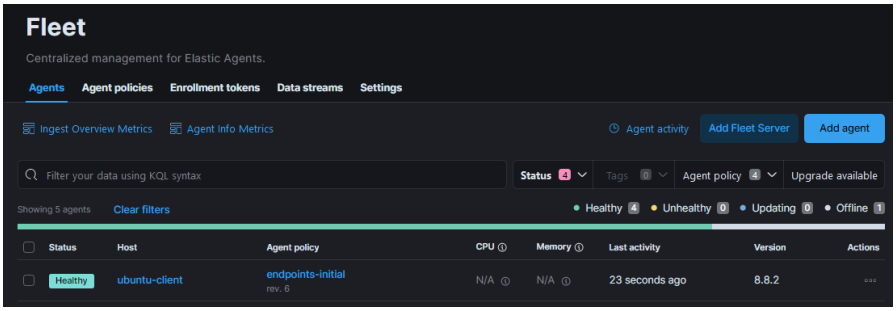


Imagen 12.75: Instalación Elastic Agent (VI)

12.4 Anexo IV – Despliegue y configuración de pfSense

La instalación de este firewall gratuita se resume en los siguientes pasos:

1. Descargar la imagen de instalación desde la página oficial: https://www.pfsense.org/download/

2. Crear la máquina virtual con los recursos recomendados por el desarrollador e iniciar la instalación con la imagen descargada previamente.

3. Aceptar el acuerdo de licencia

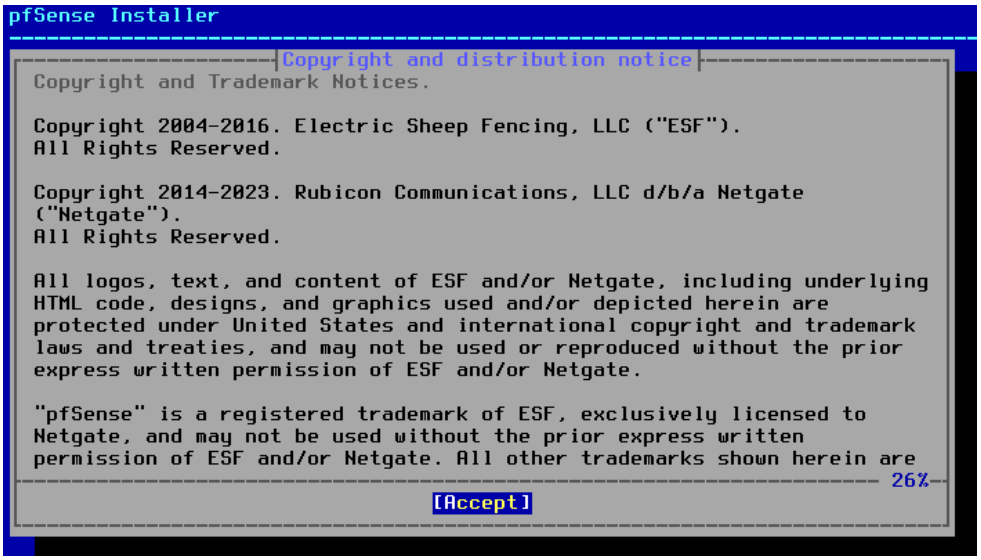


Imagen 12.76: Instalación pfSense (I)

4. Confirmar la instalación y esperar a que termine. Una vez finalizada la instalación hay que extraer la imagen de instalación y reiniciar la máquina virtual.

Imagen 12.77: Instalación pfSense (II)

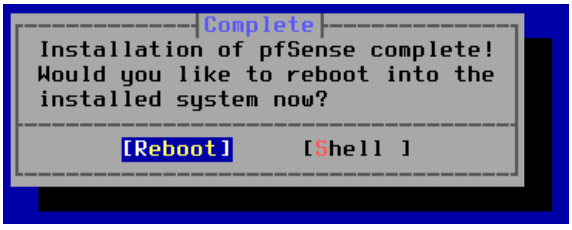


Imagen 12.78: Instalación pfSense (III)

5. Una vez arrancada la máquina virtual hay que configurar las interfaces de red.

-Asignar las interfaces (opción 1)

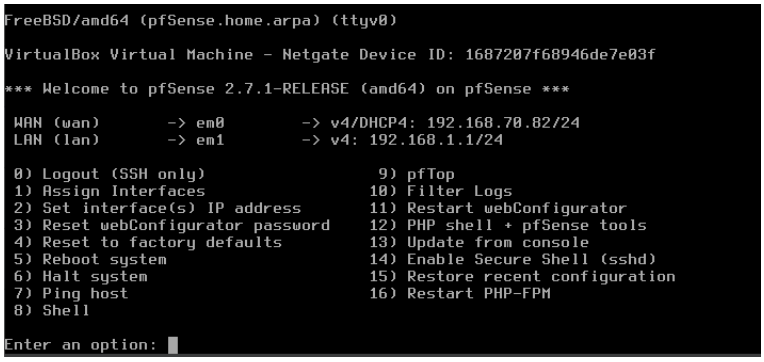


Imagen 12.79: Instalación pfSense (IV)

No tocar las VLANs

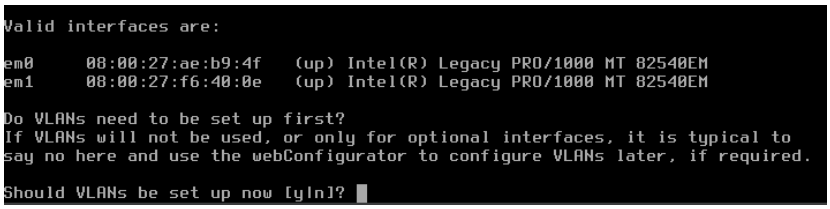


Imagen 12.80: Instalación pfSense (V)

Escoger la interfaz que hará de WAN (salida a Internet).

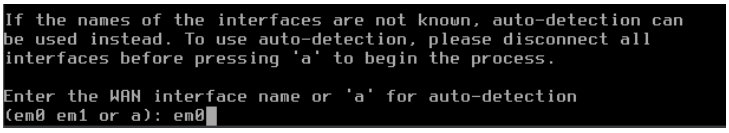


Imagen 12.81: Instalación pfSense (VI)

Escoger la interfaz que hará de LAN (red solo-anfitrión).

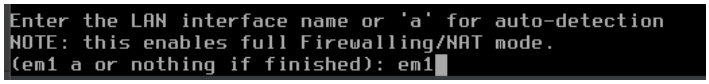


Imagen 12.82: Instalación pfSense (VII)

Confirmar la selección.

-Configurar el direccionamiento IP (opción 2).

Dejar la asignación de IP para WAN por DHCP.

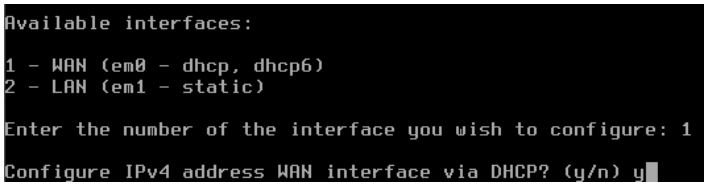


Imagen 12.83: Instalación pfSense (VIII)

Configurar la IP de LAN de forma estática con la IP 192.168.100.10/24.

```
Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.100.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Imagen 12.84: Instalación pfSense (IX)

```
The IPv4 LAN address has been set to 192.168.100.10/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.100.10/
```

Imagen 12.85: Instalación pfSense (X)

6. Terminada la configuración básica, es necesario entrar vía web para terminar de modificar los ajustes de relacionados con DNS, contraseñas por defecto o las reglas de firewall.

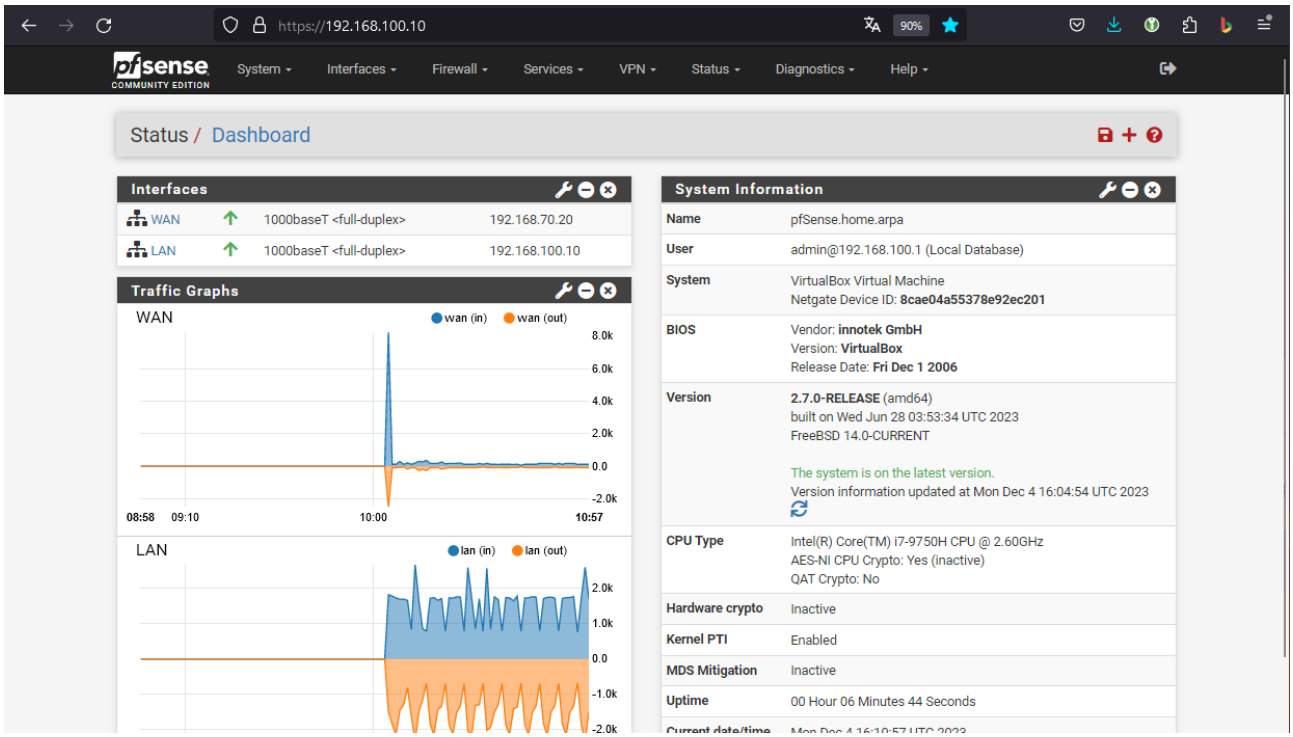


Imagen 12.86: Instalación pfSense (XI)

12.5 Anexo V – Despliegue y configuración de Kali Linux

La instalación de este sistema de pentesting es sencilla y se resume en los siguientes pasos:

1. Descargar de la máquina virtual para VirtualBox de la página oficial en el siguiente enlace:

   https://www.kali.org/get-kali/#kali-virtual-machines

2. Importar la máquina virtual descargada en el Virtual Box y configurar los recursos.

Imagen 12.87: Despliegue Kali Linux (I)

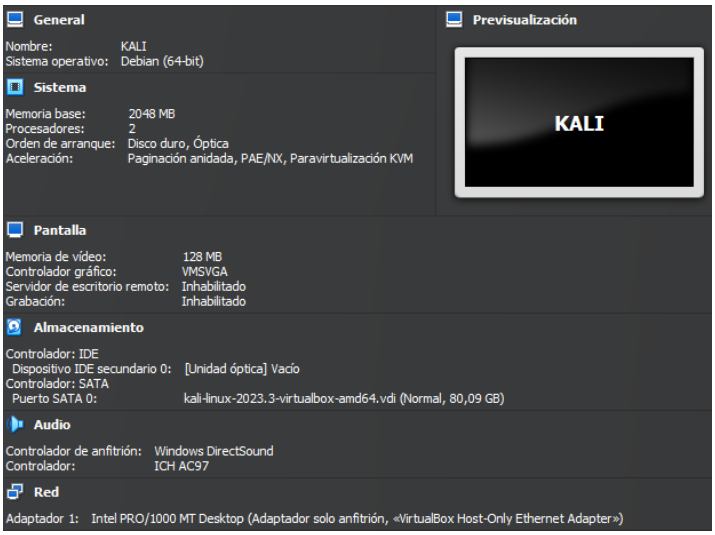


Imagen 12.88: Despliegue Kali Linux (II)

3. Arrancar la máquina virtual y configurar el direccionamiento IP.

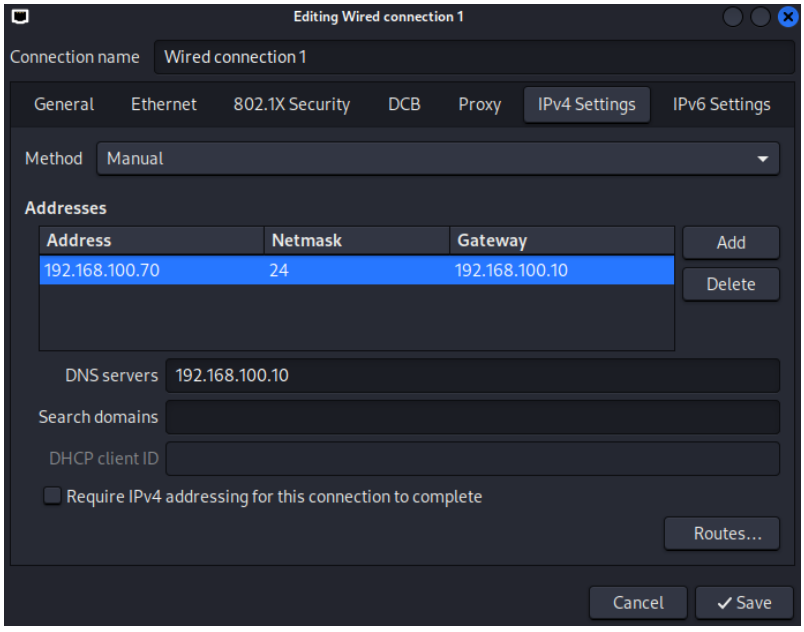


Imagen 12.89: Despliegue Kali Linux (III)

4. Verificar el funcionamiento de la conexión.

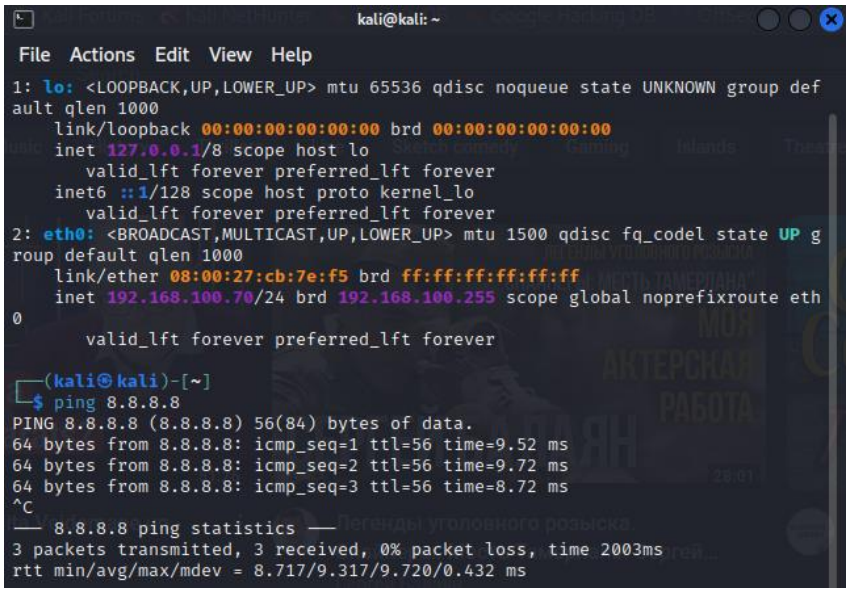


Imagen 12.90: Despliegue Kali Linux (IV)