PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERIA EN TECNOLOGIAS DE LA INFORMACIÓN

TRABAJO DE TITULACIÓN

ANÁLISIS DEL TRÁFICO DE RED MEDIANTE EL USO DE LA HERRAMIENTA SURICATA COMO IDS

AUTOR:

ARIEL FERNANDO BENAVIDES MORETA

DIRECTOR:

MIGUEL DIMITRI ORTIZ NAVARRETE MTR.

QUITO DM, OCTUBRE DE 2024

AGRADECIMIENTO

Durante el proceso de del desarrollo del presente trabajo de titulación, quiero agradecer a todas las personas que me acompañaron durante todo este proceso, no solo en el desarrollo del presente trabajo, sino durante toda mi carrera universitaria. Quiero agradecer a mi familia, mis hermanas, mis compañeros, mis amigos y a las personas que más amo, me han apoyado y han estado conmigo durante todo este tiempo sobre todo en los momentos más difíciles por los que he pasado.

Quiero agradecer a mi papá, Joffre, porque él siempre me ha motivado y me ha inspirado a seguir adelante, a siempre seguir con mis estudios y sobre todo nunca rendirme. Gracias, papá, gracias a ti pude culminar este enorme logro, gracias a ti pude lograr un sueño y culminar con el desarrollo del presente trabajo, eres una luz en mi vida y siempre has estado conmigo, en cualquier momento que necesito y por eso quiero decirte gracias. Quiero agradecer a mi mamá, Priscila, porque ella es una mujer que me ha enseñado el valor de la perseverancia, de jamás rendirme y sobre todo culminar mis estudios y siempre seguir adelante, junto a mis proyectos y con el amor de madre que me ha brindado y me ha apoyado durante este proceso simplemente quiero decirte gracias. Quiero agradecer a mi hermana, Pamela, la persona más valiente que conozco del planeta. Pame, eres la mujer más fuerte que he conocido, tus logros y tus metas me motivan a seguir adelante, eres única y me siento orgulloso de ser tu hermano, me has enseñado mucho y sobre todo me has dado fuerza y luz en mis días más difíciles. Además, quiero agradecer a las demás personas que me han acompañado en este proceso, a ti, mi primo, alguien que considero mi hermano, Sebas, porque siempre me has enseñado el valor de la responsabilidad y sobre todo porque has estado conmigo durante todo este proceso. Me has enseñado mucho y siempre voy a estar agradecido por cada consejo, cada mano, cada paso que me has acompañado durante este proceso.

Gracias a todos ustedes por estar siempre en este proceso conmigo apoyándome y sobre todo alentándome a seguir adelante, a jamás rendirme. Simplemente quiero agradecer y decir que este logro es gracias a ustedes.

RESUMEN

Actualmente, vivimos en una época de revolución digital en donde las redes informáticas son uno de los papeles más fundamentales dentro de las empresas y organizaciones, ya que son el medio por donde se transmiten los datos sensibles, se ejecutan los procesos críticos y ayudan a conectar sistemas. Así, como existe un crecimiento potencial en las redes informáticas, también trajo consigo un aumento en cantidad tanto en ciberdelincuentes como en amenazas sofisticadas. Dentro de estas amenazas se encuentran ataques de tipo denegación de servicio, ataque por intrusiones, malware y otras actividades cibernéticas maliciosas. Por este motivo, es necesario utilizar herramientas robustas y de personal capacitado para que pueda contrarrestar este tipo de ataques y delitos cibernéticos, con el fin de mitigar riesgos.

Suricata es una herramienta open source (software libre) que funciona como un sistema de detección de intrusos (IDS) además de otras capacidades como por ejemplo prevención de intrusos (IPS). Esta herramienta ha ganado popularidad dentro del mundo de la ciberseguridad ya que tiene una gran capacidad de monitorear y analizar grandes cantidades de datos del tráfico de red dentro de cualquier ambiente en tiempo real.

A diferencia de otros IDS, Suricata utiliza múltiples hilos para así poder procesar grandes volúmenes de datos, lo que lo convierte en una solución fiable y eficiente. Además, mediante el análisis del tráfico de red mediante el uso de la herramienta Suricata, ofrece la oportunidad de poder verificar diferentes comportamientos anormales y anómalos que existen en el tráfico, por lo que puede ayudar a la implementación de diferentes políticas de seguridad además de estrategias para implementar una seguridad proactiva.

En el presente trabajo de titulación, se va a realizar un análisis del tráfico de red utilizando Suricata como herramienta de IDS. El análisis que se va a realizar va a ser en una PYME en la ciudad de Quito. El análisis del tráfico de red que se va a realizar va a ser dentro de un ambiente controlado en donde los empleados se conectan hacia el internet para poder realizar distintas actividades, por lo que la herramienta suricata va a estar alojado dentro de su entorno para recibir y capturar el tráfico generado. Una vez que reciba el

tráfico, se va a visualizar los datos capturados con la herramienta Zui. Zui es una herramienta para visualizar grandes volúmenes de datos de manera estructurada. Zui tiene la función de realizar consultas para filtrar y mostrar los resultados a base de tablas. También, se va a utilizar la herramienta Power BI para poder visualizar, generar y analizar gráficos de manera interactiva.

TABLA DE CONTENIDOS

TABLA DE ILUSTRACIONES

CAPÍTULO I: INTRODUCCIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad, las empresas de todos los tamaños, dependen en gran medida de sus redes informáticas para el manejo de información crítica, los datos y la información logística. Estas redes soportan sistemas de gestión de cobros, bases de datos de clientes, comunicación entre sucursales o colaboradores, además de la comunicación entre sus clientes con los portales, etc. Este manejo de información las convierte en un objetivo atractivo para ciberdelincuentes que buscan acceder a datos sensibles para así tener acceso a la información crítica o interrumpir operaciones que manejan las mismas.

Una de las principales amenazas para este tipo de empresas son los ataques cibernéticos, que incluyen desde intrusiones no autorizadas hasta ataques más sofisticados como el ransomware o el phishing. A pesar de que el caso de estudio es en una empresa mediana, las implicaciones de un ataque cibernético exitoso pueden ser devastadoras, las cuales traen pérdida de datos sensibles de clientes, interrupciones en los procesos operativos, daños financieros y pérdida de confianza por parte de los clientes. Sin embargo, muchas de estas empresas no cuentan con recursos suficientes para implementar costosos sistemas de seguridad ni con personal especializado para gestionar estos riesgos de manera eficiente.

El problema que se plantea en este trabajo es la falta de una estrategia clara y eficiente para analizar el tráfico de red y detectar amenazas de seguridad cibernética, poniendo en riesgo la integridad de los sistemas y la protección de datos sensibles. A través de un estudio de caso en una empresa dedicada a tratar asuntos judiciales, se investigará cómo la implementación de Suricata como IDS puede contribuir a mejorar la seguridad de la red, optimizando la detección de intrusiones y minimizando el riesgo de ataques cibernéticos.

1.2 JUSTIFICACIÓN

Uno de los mayores desafíos que vivimos en la era digital que atravesamos actualmente es la protección de las redes informáticas. Es importante detectar patrones y

amenazas que pueden comprometer con las redes informáticas, esto con el fin de proteger los datos más críticos de una empresa o de una organización.

Dentro del caso de estudio, se va a realizar el análisis de la infraestructura de red de la empresa con la que se va a trabajar. Es fundamental entender como está estructurado la red empresarial para así determinar los puntos y procesos más críticos que maneja. Con esa información, se puede realizar el análisis de tráfico y analizar posible detección de intrusos mediante el uso de la herramienta Suricata.

Gracias al análisis, la empresa donde se aplica el estudio puede beneficiarse considerablemente al punto de poder adoptar las medidas necesarias en cuanto a la aplicación de diferentes políticas de seguridad. Esto va a ayudar a poder mitigar y disminuir brechas que pueden exponer los datos más críticos, además de conocer patrones o comportamientos sospechosos que puedan afectar en un futuro las diferentes operaciones con las que trabaja.

Además, Suricata permite realizar un análisis detallado y segmentado del tráfico, contribuyendo a una mayor precisión en la identificación de actividades maliciosas y reforzando la seguridad de la red junto a su capacidad avanzada de monitoreo y análisis en tiempo real.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Realizar un análisis del tráfico de red en una empresa mediana dedicada a tratar asuntos judiciales mediante el uso de la herramienta Suricata como sistema de detección de intrusos (IDS), con el fin de mejorar la detección de amenazas cibernéticas y optimizar la seguridad de la red.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar la infraestructura de red de la empresa del caso de estudio para así identificar los puntos y procesos críticos que requieren monitoreo constante.
- Aplicar la herramienta Suricata dentro del entorno de la empresa para así poder realizar monitoreo y analizar el tráfico más crítico de red.

- Evaluar la efectividad de la herramienta como detección de intrusos en el contexto, midiendo su capacidad para identificar amenazas potenciales con precisión y rapidez
- Analizar los hallazgos obtenidos del monitoreo del tráfico de red con Suricata y proponer recomendaciones de mejora para fortalecer la seguridad de la infraestructura de red de la empresa.

1.4 UNIDAD DE ANÁLISIS

La unidad de análisis se va a ser en una empresa mediana de once a cincuenta empleados que tiene sede en Quito, Pichincha. El tipo de empresa es de financiación privada y se dedica a brindar servicios tecnológicos y operativos en consultoría y servicios a empresas. Esta empresa es especializada en brindar un servicio integral en prevención de lavado de activos, providencias judiciales y relacionados a las áreas de cumplimiento y operativa de sujetos obligados a reportar a entidades de control gubernamental en el Ecuador. Una de las actividades de la empresa es generar oficios que son cartas de respuesta que generan por las providencias. Una vez que se generan los oficios las empresas envían estos oficios vía correo de manera masiva todos los días. La empresa maneja en un servidor en donde se encuentran diferentes máquinas virtuales de cada cliente con los que trabaja.

1.5 ALCANCE

El presente trabajo de investigación se va a enfocar en realizar un análisis del tráfico de red de la empresa que se seleccionó usando la herramienta Suricata como sistema de detección de intrusiones (IDS). El propósito principal es realizar un análisis detallado de como esta herramienta permite identificar amenazas y patrones de tráfico inusuales y sospechosos en el entorno de red de la empresa. El análisis que se va a realizar va a ser dentro del servidor donde se alojan las máquinas virtuales de los distintos clientes en donde realizan la generación de oficios y el envío masivo de correos. Esta investigación cubrirá un periodo específico de monitoreo simulado en el que se recopilarán datos sobre posibles ataques, comportamientos anómalos y otros eventos que puedan afectar a la seguridad de la red.

La presente investigación no incluirá cambios físicos en la red de la empresa ni aplicación de políticas de seguridad sobre la infraestructura. Esto es ya que el enfoque principal es el análisis potencial de la red empresarial y las limitaciones de Suricata para detectar intrusiones de la empresa, evaluando así su efectividad y eficiencia de la herramienta.

CAPÍTULO II: MARCO TEÓRICO

2.1 CONCEPTOS Y TOPOLOGÍAS DE RED

La conexión de red, también denominado interconexión informática, es el proceso de conectar dos o más dispositivos informáticos, por ejemplo, la conexión entre dos o más ordenadores, dispositivos móviles, enrutadores, o cualquier otro dispositivo tecnológico que pueda permitir la transmisión y el intercambio de información de recursos. El conjunto de dos o más dispositivos informáticos que estén conectados en una red y puedan recibir y transmitir información se lo denomina una red informática (IBM, 2021).

Los dispositivos conectados en la red se basan en protocolos que son reglas que describen como se deben transmitir o intercambiar datos dentro de la red. Antes de la creación de las redes informáticas, los ingenieros debían mover los ordenadores o equipos de trabajo sitio a sitio para poder compartir los datos entre sí, era una tarea muy pesada y muy poco práctica ya que en el pasado los equipos que se utilizaban eran muy pesados. Por ello para poder simplificar el proceso nació la necesidad de buscar una alternativa de poder conectar los equipos de comunicación sin la necesidad de trasladarlos de un sitio a otro, especialmente para los trabajadores de administración. El Departamento de Defensa de los Estados Unidos (ARPA) financió la creación de la primera red informática operativa ARPANET a finales de la década de 1960 (IBM, 2021).

Desde entonces, las prácticas de conexión de red hasta la actualidad han ido evolucionando de manera considerable. Las redes informáticas actuales facilitan y mejoran la comunicación a gran escala entre dispositivos y como resultado la comunicación entre personas. El internet, las búsquedas en línea, el envío de mensajes ya sea por correo o aplicaciones de comunicación como WhatsApp, el intercambio de audio y video, las redes

sociales, etc. Todas estas posibilidades y usos se han dado gracias a evolución de las redes informáticas.

Las redes informáticas son fundamentales para nuestro diario vivir ya que están presentes en muchos aspectos de la vida moderna y también para el funcionamiento de las empresas modernas (IBM, 2021). Las redes informáticas ofrecen muchos beneficios tales como:

- Transferencia de datos eficiente.
- Intercambio de conocimientos racionalizado.
- Mayor almacenamiento de datos.
- Mayor seguridad y protección de datos.

Para el presente trabajo de integración curricular resulta fundamental comprender el significado y la importancia de las redes informáticas, ya que estas constituyen la base para el intercambio de datos y recursos entre dispositivos. Este conocimiento complementa el análisis del tráfico de red que se va a realizar con la herramienta Suricata, permitiendo así una evaluación más eficaz del tráfico de la red dentro del caso de estudio. Además, gracias al el resultado del análisis, puede mejorar de manera significativa la gestión de las redes informáticas al establecer una comunicación más segura y eficiente entre los dispositivos de la red corporativa, optimizando tanto la operación como la seguridad de los sistemas.

2.1.1 REDES LAN Y REDES WAN

Las redes de área local (LAN) y las redes de área amplia (WAN) son los dos tipos de redes más fundamentales que tienen las redes informáticas ya que se consideran como la columna vertebral de los sistemas de comunicación modernos (EITCA Academy, 2024). Entender el significado y las diferencias de ambos tipos de redes es fundamental ya que se puede comprender cómo se transmiten y se comparten los datos dentro de un hogar, una organización y el internet en general a nivel global.

Las redes LAN (Local Area Network, por sus siglas en inglés) son un grupo servidores, computadores o dispositivos periféricos que se conectan mediante una misma línea de comunicaciones de manera física, o mediante un enlace inalámbrico a un servidor

dentro de un área geográfica pequeña. Un ejemplo de una LAN puede ser dispositivos conectados dentro de un hogar o diferentes dispositivos conectados dentro de una oficina (Hwang, 2021).

Las redes WAN (Wide Area Network, por sus siglas en inglés) es una red más amplia que ofrece una conexión entre oficinas, centro de datos, etc. Esta red amplia tiene un alcance de más de 50 km. Esta red se la denomina amplia ya que se extiende más allá de un solo lugar, para así incluir múltiples ubicaciones localizada a lo largo de una zona geográfica concreta, incluso por todo el mundo. Una WAN puede ser una conexión de una red LAN que se conecta con otras redes LAN siendo así una red de redes (GeeksforGeeks, 2017).

Principalmente, las redes LAN se utilizan para la comunicación interna de una organización. Por ejemplo, dentro de una empresa es común utilizar una red local que se utilice para comunicar computadoras, impresoras, servidores y cualquier otro dispositivo que se utilice para poder transmitir información y facilite el intercambio de recursos y la comunicación. Otro ejemplo de uso de las redes LAN es dentro de un hogar ya que permite conectar de igual manera múltiples dispositivos ya sea computadoras, teléfonos inteligentes, impresoras, entre otros (EITCA Academy, 2024).

Mientras tanto, las redes WAN se utilizan para necesidades de comunicación más amplias que se extienden más allá de los límites de un hogar o más allá de los límites de una oficina en particular. Las redes WAN dan la posibilidad de permitir a las organizaciones conectarse a diversas sucursales, centros de datos y empleados de manera remota entre diferentes ciudades, países o incluso continentes (EITCA Academy, 2024).

En el presente trabajo de integración curricular, el estudio de las redes LAN y WAN resulta crucial ya que constituye la base de la infraestructura de red para cualquier organización. Para la empresa donde se va a realizar la evaluación, la identificación del tipo de red es fundamental para poder establecer un marco claro de los puntos estratégicos donde se llevará acabo el análisis y poder detectar posibles vulnerabilidades. Al conectar la red LAN interna de la empresa con ubicaciones remotas externas a través de conexiones de largo alcance, pone en riesgo la seguridad de los datos que maneja la empresa dentro de su

red interna, como la conexión hacia el Internet. La implementación de Suricata dentro de la red corporativa podrá analizar el tráfico proveniente de redes externas, detectando posibles intrusiones o posibles patrones de seguridad sospechosos que puedan comprometer con la seguridad de la red.

2.1.2 TOPOLOGÍAS DE RED

La topología de red es fundamental para la administración de la red de una empresa ya que se le considera como la columna vertebral de cualquier red comunicaciones y desempeña un papel fundamental en la administración, diseño y solución de problemas de la red. La topología de red es la disposición de todos los dispositivos o nodos dentro de una red en términos de su diseño físico y lógico. Se lo considera como un plano de toda la red que nos muestra cómo se conectan todos los dispositivos de una red y como se transmiten datos entre ellos (Moes, 2023).

Las topologías de red se clasifican en topologías de red física y topologías de red lógicas. Las topologías de red física representan la disposición física de los equipos, cables y dispositivos de red. En este tipo de topología, los dispositivos o los nodos de la red están conectados entre sí y la transmisión de información se lo hace mediante cables que mantienen conectados a los dispositivos en una disposición específica (Axess Network, 2022).

Las topologías de red lógicas describen como los datos viajan a través de la red independientemente de la conexión o disposición física de los nodos. La topología lógica representa conceptualmente como los datos viajan y se transmiten en diferentes nodos. Es importante entender la topología lógica de una red ya que su diseño y gestión nos puede ayudar en el rendimiento, seguridad y la resiliencia de un sistema (Cuadrado, 2021).

2.1.2.1 TIPOS DE TOPOLOGÍA DE RED

Existen diversos tipos de topología de red que varían según el tamaño de la red, la escalabilidad, los objetivos empresariales y el presupuesto de cada empresa. Existen diferentes tipos de topologías de red, cada uno con características diferentes que se adaptan a los distintos escenarios con contextos y requerimientos específicos (Axess Network, 2022).

Topología de Malla.

En este tipo de topología cada dispositivo está conectado a otro con un canal en particular (ver figura 1). Algunos de protocolos que utiliza son AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc. (Axess Network, 2022).

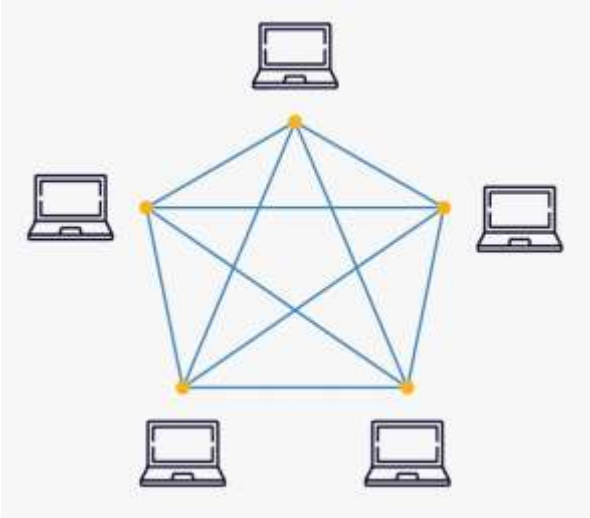


Figura 1 Topología Malla. Fuente: Axessnet (2022)

Topología de Estrella.

En este tipo de topología, todos los dispositivos están conectados a un solo concentrador a través de un cable de red (ver figura 2). Este concentrador actúa como nodo central y todos los demás nodos están conectados al nodo central. El concentrador puede tener dos naturalezas. Puede actuar como un concentrador pasivo, es decir no es inteligente como los dispositivos de transmisión, y al mismo tiempo el concentrador puede ser inteligente, actuando como concentrador activo. Los concentradores activos tienen repetidores en ellos (Axess Network, 2022).

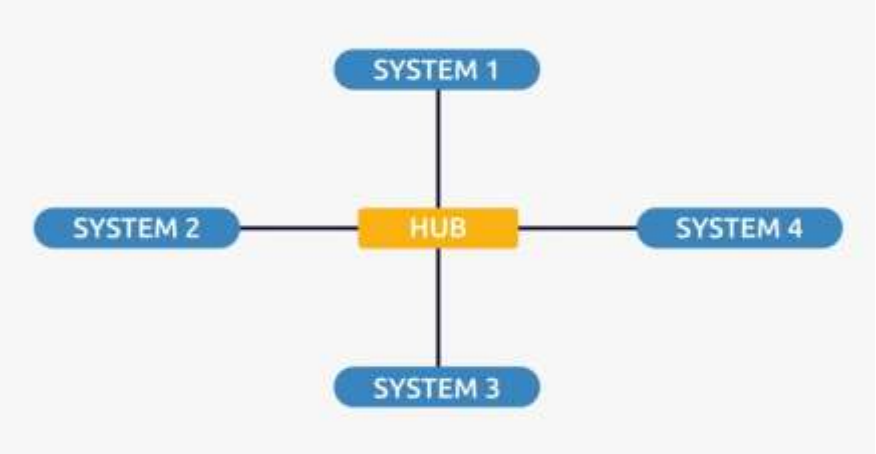


Figura 2 Topología de Estrella. Fuente: Axessnet (2022)

Topología de Bus.

La topología de bus es un tipo de topología en donde cada nodo está conectado hacia un solo cable (ver figura 3). Este tipo de topología es bidireccional, tiene una conexión multipunto y no se lo considera como una topología robusta ya que, si falla la red troncal, falla toda la topología (Axess Network, 2022).

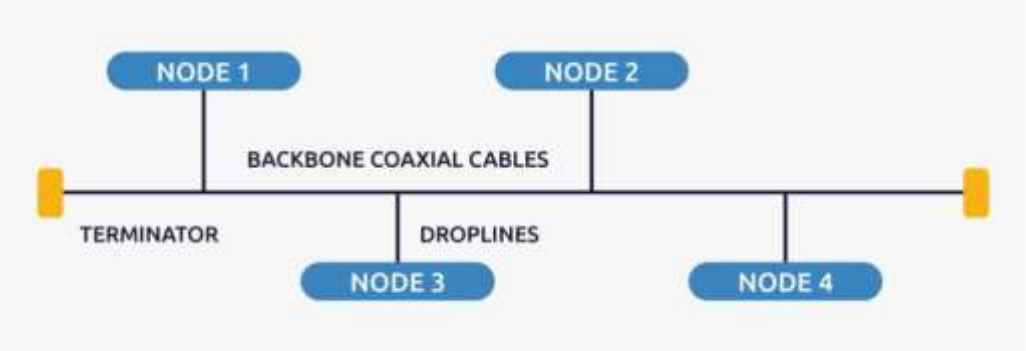


Figura 3 Topología de Bus. Fuente: Axessnet (2022)

Topología de Anillo.

En esta topología, se forma un anillo que conecta los dispositivos con exactamente dos dispositivos vecinos (ver figura 4). Se utilizan varios repetidores en la topología anillo cuando se tiene una gran cantidad de nodos, ya que, se si quieren enviar datos al último nodo en una topología anillo de cien nodos, los datos tendrán que pasar a través de noventa

y nueve nodos para llegar al nodo cien. Por eso se utilizan repetidores en la red para la pérdida de datos.

Los datos de la topología anillo se transmiten en una sola dirección, es decir, unidireccional. Sin embargo, se puede hacer bidireccional al tener 2 conexiones entre cada nodo de red. Este efecto se denomina topología de doble anillo (Axess Network, 2022).

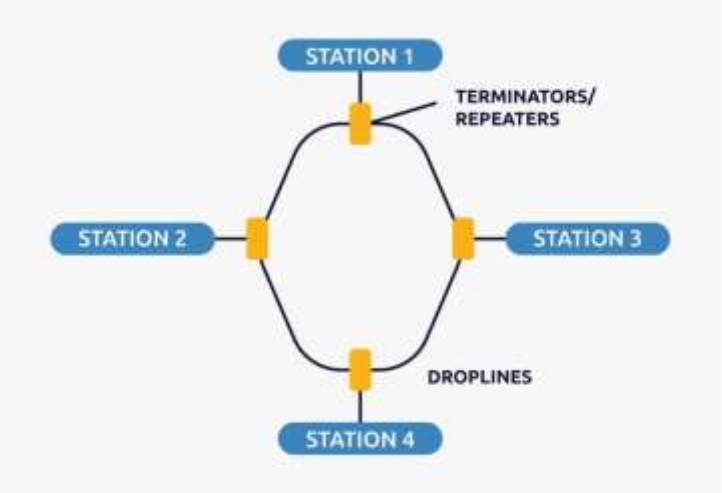


Figura 4 Topología de Anillo. Fuente: Axessnet (2022)

Topología de Árbol.

Esta topología es una variación de la topología estrella, sin embargo, la distribución de los nodos y transmisión de datos tienen un flujo jerárquico (ver figura 5). En esta topología, los concentradores secundarios están conectados al concentrador central que contiene un repetidor. Los datos fluyen desde el concentrador central hacia los concentradores secundarios, y de ellos hacia los nodos. De igual manera los datos pueden fluir de abajo hacia arriba, es decir, de los nodos al concentrador secundario y del concentrador secundarios hacia el concentrador central. Se debe tomar en cuenta que, si falla la red troncal, toda la topología falla (Axess Network, 2022).

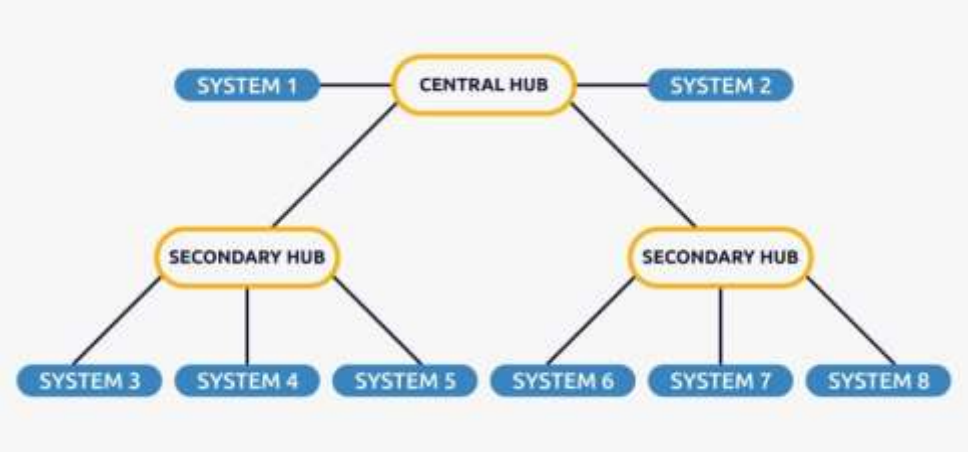


Figura 5 Topología de Árbol. Fuente: Axessnet (2022)

Topología Híbrida.

La topología híbrida es la combinación entre dos o más topologías (ver figura 6). Se utiliza cuando los nodos son libres de tomar cualquier forma y combina topologías individuales, como la topología estrella junto a la topología anillo, creando una topología más robusta y grande. Esta topología es muy flexible, aunque el verdadero reto es el diseño de una arquitectura de red híbrida (Axess Network, 2022).

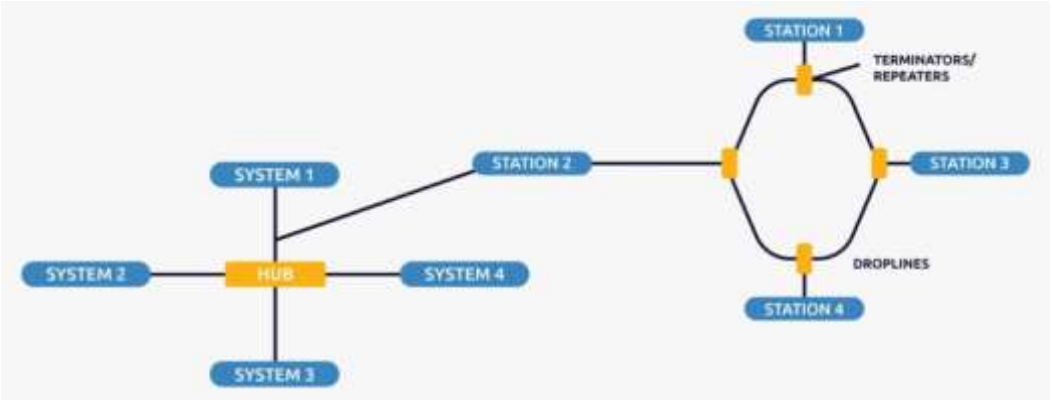


Figura 6 Topología Híbrida. Fuente: Axessnet (2022)

2.1.2.2 IMPORTANCIA DE LA TOPOLOGÍA DE RED

El diseño de la topología de red juega un papel muy importante ya que tiene un impacto directo en la funcionalidad de la red. Seleccionar la topología de red correcta ayuda a mejorar notablemente el rendimiento y la eficiencia en la transmisión de los datos ya que

puede llegar a optimizar los recursos y reducir los costos operativos. Los diagramas de topologías de red pueden ayudar a los ingenieros a comprender como se manejan y se transmiten los datos en una infraestructura red, además, junto con esa información, se puede diagnosticar los posibles problemas de conectividad que se presenten en la red a nivel general (Axess Network, 2022).

En el presente trabajo de titulación, es fundamental comprender la topología de red que maneja la empresa donde se va a realizar el caso de estudio para lograr un análisis efectivo del tráfico de datos. La topología de red define cómo los dispositivos están conectados y como los datos fluyen a través de ellos, lo cual, permite conocer puntos críticos donde los datos se encuentren más vulnerables a posibles amenazas. Con este conocimiento se puede ubicar estratégicamente la herramienta Suricata con el objetivo de hacer una evaluación y análisis del tráfico de red sin poner en riesgo la infraestructura. Sin una comprensión clara de la topología de red, es complicado fijar un análisis estructurado y preciso, por lo que el resultado del estudio se vería comprometido y afectaría a las propuestas de mejora en la seguridad de la red corporativa.

2.2 SEGURIDAD DE REDES

Para entender el contexto de la seguridad en las redes primero se debe entender sobre la definición de ciberseguridad. La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. La ciberseguridad también se conoce como la seguridad de las tecnologías de la información y se puede aplicar en diferentes contextos no solo en las redes de alguna organización o negocios de gran tamaño, también en servicios comunes como en los dispositivos móviles o en cualquier dispositivo tecnológico que pueda usar una persona en su diario vivir (Kaspersky, 2020).

Hay que entender que, en su mayoría, muchas personas creen que la ciberseguridad es la aplicación de tecnologías específicas para proteger redes o equipos tecnológicos específicos, pero no es así. La ciberseguridad es una práctica que no se limita solo en el contexto técnico, sino, son el conjunto de buenas prácticas que los usuarios deben gestionar para así poder proteger sus dispositivos. La ciberseguridad se divide en diferentes campos

como la seguridad de la información, la seguridad de aplicaciones, la seguridad operativa y la seguridad de redes.

La seguridad de redes es el campo de la ciberseguridad centrado en la protección de las redes y sistemas informáticos frente a ciberamenazas y ataques internos. El principal enfoque de la seguridad de redes es proteger los datos que se manejan dentro de una corporación y los sistemas informáticos que utiliza, estos sistemas informáticos pueden ser aplicaciones, bases de datos, etc. (IBM, 2021). La seguridad de red tiene tres objetivos principales que son:

- Denegar el acceso no autorizado a los recursos de la red.
- Detectar y mitigar ataques maliciosos y violaciones a la seguridad.
- Garantizar que los usuarios autorizados tengan un acceso seguro y disponible a los recursos de red que necesiten.

En el presente trabajo de integración curricular, la seguridad de redes se va a aplicar en el contexto de proteger la infraestructura de red y el flujo de datos que existe entre el portal que maneja la empresa y los usuarios. Al implementar suricata como herramienta de detección de intrusos (IDS), se va a poder identificar posibles amenazas que puedan comprometer con la integridad y disponibilidad de los servicios de consulta y de cargas de las diferentes providencias judiciales. Esto nos va a ayudar a poder intervenir y actuar ante accesos no autorizados y prevención de posibles intentos de explotación de vulnerabilidades.

2.2.1 PRINCIPALES AMENZAS Y VULNERABILIDADES

Las amenazas cibernéticas es cualquier actividad dañina potencial que pueden infringir daños a los recursos, sistemas o datos afectando directamente a la confidencialidad, disponibilidad e integridad de un sistema, la red o infraestructura de una organización.

Las vulnerabilidades son debilidades o fallas que pueden utilizar los actores maliciosos para así aprovechar de estas y poder violar las políticas de seguridad. Generalmente los actores maliciosos buscan vulnerabilidades en sistemas informáticos para robar información, aunque también, se debe tomar en cuenta que existen vulnerabilidades

físicas como debilidades en el acceso hacia un centro de datos o debilidades en acceso directo a equipos críticos.

Las amenazas cibernéticas han aumentado y siguen en contaste aumento durante los últimos años, desde programas para robar información confidencial como credenciales, hasta ataques que pueden provocar la caída de servidores. Es importante mantenerse actualizados ante las nuevas amenazas, comprender los distintos de ataques que pueden surgir y tomar las medidas preventivas y precauciones necesarias para evitarlos (Santos, 2023).

Hoy en día, existen amenazas que están relacionados con fallas humanas, siendo una de las principales afectaciones a los sistemas informáticos y redes, amenazas relacionadas con ataques con intenciones maliciosas y con catástrofes naturales. La explotación de las amenazas frente a estos recursos puede dar lugar al acceso no autorizado, modificación o eliminación de información, interrupción de un servicio, daños físicos o robo de equipamiento y medios donde se almacena la información (Universidad Nacional De La Plata, 2017).

Para el siguiente apartado, se ha hecho un listado entre las principales amenazas de ciberseguridad que existen actualmente y que pueden poner en riesgo a una empresa.

Ingeniería social: La ingeniería social consiste en técnicas para engañar a las personas utilizando trucos, tretas, mentiras, a fin de que se pueda relevar información de interés al atacante, por ejemplo, revelar contraseñas de acceso. Esta amenaza se diferencia de las demás ya que no necesita de una debilidad directa del sistema o una vulnerabilidad propia de un componente informático para acceder a la información (Universidad Nacional De La Plata, 2017).

Phishing: Esta amenaza consiste en el envío de mensajes, sobre todo correos electrónicos, que simulan ser mensajes de entidades reales o entidades oficiales de empresas legitimas. Sin embargo, estos correos no son oficiales ya que suelen cambiar en el dominio del correo o en el mensaje ciertos puntos específicos, buscando así que el usuario evite notar la diferencia del correo real. El fin de este ataque malicioso es obtener

información como datos personales y en su uso más común datos bancarios de usuarios (Universidad Nacional De La Plata, 2017).

Esta amenaza se considera uno de los ataques más populares que utilizan los ciberdelincuentes para obtener la información privada de los usuarios o del punto final hacia donde vaya dirigido el ataque. La información que pueden capturar puede ser números de tarjetas de crédito, nombres de usuario, contraseñas, etc. Los atacantes simulan pasar por una institución verificada, comúnmente una institución financiera, o por individuos confiables que conoce el objetivo y envían un mensaje electrónico solicitando al usuario que ingrese a un link. Este mensaje puede ser vía correo electrónico o SMS y al enlace que ingresa será muy parecido al de una página oficial, sin embargo, no lo es, y mediante este medio roban las credenciales privadas (Santos, 2023).

Código malicioso / Virus: El código malicioso o virus se define como cualquier programa que genera un daño, interfiriendo en el funcionamiento regular de un sistema. Generalmente este programa o código es ejecutable y vienen en archivos ejecutables o programas que se deban ejecutar (Universidad Nacional De La Plata, 2017).

También al código o software malicioso se denomina malware, tiene como objetivo explorar las vulnerabilidades del sistema informático y así poder infligir el ataque explotando esas vulnerabilidades. El malware puede ejecutar o desinstalar programas a voluntad, acceder a funciones críticas del sistema, permitir extracción de información, etc. Este tipo de software se encuentra frecuentemente en páginas web de anuncios publicitarios o instalamos programas desconocidos de páginas no oficiales con el riesgo de que se encuentre malware en ellos (Santos, 2023).

Ataques de contraseña: Los ataques de contraseña se basan en una prueba metódica de contraseñas para así acceder a un sistema Este ataque puede ser efectivo si el sistema no presenta un control de intentos fallidos por acceso. El ataque de contraseña puede ser mediante un diccionario de palabras en el cual una herramienta va a intentar acceder a sistema probando palabra por palabra que este registrada dentro de un diccionario. Generalmente estos diccionarios suelen tener miles llegando a millones de palabras. Y el otro ataque es de fuerza bruta, donde una herramienta generará combinaciones entre

números, letras y símbolos buscando las posibles contraseñas y probando una por una (Universidad Nacional De La Plata, 2017).

Robo de identidad: Esta amenaza ocurre cuando un tercero obtiene y utiliza, mediante medios informáticos, información personal ajena (nombre, identificación, tarjetas, numero de afiliación al seguro o información bancaria) sin la autorización del propietario intelectual. Esto es con el fin de realizar actividades fraudulentas, generalmente robar dinero y hacer transferencias o compras hacia otros destinos (Universidad Nacional De La Plata, 2017).

Se debe tomar en cuenta que el robo de identidad se puede considerar como una amenaza interna para las empresas por parte de los empleados. Los empleados tienen la autoridad y los permisos para acceder al sistema, independientemente del nivel de acceso, por lo que un pequeño error que cometan al momento de acceder o utilizar el sistema puede resultar en una vulnerabilidad que será aprovechada por terceros. También, existe la posibilidad que uno de los empleados sea el responsable directo del robo de información o la filtración, ya sea de manera involuntaria o no (Santos, 2023).

Daños físicos al equipamiento: Los daños físicos al equipamiento que maneja una organización ya sea en su centro de datos o portátiles individuales de trabajo pueden ser ocasionados por acciones intencionadas, negligencia de los usuarios (ej.: derrame de líquidos) o catástrofes naturales. Es importante tomar en cuenta que sin el hardware no se puede manejar los datos o servicios de una organización por lo que el acceso a centros de datos debe ser restringido por el personal autorizado, el personal debe ser capacitado para evitar accidentes como golpes o ya mencionado el derrame de líquidos y en caso de catástrofes naturales siempre contar con sistemas de respaldos aislados como por ejemplo en la nube para que la información no se pierda (Universidad Nacional De La Plata, 2017).

En el contexto de este trabajo, el análisis del tráfico de red mediante la herramienta Suricata va a permitir identificar las posibles amenazas y vulnerabilidades ya mencionadas que suelen afectar a pequeñas y medianas empresas como la pyme del presente caso de estudio. Suricata es una herramienta que actúa como un sistema detección de intrusos, por lo que es posible detectar patrones sospechosos y señales de posibles ataques como

phishing, malware, ataques de contraseña, etc. Además, la herramienta suricata permitirá visualizar los puntos críticos de la red, ayudando a mejorar la seguridad general de la infraestructura y así, poder tomar decisiones para mitigar las vulnerabilidades.

2.2.2 TECNOLOGÍAS DE SEGURIDAD EN REDES

Los sistemas de seguridad de red funcionan en dos niveles: en el perímetro de la red empresarial y dentro de la red empresarial. En el perímetro de la red se va a evitar que los atacantes puedan traspasar para así tener acceso a la red o a la información imponiendo controles de seguridad, sin embargo, en algunos casos los atacantes logran romper esa seguridad, por lo que los equipos de seguridad de TI ponen controles dentro de la red empresarial ya sea en dispositivos finales o los datos que se transmiten. Esta estrategia de múltiples capas se denomina defensa de profundidad (IBM, 2021).

Existen diversos tipos de tecnología de seguridad en las redes que buscan proteger los recursos digitales dentro de una organización frente a diversas amenazas y delincuentes cibernéticos. Estos diferentes tipos de tecnología tienen diferentes ventajas y sus objetivos varían según su enfoque, además, estas diferentes tecnologías se pueden aplicar para proteger la empresa u organización, dependiendo del tipo de seguridad ideal que necesite (Santos, 2022).

Firewalls: Los firewalls o cortafuegos son programas de software o dispositivos de hardware que nos ayudan a impedir que usuarios no autorizados puedan ingresar a la red interna, filtrando tráfico sospechoso y solo aceptando tráfico legítimo (Santos, 2022).

Existen diferentes tipos de firewall que se pueden utilizar de acuerdo con el enfoque y nivel de seguridad. Pueden ser servidores proxy, firewalls de filtrado de paquetes y firewalls de última generación o NGFW que son firewall diseñados para proteger contra amenazas cibernéticas de última generación empleando inteligencia artificial (IBM, 2021).

Software antivirus o antimalware: Un software antivirus o antimalware es una herramienta que sirve para detectar y eliminar malware, por ejemplo, virus, troyanos, spyware, etc. Estas herramientas utilizan algoritmos y firmas de detección en base al comportamiento del sistema para detectar amenazas y eliminarlas antes que puedan ocasionar daño (Team Ambit, 2024).

Algunos de estos virus pueden ingresar a un sistema informático y permanecer en la red por días o semanas y en algunos casos expandirse, como en el caso de los gusanos. Es importante utilizar los software antivirus o programas antimalware ya que nos ayudan a detectar estos programas maliciosos y, además, poder dar un seguimiento para identificar posibles anomalías, eliminar el programa malicioso y reparar los daños (Santos, 2022).

Control de acceso a la red (NAC): El control de acceso a la red (Network Access Control o NAC), es una de las primeras líneas de defensa que se encuentra en los dispositivos finales o endpoints. El NAC es utilizado como verificador de acceso a la red, donde examina cada dispositivo y luego poder comprobar si tiene una protección antivirus adecuada, tenga las configuraciones correctas y esté actualizado antes de ingresar a la red (Santos, 2022).

La NAC se puede programar para controlar el acceso basado en roles. El acceso del usuario está limitado en función al perfil que maneje y el rol que obtenga según los administradores de red. Una vez que el usuario ingrese a la red, solo puede tener acceso a ciertos archivos o datos aprobados (IBM, 2021).

Redes privadas virtuales (VPN): La red privada virtual (Virtual Private Network, por sus siglas en inglés) es una herramienta software que protege la identidad del usuario, cifrando sus datos y enmascarando la ubicación del usuario y la dirección IP del dispositivo que se encuentre dentro de la VPN. Cuando un usuario quiere conectarse al internet mediante VPN, primero se conecta a un servidor seguro que luego se conecta al internet en su nombre (IBM, 2021).

Las VPN son una de las medidas de seguridad más comunes en las empresas ya que son necesarias para cualquier persona que deseen conectarse hacia el internet de manera segura. Ayuda con la protección contra ciberdelincuentes que desean interceptar y robar los datos como fotos, número de tarjetas de crédito o la identidad de un usuario (Santos, 2022).

Sistemas de detección y prevención de intrusiones (IDPS): Un sistema de detección y prevención de intrusiones (Intrusion Detection and Prevention System o IDPS) se ejecutan detrás de un firewall con el fin de crear otra capa de seguridad que pueda proteger contra posibles ataques. Estos sistemas trabajan en paralelo con un sistema de

detección de intrusiones (IDS) que es un sistema más pasivo pero muy importante ya que añade una parada extra al tráfico de red que desea ingresar con el fin de poder hacer un análisis y seguimiento más profundo. Existen IDPS más avanzados que examinan inmediatamente los datos entrantes y activan un proceso automatizado de alarmas que bloquea el tráfico entrante al detectar una actividad sospechosa (Santos, 2022).

En el presente trabajo de titulación, se va a utilizar un sistema de detección de intrusos (IDS) y la herramienta que se va a utilizar es Suricata. Suricata es ideal para realizar un monitoreo detallado y pasivo a tiempo real, a diferencia de un IPS, cuyo objetivo principal es el bloqueo de amenazas de forma activa. Suricata es fundamental para capturar tráfico y analizar paquetes, proporcionando así información detallada sobre posibles amenazas que pueden comprometer con la seguridad de la red y poder dar un seguimiento profundo y preciso de las posibles vulnerabilidades. Además, el uso de esta herramienta es importante en el contexto actual, donde las organizaciones enfrentan un número significativo de amenazas, la detección y prevención es crucial para contribuir en el proceso de evitar el posible acceso no autorizado e ingreso de tráfico sospechoso dentro de la red corporativa. Se debe tomar en cuenta que la configuración de Suricata va a ser directamente proporcional a las reglas predefinidas establecidas.

2.2.3 ESTRATEGIAS DE MITIGACIÓN

Las estrategias de mitigación en la seguridad de redes son un conjunto de prácticas que se pueden aplicar dentro de un entorno laboral con el fin de prevenir ataques maliciosos y proteger los sistemas y datos. La práctica e implementación de medidas de ciberseguridad no debe ser costosa ni tampoco debe ser compleja. La clave es realizar acciones simples, pero con eficacia, como investigación y la implementación de estrategias de mitigación incluyendo el uso de herramientas confiables y gratuitas. Es posible la implementación de estas estrategias con el mínimo esfuerzo y con un gran alcance en la protección de las redes y los datos (National Cybersecurity Alliance, 2022).

Existen diferentes medidas y prácticas de ciberseguridad las cuales se basan en los comportamientos más comunes e impactantes, por ejemplo, la suplantación de identidad o compromiso de credenciales en un sistema. Diferentes organizaciones pueden aplicar estas

medidas de mitigación y recomendaciones para que puedan mitigar amenazas de operaciones cibernéticas, basándose en comportamientos maliciosos analizados y observados. Además, se recomienda aplicar estas diferentes prácticas con el fin de que sirva de apoyo para poder proteger los sistemas, las redes y los datos que circulan por la red interna de una organización (CISA, 2024).

- Mantener el software actualizado en los dispositivos de los usuarios y en la infraestructura informática.
- Implementar una autenticación multifactor (MFA, por sus siglas en inglés) que resista a la suplantación de identidad.
- Auditar las cuentas y desactivar las cuentas que ya no se utilicen o sean necesarias.
- Deshabilitar las cuentas de ususario y el acceso a los recursos de la organización para el personal saliente.
- Gestionar los riesgos de la infraestructura de red y aplicar las medidas y políticas necesarias para la protección de la arquitectura.
- Implementar al personal de la organización una capacitación de ciberseguridad.
- Desarrollar y poner en práctica planes de respuesta a incidentes y recuperación.
- Utilizar un gestor para la administración contraseña que se utiliza para los diferentes accesos.
- Revisar las relaciones contractuales con todos los proveedores de servicios y dar prioridad a los proveedores de servicios críticos.
- Aplicar el principio del privilegio mínimo en la gestión de cuentas y accesos limitados.

Estas diferentes estrategias de mitigación complementarán en el presente trabajo de titulación al fortalecer el análisis del tráfico de red y los sistemas de detección de intrusos (IDS), como Suricata al proporcionar acciones concretas y poder mitigar o neutralizar las posibles amenazas identificadas. Además, junto al análisis que se va a realizar en el caso de estudio utilizando la herramienta Suricata y los hallazgos que se puedan obtener del mismo, se puede poner en práctica las prácticas recomendadas mejorando

significativamente la seguridad de la infraestructura de red de la empresa y asegurando un entorno más robusto frente a riesgos potenciales.

2.2.4 NORMATIVAS Y ESTÁNDARES

Los estándares son un conjunto de normas y prácticas diseñadas para garantizar la protección de información, activos y personas en diferentes ámbitos, ya sea en el ámbito digital, industrial o personal. En el mundo que vivimos actualmente es cada más conectado e interdependiente, por lo que la seguridad se ha vuelto uno de los campos más importantes y una preocupación constante para los individuos, empresas e incluso diferentes gobiernos. Con el crecimiento de las amenazas cibernéticas, es importante conocer los diferentes estándares de seguridades más importantes y cómo implementarlos de manera efectiva para que así, podamos garantizar la seguridad y la protección de nuestros datos (SensorTech, 2023).

La legislación del gobierno de España en el Artículo 8 de la Ley 21/1992, de 16 de Julio, de Industrias, define a norma como "La especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas, que aprueben un Organismo reconocido, a nivel nacional o internacional, por su actividad normativa." (España, 1992).

El campo de la ciberseguridad está en auge hoy en día eso es debido al creciente número de amenazas ataques e incidentes que van dirigidos hacia la información y los datos ya sean individuales o de organizaciones y empresas más grandes. Esto hace que surja la necesidad de implementar controles y seguridad para garantizar la protección de la información, dispositivos, redes de comunicación y los activos más críticos. Estamos en un mundo actual donde existen diversos tipos de tecnología y un sin número de equipos, que dificulta la implementación de medidas de ciberseguridad. Sin embargo, para que el proceso de implementación de dichas medidas de seguridad informática sea más preciso y con más naturalidad, nacieron los estándares normas ISO relacionadas con la ciberseguridad y seguridad de la información (Departamento de Consultoría, 2021).

Las normas ISO (International Organization for Standardization, por sus siglas en inglés) es la organización que se encarga de establecer estándares para diferentes áreas,

incluido el área de la ciberseguridad. Además de ISO, el IEC (International Electrotechnical Commision, por sus siglas en inglés) son las organizaciones encargadas de establecer las normativas a nivel mundial. Las normas establecidas por la ISO/IEC constituyen, hoy en día, un valor indispensable en el cumplimiento de las organizaciones ya que otorgan valor a la empresa, prestigio y reconocimiento a nivel internacional. Se debe tomar en cuenta que los estándares certificados son revisados y auditados periódicamente para garantizar el cumplimiento (Departamento de Consultoría, 2021).

La ISO/IEC 27000 es una serie compuesta por varias normas de seguridad de la información que nos brinda información sobre las pautas y detalles específicos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Dentro del conjunto de normas se encuentra la norma ISO/IEC 27001, esta norma establece los diferentes requisitos para implementar un SGSI. Esta norma está basada en un proceso llamado Ciclo Deming o PDCA (Plan-Do-Check-Act, por sus siglas en inglés) que consta de 4 procesos que siguen un ciclo continuo con el fin de establecer una mejora continua en el sistema. (Departamento de Consultoría, 2021). A continuación, se presenta una imagen del ciclo Deming o PDCA en la figura 7.

Figura 7 Ciclo PDCA: Planificar, hacer, verificar, actuar. Fuente: Global Suite Solutions (2023)

La norma ISO/IEC 27033 es una norma que se basa en establecer los requisitos y recomendaciones para garantizar la seguridad y protección en la comunicación de redes. Esta norma es también conocida como “Tecnología de Información – Técnicas de Seguridad – Redes de Comunicación” ya que proporciona directrices especializadas y

buenas prácticas para poder mantener seguro la disponibilidad, integridad y confidencialidad de la información que se transmite a través de las diferentes redes de comunicación (NormasISO.org, 2023).

La norma ISO/IEC 27033 es esencial en la seguridad de la comunicación de redes ya que su implementación ayuda a proteger la información sensible y garantiza la confianza de los socios comerciales y los clientes dentro de una organización. La ISO/IEC 27033 abarca diversos aspectos como el análisis de riesgos, definición de políticas se seguridad e implementación de controles para proteger la información durante la transmisión de información en las diferentes redes de comunicación (NormasISO.org, 2023).

Existen también otras organizaciones y agencias que proporcionan directrices completas además de implementar mejores prácticas para reforzar y gestionar los riesgos de la seguridad. Otro marco que nos brinda estas directrices es NIST.

El Instituto Nacional de Estándares y Tecnología, NIST (National Institute of Standars and Technology, por sus siglas en inglés) es una agencia que desarrolla e impulsa la innovación de normas, tecnología y metrología. El marco de ciberseguridad de NIST consta de un marco de normas y prácticas que orientan a las empresas de cualquier tamaño a mejorar su riesgo en la gestión de ciberseguridad (IBM, 2023).

El marco de ciberseguridad de NIST consta de cinco etapas: identificación, protección, detección, respuesta y recuperación (Comisión Federal de Comercio, 2019)

- Identificación: Se debe realizar una lista con todos los equipos, programas y herramientas software que se utilice dentro de la organización. Una vez identificado todos los recursos, ya sea software o hardware, se debe además conocer los riesgos asociados o las posibles vulnerabilidades que puedan ser explotadas por un ataque cibernético (Comisión Federal de Comercio, 2019).
- Protección: Se debe controlar quienes tienen acceso a los diferentes dispositivos, datos y quienes acceden a la red. Además, se debe implementar políticas de seguridad y diferentes medidas para poner en protección los activos o datos más críticos (Comisión Federal de Comercio, 2019).

- Detección: En la etapa de detección se debe monitorear las actividades anómalas y comportamientos sospechosos que puedan poner en riesgo los datos que se manejan en la organización. En caso de encontrar cualquier actividad inusual, se debe realizar una investigación cautelosa por parte del personal capacitado (Comisión Federal de Comercio, 2019).
- Respuesta: Se debe tener un plan para poder reducir o mitigar completamente los daños en caso de que el ataque haya tenido éxito. El plan debe mantener en función las operaciones del negocio, contener el ataque y notificar a los clientes o posibles usuarios que son afectados o pudieran estar en riesgo (Comisión Federal de Comercio, 2019).
- Recuperación: En la siguiente etapa final, se debe restaurar las operaciones normales y los equipos que salieron afectados luego del ataque. Es importante mantener informados a los clientes y empleados las actividades de respuesta y recuperación que se realizaron luego del incidente (Comisión Federal de Comercio, 2019).

En el presente trabajo de titulación, el análisis del tráfico de red mediante la herramienta Suricata se alinea con las recomendaciones establecidas por la norma ISO/IEC 27033 y con la implementación de las cinco etapas del marco de ciberseguridad de NIST. La norma ISO/IEC 27033 establecida nos planea diferentes directrices para poder gestionar y proteger la información mediante la definición de políticas y control de la comunicación de las distintas redes corporativas, además de la infraestructura de red. Por otro lado, la aplicación de las cinco etapas del marco de ciberseguridad de NIST dentro de una empresa puede ser útil al momento de saber manejar y gestionar un incidente. Se debe tomar en cuenta que uno de los aspectos que abarcan ambas instituciones es el análisis de riesgos, por lo que el análisis del tráfico de red se ajusta a los requisitos para cumplir con las normativas y así, se puede complementar los hallazgos del presente trabajo de titulación, orientado hacia marcos internacionalmente reconocidos para la seguridad y protección de las redes.

2.3 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Una intrusión es una penetración no autorizada en la red de una empresa o en una dirección de una máquina individual en un dominio asignado. Existen dos tipos de intrusiones: las intrusiones pasivas la penetración se realiza de forma sigilosa y sin detección, mientras que las intrusiones activas se efectúan cambios en la red. Las intrusiones de red pueden tener un origen externo, es decir, fuera del entorno de la red empresarial o puede ser interna dentro del entorno de la red empresarial, puede ser ocasionado por empelados internos. El objetivo de las intrusiones es extraer información crítica o informarle al intruso sobre las actividades que se realiza en la red ya se con la muestra de imágenes o varios mensajes (West, 2014).

La detección de intrusiones en un sistema es el proceso de monitorizar los diferentes eventos que ocurren en un sistema informático o en la red, para luego analizarlos y poder detectar las posibles sospechas de incidentes, que son violaciones o amenazas próximas ante posibles violaciones, hacia las políticas de seguridad informática. Un sistema de detección de intrusiones (IDS) es una herramienta de seguridad de red que se basa principalmente en la identificación de posibles incidentes que se pueden encontrar al realizar un análisis del tráfico de red, el registro de la información sobre los posibles incidentes encontrados y la notificación de los mismos hacia los administradores de seguridad. Otras organizaciones han dado diferentes usos al IDS, como identificación de los problemas de la política de seguridad de los sistemas informáticos o de la red conociendo diferentes brechas que se pueden presentar, la documentación de las amenazas existentes que pueden infringir en los sistemas y la prevención de violaciones hacia las políticas de seguridad en la mayoría de los casos (Almantas Kakareka, 2014)

La implementación de un sistema de detección de intrusiones es fundamental en una organización que maneja datos sensibles ya que ayuda a evitar que un atacante intente realizar un sin número de ataques hasta lograr que de acierto o logre el éxito de uno. Esto es posible ya que un sistema de detección de intrusiones ayuda a identificar el ataque mucho antes de que sea un posible éxito para el atacante. Una vez que el IDS detecta y reporta los incidentes, el administrador de seguridad es el encargado de tomar las medidas o acciones necesarias dependiendo del grado de impacto que logró analizar (OWASP Foundation, s.f.).

El sistema de detección de intrusiones se ha convertido en una herramienta necesaria para prevalecer la seguridad y proteger la información en casi todas las organizaciones. Para el presente trabajo de integración curricular, se va a dar el uso de una herramienta que se utiliza especialmente en el campo de la ciberseguridad. Suricata es una herramienta de detección de intrusos que nos va a permitir vigilar y monitorizar el tráfico de red que se maneja internamente dentro de una organización y, para el presente trabajo se va a utilizar en la empresa donde se va a realizar el caso de estudio. Esta herramienta nos va a permitir detectar posibles amenazas que puedan comprometer con los sistemas de información y también con los datos sensibles que maneja la empresa. La detección de posibles incidentes puede ayudar a establecer diferentes medidas necesarias para mantener seguros los sistemas de información y los canales donde se transmiten los datos.

2.3.1 FUNCIONAMIENTO DE UN IDS

Un sistema de detección de intrusos puede ser ya sea una aplicación de software instalada en un endpoint o un nodo que esté dentro de la red, o también un sistema de detección de intrusos puede ser una unidad de hardware especifica que esté conectada a la red. Incluso, algunas soluciones de IDS están disponibles como servicios. Aunque existe una diversa clasificación y tipo de IDS, todos los sistemas de intrusión deben responder al objetivo de identificar y responder ante actividades sospechosas que puedan comprometer una red o un sistema informático (IBM, 2023).

Como ya se había mencionado anteriormente, todos los sistemas de detección de intrusiones buscan detectar y prevenir cualquier amenaza y accesos no autorizados, además de proporcionar alertas y registros para que así, los administradores de seguridad puedan tomar las medidas necesarias. El funcionamiento de un IDS empieza por varias etapas desde la recopilación de datos hasta la respuesta ante amenazas (Software y Hardware, 2023):

1. **Recopilación de datos de red:** El IDS primero debe recopilar los datos de la red monitoreando y analizando el tráfico de red en busca de signos de actividades sospechosas. La recopilación de datos es un proceso continuo y constante ya que el IDS debe estar alerta ante posibles riesgos y amenazas. La recopilación de datos

puede ser de registro de eventos, registro de sesiones y de paquetes de datos que viajan en la red (Software y Hardware, 2023).

2. **Análisis de datos:** Una vez que el IDS haya recopilado los datos de la red, el IDS realizará un análisis profundo de los mismos. Para ello, utiliza algoritmos y reglas ya predefinidas para poder identificar patrones y comportamientos anómalos que puedan comprometer y afectar la integridad y seguridad de la información. Para el análisis incluye la detección de actividades sospechosas, por ejemplo, intentos de acceso no autorizado o tráfico malicioso (Software y Hardware, 2023).
3. **Alertas y notificaciones:** El IDS tiene la capacidad de detectar una actividad sospechosa ante una posible intrusión luego de realizar el respectivo análisis, por lo que si en caso de existir la amenaza, envía una alerta o notificación para informar a los administradores de red. Las alertas pueden enviarse por correo electrónico, mensaje de texto o a través de una interfaz gráfica de ususario. Es importante que los administradores de red se mantengan pendientes ante cualquier alerta para que así puedan tomar las diferentes medidas adecuadas y mitigar cualquier amenaza (Software y Hardware, 2023).
4. **Respuesta y mitigación:** Cuando los administradores de red ya reciben una respuesta por parte del sistema de detección de intrusiones con el que se trabaje, deben hacer una investigación más profunda y con ello realizar una respuesta ante la posible amenaza. El resultado puede variar dependiendo el tipo de amenaza que se encuentre, puede ser el aislamiento del sistema afectado, eliminación del malware o la implementación de medidas adicionales de seguridad para eliminar la amenaza informática (Software y Hardware, 2023).
5. **Registro y análisis forense:** Uno de los aspectos más importantes de un IDS es su capacidad de poder registrar y además analizar la posible amenaza que quiere comprometer el sistema informático o la red. Esto sirve de contribución para los administradores de red ya que puede analizar los datos recopilados durante una intrusión y así tomar las medidas necesarias que requiera el caso. El IDS permite también realizar el análisis forense en caso de investigaciones o acciones legales (Software y Hardware, 2023).

Independientemente del tipo, ya sea una aplicación de software o una unidad específica de hardware, los IDS utilizan uno de los dos métodos principales de detección de amenazas: detección basa en firmas y detección basada en anomalías (IBM, 2023).

El método de detección basada en firmas analiza los paquetes de la red en busca de firmas de ataque, es decir, busca características o comportamientos sospechosos exclusivos de cada paquete en relación con una amenaza específica. Un ejemplo de firma de paquete puede ser na secuencia de código específico asociado a una variante de malware (IBM, 2023).

Los IDS basados en firmas funcionan con una base de datos de firmas de ataque con las que compara los paquetes de red. Si el IDS encuentra un paquete con una firma de ataque lo compara con la base de datos y si coincide, envía la alerta. Para que este método sea eficaz, la base de datos de firmas de ataque debe actualizarse constantemente con nueva información sobre amenazas para que el IDS esté actualizado y actúe conforme las nuevas amenazas y nuevos ciberataques que se van generando. Si no se actualiza la base de datos, los nuevos ataques pueden evadir un IDS basado en firmas (IBM, 2023)

Los métodos de detección basados en anomalías utilizan el machine learning para crear modelos de referencia de la actividad normal que se establece en la red. Estos modelos de referencia se perfeccionan continuamente en base a la actividad que se realice en la red. Para la detección de intrusos, el modelo de referencia que se creó gracias al machine learning compara con las diferentes actividades de la red, marcando así las diferentes actividades y desviándolas. Por ejemplo, puede ser un proceso que utiliza más ancho de banda de lo normal o un puerto que es abierto por un dispositivo (IBM, 2023).

Una de las ventajas que tiene el método de detección basado en anomalías es que pueden detectar cualquier tipo de comportamiento anómalo, es decir, pueden detectar ataques y amenazas nuevas que afecten a la actividad normal de la red, esto es posible por el modelo de referencia que crean a base del machine learning. Un ejemplo puede ser la detección de ataques de día cero, es decir, ataques que aprovechan las vulnerabilidades que tiene el software o la red antes que el administrador las detecte o aplique diferentes parches en la vulnerabilidad. Sin embargo, una desventaja de este método es que puede ser más

propenso a los falsos positivos. Esto puede incluir actividades benignas, por ejemplo, el registro de un nuevo ususario al sistema o el acceso de un nuevo ususario hacia un recurso de la red puede enviar una alerta al IDS (IBM, 2023).

Es importante que los administradores de red puedan manejar y gestionar correctamente un IDS. Ya sea un IDS que utilice el método de detección basado en firmas, el administrador de red debe estar al pendiente de las nuevas amenazas que surgen y actualizar la base de datos del IDS para que pueda detectar los nuevos ataques de paquetes basados en firmas. Por otro lado, si el IDS utiliza el método de detección basado en anomalías, el administrador de red debe conocer las diferencias de las diferentes alertas que puede generar el IDS, estas alertas pueden ser falsos positivos, o alertas de ataques y amenazas de red que requieren intervención y mitigación inmediata.

2.3.2 TIPOS DE IDS

Antes de describir los diferentes tipos de IDS, es importante comprender que estos sistemas de detección de intrusos pueden trabajar en dos modos operativos: pasivos y activos. Estos modos no son exclusivos de un IDS en particular, sino que ayudan a determinar el enfoque y el tipo de trabajo que va a realizar al responder ante la detección de una posible amenaza o comportamiento sospechoso.

IDS pasivos: Los IDS que operan de modo pasivo son conocidos ya que solo se dedican a monitorear el tráfico de la red o las actividades del sistema sin tomar acción alguna sobre ellos. Realizan análisis del tráfico de red en busca de signos sospechoso y si caso de detectar algún comportamiento anómalo, generan las respectivas alertas para que el administrador de red pueda realizar una mayor investigación. Los IDS que operan de modo pasivo no son intrusivos, quiere decir, que interrumpen o toman acciones frente a la detección de una amenaza, lo que los hace necesarios para minimizar las interrupciones de la red o de falsos positivos. Las acciones que se van a tomar frente a las amenazas detectadas dependen directamente del personal encargado de la administración de red (Seguridad de la información Asia, 2024).

IDS activos: Los IDS que operan de modo activo no solo detectan las amenazas potenciales como los IDS pasivos, una de las funciones de los IDS activos es que también

toman las medidas necesarias en ese instante para prevenir las amenazas o mitigarlas. Cuando un IDS opera de modo activo, puede intervenir en los procesos de la actividad de la red en el momento que detecta alguna amenaza o posible intrusión o violación de seguridad. Puede responder activamente dependiendo de la configuración que tenga, por ejemplo, puede bloquear el tráfico de la red, finalizar conexiones entre dispositivos o aplicar otras medidas defensivas. A diferencia de los IDS pasivos, los IDS activos operan de manera más proactiva y pueden otorgar protección en tiempo real contra diferentes patrones de ataque, sin embargo, en su mayoría pueden causar falsos positivos (Seguridad de la información Asia, 2024).

Gracias a esta distinción de en los modos de operación de un IDS, es posible implementar los diferentes tipos de IDS, cada uno es distinguido por sus características particulares adaptados a las necesidades requeridas de la organización para la protección y monitoreo. Los sistemas de detección de intrusos se clasifican según su ubicación en el sistema y el tipo de actividad que supervisan.

NIDS: Los sistemas de detección de intrusiones en la red (Network Intrusion Detection System, por sus siglas en inglés) monitorizan el tráfico entrante y saliente de los dispositivos que se encuentran en la red. La ubicación de los NIDS puede variar según el enfoque estratégico del tráfico que se desee monitorizar y analizar. Los NIDS a menudo se pueden colocar detrás de los firewalls, en el perímetro de la red, para que puedan registrar y alertar cualquier tráfico malicioso que se abra paso. También, un NIDS se puede colocar dentro de la red para que pueda detectar amenazas internas o cuentas de usuarios que hayan sido comprometidas, esto ayuda a monitorizar el tráfico que fluye entre subredes dentro de una red segmentada (IBM, 2023).

Para no dificultar y obstruir el tráfico de la red, los NIDS usualmente se colocan fuera de banda, quiere decir, que el tráfico de la red no pasa directamente por el NIDS. Realmente un NIDS analiza copias de paquetes de red en lugar de los paquetes originales que transitan por la red. De esta manera, el tráfico original o legítimo no tiene que esperar a ser analizado ya que en ese momento el NIDS analiza las copias de los paquetes y puede detectar el tráfico malicioso (IBM, 2023).

HIDS: Los sistemas de detección de intrusiones basados en host (Host Intrusion Detection System, por sus siglas en inglés) se instala en un endpoint (punto final) en específico, puede ser un servidor, una portátil o un router. El HIDS solo va a supervisar y monitorizar la actividad de ese dispositivo donde se instale, incluido el tráfico que llega hacia él y se envía desde él. El HIDS funciona tomando instantáneas periódicas, es decir, capturas del estado actual o snapshots, que pueden ser archivos del sistema, archivos críticos del sistema operativo, registros (logs) o configuraciones clave. Una vez que el HIDS toma estas instantáneas periódicas, empieza comparando la nueva instantánea con las anteriores para detectar cambios, como la modificación de archivos de configuración, cambios en permisos de usuarios o alteración de configuraciones. Si el HIDS detecta estos cambios en el proceso de comparación de instantáneas, envía una alerta inmediatamente al equipo de seguridad (IBM, 2023).

PIDS: Los sistemas de detección de intrusiones basados en prototipos (Protocol-based Intrusion Detection System, por sus siglas en inglés) es un IDS especializado para monitorizar y analizar protocolos de conexión entre servidores y dispositivos. Este tipo de IDS supervisa las interacciones entre protocolos de red y detecta las anomalías o comportamientos sospechosos en esas conexiones. Generalmente los PIDS se colocan en los servidores web para poder realizar el monitoreo y análisis de conexiones HTTP, HTTPS, FTP, SMTP, entre otros (IBM, 2023).

APIDS: Los sistemas de detección de intrusiones basado en aplicaciones (Application-based Intrusion Detection System, por sus siglas en inglés) es un tipo de IDS que está diseñado para monitorear y analizar interacciones dentro de una aplicación específica. Funciona en la capa de aplicación y, además, supervisa los protocolos específicos de la aplicación. A menudo, un APID se coloca entre el servidor web de aplicaciones y la base de datos SQL para detectar inyecciones SQL que puedan comprometer la aplicación y detectar consultas maliciosas (IBM, 2023).

La clasificación de los diferentes tipos de IDS nos ayuda a determinar la categoría que se va a utilizar en los diferentes sistemas para que puedan satisfacer las necesidades de seguridad que requiera la organización. Para el desarrollo del presente trabajo de integración curricular el enfoque se centra en el uso de la herramienta Suricata como NIDS

ya que tiene la capacidad de analizar el tráfico en tiempo real y así detectar patrones de comportamientos sospechosos que puedan infringir redes empresariales.

La implementación de Suricata como una herramienta NIDS nos va a ayudar a abordar distintos desafíos en la detección de amenazas en diferentes entornos donde la conexión ya el intercambio de datos son esenciales. Además, la aplicación de Suricata como un NIDS para el caso de estudio en la empresa seleccionada, nos va a ayudar mitigar posibles riesgos de seguridad al analizar y aplicar medidas requeridas en la infraestructura de red.

2.3.3 IDS VS IPS

Dentro del mundo de la seguridad de la información, la detección y prevención son dos términos generales que nos ayudan a describir las prácticas de seguridad utilizadas dentro de una empresa o una organización para poder detectar amenazas, mitigar ataques y bloquear nuevas amenazas que surgen con el paso de los años (Becolve, 2020).

La prevención de intrusiones es el proceso de detectar intrusiones y posibles amenazas para así detener los posibles intentos de los incidentes detectados. Un sistema de prevención de intrusiones (Intrusion Prevention System, por sus siglas en inglés) es una herramienta que se utiliza principalmente para proteger sistemas o la red de ataques e intrusiones. El enfoque principal de un sistema de prevención de intrusiones es identificar los posibles incidentes, registrar la información de los incidentes, aplicar medidas y políticas para detenerlos e informar sobre los incidentes a los administradores de red. Los IPS responden ante las posibles amenazas que detectan dentro del sistema o de la red utilizando varias técnicas de respuesta evitando que el ataque logre éxito (West, 2014).

Los IPS pueden analizar los protocolos y el tráfico de las conexiones en tiempo real para así poder determinar si se está produciendo o se va a producir un incidente. Identifican los ataques según los patrones, anomalías y comportamientos sospechosos que pueden comprometer los sistemas y después del análisis, permite bloquear o tener acceso a la red, esto es posible mediante la implementación de políticas que se basan en un monitoreo de tráfico monitorizado, es decir, el IPS tiene la capacidad de poder descartar paquetes y

desconectar conexiones en caso de detectar un posible intruso o amenaza dentro de la red (INCIBE, 2020).

La principal diferencia que existe entre un sistema de detección de intrusiones y un sistema de prevención de intrusiones se basa en la respuesta que brindan luego de detectar una amenaza. Los IDS reaccionan de manera reactiva, es decir identifica la detección de intrusos y amenazas para luego enviar alertas a los administradores de red para que tomen las respectivas medidas según la amenaza. Sin embargo, los IPS reaccionan de una manera más proactiva ya que además de detectar las posibles amenazas, bloquea en ese instante el tráfico malicioso, desconecta conexiones o bloquea ataques preventivos de aplicaciones utilizando patrones, todo depende de la política o configuración que se le establezca al IPS.

Las semejanzas que comparten un IDS con un IPS radican principalmente en los procesos iniciales de detección ya que ambos supervisan y detectan el sistema o la red en busca de actividades maliciosas (Geekflare, 2021). Algunos puntos en común que comparten son los siguientes:

- Monitorización: Tanto como los IDS e IPS monitorizan y supervisan la red en función de los parámetros especificados y las necesidades de seguridad (Geekflare, 2021).
- Detección de amenazas: Ambas herramientas leen los paquetes que transitan por la red y detectan las posibles amenazas. En caso de encontrar una amenaza, marcan ese paquete de datos como malicioso (Geekflare, 2021).
- Aprendizaje: Ambas herramientas utilizan tecnologías que permiten aprendizaje automático y así comprender nuevas amenazas emergentes además de patrones de ataque. De esta manera responden mejor ante amenazas modernas (Geekflare, 2021).
- Registro: Una vez que el IPS o el IDS analicen y detecten una amenaza, registran la amenaza para que, en futuras ocasiones, si se encuentran con la misma amenaza o un patrón similar, reaccionen inmediatamente dependiendo del tipo de herramienta (Geekflare, 2021).
- Alerta: Los IDS y los IPS envían alertas a los administradores de red una vez que detecten una amenaza. Esto ayuda a que el personal de seguridad se

encuentre preparado para cualquier escenario y actuar con rapidez (Geekflare, 2021).

Para el presente trabajo de integración curricular, es importante comprender las diferencias que existen entre un IDS (Sistema de Detección de Intrusos) y un IPS (Sistema de Prevención de intrusos), ya que nos proporciona la información necesaria para la descripción de la herramienta seleccionada que se va a utilizar en el caso de estudio. El análisis de tráfico de red se va a limitar con el uso de la herramienta Suricata como IDS dado la naturaleza de la red empresarial y los objetivos de la presente investigación. La elección de Suricata como un IDS permite ajustar de mejor manera la perspectiva de una detección pasiva al monitorizar, analizar el tráfico de red y alertar cualquier incidencia o comportamiento sospechoso que encuentre, sin interferir en las operaciones normales de la red. El conocimiento de las diferencias que existen entre un IDS y un IPS es fundamental para optimizar la configuración de la herramienta que se va a aplicar, además, de las expectativas del rendimiento al momento de analizar el tráfico de red dentro del presente caso de estudio.

2.4 HERRAMIENTA SURICATA COMO IDS

En el mundo de la ciberseguridad, la integridad, seguridad y disponibilidad de la red es fundamental dentro de cualquier organización. A medida que las redes van creciendo con el paso del tiempo, la complejidad en infraestructura y en tamaño cada día es más vulnerable frente ataques, por lo que es importante tener en cuenta el uso de un sistema de detección de intrusiones y prevención de intrusiones robusto (Gunashree, 2024).

2.4.1 QUÉ ES SURICATA

Suricata es una herramienta software que sirve como sistema de detección de amenazas y análisis del tráfico de redes. Suricata es una herramienta de código abierto desarrollada por la Open Information Security Foundation (OISF) que se utiliza en redes de alto rendimiento y por la mayoría de las organizaciones privadas y públicas, para proteger sus activos más importantes (Gunashree, 2024).

La capacidad de Suricata le permite trabajar de las siguientes maneras:

- Sistemas de Detección de Intrusiones (IDS): Suricata permite monitorear el tráfico de red en busca de actividades sospechosas o violaciones de políticas para luego registrar estas actividades en base de alertas y posteriormente realizar su análisis (Gunashree, 2024).
- Sistema de Prevención de Intrusiones (IPS): Además de que Suricata trabaje como un IDS, puede funcionar como IPS, detectando actividades sospechosas y así bloqueando activamente el tráfico aplicando políticas y reglas específicas en su configuración de reglas (Gunashree, 2024).
- Monitoreo de Seguridad de Red (NSM): Suricata es una herramienta que ayuda a monitorear la red de manera integral. Captura todo el tráfico que pasa por la red y analiza los datos de la red para detectar posibles amenazas potenciales, por lo que es una excelente herramienta para monitorear la seguridad de la red (Gunashree, 2024).

2.4.2 USO DE SURICATA COMO IDS

Suricata puede actuar como un sistema de detección de intrusiones (IDS), también puede funcionar como un sistema de prevención de intrusiones (IPS), y puede utilizarse como herramienta para poder supervisar el tráfico y la seguridad de la red. Suricata se puede configurar como un IDS basado en host para poder monitorear el tráfico de una sola maquina o configurar como un IDS pasivo para poder monitorear el tráfico que pasa por una red de distintas máquinas y notificar al administrador de red cuando detecta una actividad maliciosa (Berman, 2019).

Suricata viene integrado con un conjunto de reglas que permite identificar y alertar ante diversas amenazas que encuentre en la red. Sin embargo, se puede complementar con un conjunto de reglas externas. Estas reglas externas se pueden actualizar constantemente al momento de utilizar Suricata, o se pueden modificar las reglas ya existentes para dar un mejor enfoque hacia cualquier amenaza que pueda ser un peligro en la red (Berman, 2019).

Suricata al actuar como un IDS pasivo no interfiere en el flujo de tráfico de la red en la que se está capturando los datos. Suricata establece una mezcla de varios métodos de

detección lo que permite detectar amenazas conocidas y ataques nuevos (Gunashree, 2024). Los métodos que utiliza Suricata son los siguientes:

- Detección basada en firmas: La detección basada en firmas es uno de los principales métodos que utiliza Suricata para poder identificar amenazas ya que se basa en un conjunto de reglas predefinidas, o firmas, que describen ciertos patrones que están asociados con anomalías. Cuando Suricata detecta en el tráfico un paquete que coincide con una firma genera una alerta. Las reglas de Suricata son altamente configurables y los usuarios pueden personalizar sus reglas o usar conjuntos de reglas aportados por la comunidad como Emergin Threats o Proofpoint (Gunashree, 2024).
- Detección basada en anomalías: Además de la detección basada en firmas, Suricata puede detectar e identificar anomalías que encuentre en el tráfico de red y así indicar un posible problema de seguridad. Esto puede incluir volúmenes de tráfico alto o uso inesperado de protocolos (Gunashree, 2024).
- Análisis de Protocolos: Suricata permite inspeccionar el tráfico en la capa de aplicación por lo que permite tener la capacidad de analizar los protocolos legítimos que pueden estar asociados ante posibles amenazas. Esto resulta útil para detectar ataques complejos que pueden explotar vulnerabilidades en la capa de aplicación (Gunashree, 2024).

2.4.3 HERRAMIENTAS SIMILARES A SURICATA

Además de Suricata, existen otras herramientas ampliamente utilizadas que también trabajan como sistemas de detección de intrusiones. Estas herramientas son “Snort” y “Zeek” (antes conocido como Bro)

Snort es un IDS/IPS desarrollado por Cisco que utiliza un método similar de detección basado en firmas. Snort inspecciona el tráfico de red y busca patrones predefinidos que coinciden con la actividad maliciosa. Snort se puede configurar para al momento de detectar una firma coincidente, se activen acciones predefinidas como generar alertas o bloquear el tráfico malicioso. Snort se centra en la capa de red para la inspección de tráfico (Robinette, 2024).

Zeek, anteriormente conocido la herramienta como “Bro”, no funciona como un sistema de detección de intrusos tradicional dedicado. Zeek funciona como un analizador de tráfico de red que captura y realiza un análisis profundo de todo el tráfico mediante la implementación de scripts personalizados. El personal encargado de la seguridad de red tiene el trabajo de identificar actividades sospechosas y de implementar nuevos scripts según sus necesidades. Zeek ofrece un enfoque más flexible para la investigación de red, sin embargo, requiere un mayor nivel de experiencia para la configuración e interpretación de los resultados (Robinette, 2024).

2.4.4 CUADRO COMPARATIVO ENTRE HERRAMIENTAS IDS

En el presente punto, se va a mostrar las diferencias de cada herramienta IDS (Suricata, Snort y Zeek) mediante un cuadro comparativo junto a sus características principales.

Característica	Suricata	Snort	Zeek
Tipo de Herramienta	IDS/IPS y Monitoreo de Seguridad de red (NMS)	IDS/IPS	Analizador de tráfico
Código	Abierto (OSIF)	Abierto (Cisco)	Abierto
Arquitectura	Multi-hilo	Mono-hilo	Mono-hilo
Método de Detección	Métodos basados en firmas, en anomalías y en políticas.	Métodos basados en firmas.	Métodos basados en análisis de eventos y uso de scripts.
Rendimiento	Alto rendimiento y soporte de grandes volúmenes de datos.	Limitado en redes de alto tráfico.	Limitado en grandes volúmenes de

			datos y en escalabilidad
Capacidades Adicionales	Inspección profunda de paquetes, soporte a TLS/SSL y análisis detallado de tráfico	Análisis básico de tráfico.	Análisis detallado del tráfico a nivel de aplicación.
Ventajas Principales	Proporciona detección avanzada y escalabilidad.	Tiene una mayor comunidad y reglas actualizadas.	Flexibilidad en uso para análisis a nivel de aplicación.
Limitaciones Principales	Requiere el uso de más recursos.	Menor rendimiento en redes complejas.	Requiere una experiencia técnica avanzada.

2.4.5 JUSTIFCACIÓN DEL USO DE SURICATA

En el presente trabajo de titulación, se va a utilizar Suricata como IDS pasivo para poder capturar y analizar el tráfico de red de la empresa de selección. Suricata es una herramienta diseñada para poder capturar y analizar grandes volúmenes de datos, y a diferencia de las otras herramientas ya vistas, en términos de rendimiento y seguridad y monitoreo constante, suricata destaca completamente.

Gracias a su arquitectura multi-hilo, Suricata permite manejar grandes volúmenes de tráfico sin comprometer la velocidad o precisión de los detalles capturados. Suricata permite aprovechar múltiples núcleos en procesadores modernos por lo que es ideal al analizar tráfico de redes empresariales con alta capacidad.

Suricata utiliza múltiples métodos de detección ya sea basado en firmas, basado en anomalías o el establecimiento de políticas personalizadas lo que permite ser una

herramienta que pueda detectar amenazas ya conocidas o comportamientos sospechosos dentro de la red.

Suricata ofrece múltiples capacidades avanzadas para analizar el contenido completo de los paquetes que captura, no solo se centra en el encabezado, sino que permite detectar el contenido completo incluso de tráfico cifrado por TLS/SSL. Además, suricata tiene un soporte nativo para el análisis y monitoreo de diversos protocolos (HTTP, DNS, FTP, entre otros).

Por estos motivos, se va a utilizar Suricata en el presente trabajo de titulación ya que lo convierte en una herramienta completa, ideal y robusta para realizar el análisis del tráfico de una red empresarial como la del presente caso de estudio. A diferencia de las herramientas Snort y Zeek, Suricata es una herramienta que cumple con los objetivos del presente trabajo de titulación además de ser eficiente para la detección de amenazas de manera proactiva y monitoreo continuo del tráfico de red.

CAPÍTULO III: MARCO METODOLÓGICO

3.1 DISEÑO DE LA INVESTIGACIÓN

Para el diseño metodológico del presente trabajo de titulación, no existe algún estándar establecido o una metodología fija en el que se plantee la implementación de Suricata. Sin embargo, en los siguientes temas posteriores del presente capítulo, se cubren todos los puntos que llevarán a cabo la implementación de Suricata en la empresa seleccionada. Los puntos cubren desde el análisis y preparación del entorno de red hasta la visualización y análisis del tráfico capturado con la herramienta Zui.

3.1.1 TIPO DE ESTUDIO: DESCRIPTIVO Y EXPERIMENTAL

El presente trabajo de titulación aplica un enfoque descriptivo y experimental para así poder analizar el tráfico de red mediante el uso de la herramienta Suricata como sistemas de detección de intrusiones (IDS). Este enfoque busca resolver problemas prácticos relacionados con la seguridad dentro de un entorno real y controlado.

El tipo de estudio que se aplica es descriptivo ya que se enfoca en caracterizar el tráfico de red que se captura con la herramienta Suricata. Esto incluye analizar patrones, anomalías, identificación de protocolos utilizados y eventos diarios registrados en archivos eve.json.

Además, el tipo de estudio se considera experimental ya que la herramienta Suricata se implementa dentro de un entorno controlado, asimismo, su integración con la herramienta Zui es necesario para poder analizar a profundidad los archivos eve.json de manera estructurada.

3.1.2 JUSTIFICACIÓN DEL ENFOQUE SELECCIONADO

El enfoque seleccionado combina un tipo de estudio descriptivo y experimental por las siguientes razones:

- La investigación contempla un problema real relacionado con el monitoreo del tráfico de red y la seguridad de red en varias redes virtualizadas dentro de un entorno controlado donde la empresa seleccionada maneja diversas actividades fundamentales.

- La aplicación del estudio es flexible ya que permite documentar el comportamiento del tráfico de red diariamente además de evaluar la eficacia de las herramientas utilizadas dentro de un entorno realista.
- El uso de la herramienta Suricata como IDS es crucial para reforzar la seguridad de las redes modernas, especialmente dentro de infraestructuras virtualizadas donde múltiples máquinas y componentes están en constante trabajo y compartiendo recursos.

El diseño experimental del presente trabajo de titulación ayuda a comprobar los objetivos relacionados con la capacidad y uso de la herramienta Suricata para detectar amenazas y gestionar grandes volúmenes de datos.

3.1.3 ALCANCE DEL ESTUDIO

El alcance de estudio del presente trabajo de titulación se limita al análisis diario del tráfico generado por las máquinas virtuales dentro del entorno donde se realizó la implementación de la herramienta durante un periodo específico. Se evalúa exclusivamente el desempeño de Suricata como IDS y su capacidad para integrarse con Zui para poder realizar la visualización de datos.

3.2 DISEÑO METODOLÓGICO

3.2.1 JUSTIFICACIÓN DEL DISEÑO METODOLÓGICO

El diseño metodológico del presente trabajo de titulación busca la manera de poder estructurar de manera lógica y sistemática las actividades necesarias para implementar, configurar y evaluar el uso de Suricata como un sistema de detección de intrusiones (IDS) dentro de un entorno virtualizado. El diseño se fundamenta en poder analizar de manera correcta el tráfico de red de múltiples máquinas virtuales que se encuentran en constante trabajo y compartiendo recursos, garantizando una correcta integración con la herramienta Zui que sirve para la visualización y análisis de los datos.

La metodología aplicada permite la implementación técnica de las diferentes herramientas que se van a utilizar dentro del trabajo de titulación, además, permite la evaluación práctica del sistema dentro de un entorno controlado.

3.2.2 PREPARACIÓN DEL ENTORNO

Para preparar el entorno donde se va a realizar la implementación de la herramienta Suricata se van a aplicar los siguientes puntos:

- Comprensión y análisis de la topología de red que maneja actualmente la empresa para un mejor entendimiento de la configuración de los equipos y las actividades que realizan.
- Creación de una máquina virtual dedicada para Suricata, asegurando que tenga acceso a la interfaz de red que recopila el tráfico de todas las máquinas virtuales.

3.2.3 IMPLEMENTACIÓN DE SURICATA COMO IDS

Una vez analizado y preparado el entorno donde se va a aplicar la herramienta Suricata, se prosigue con la implementación de la herramienta cubriendo los siguientes aspectos:

- Instalación y configuración de la herramienta Suricata dentro de la máquina virtual designada.
- Definición y configuración de las reglas específicas para poder monitorear el tráfico en la interfaz compartida por las máquinas virtuales.
- Validación del funcionamiento mediante capturas de tráfico que registre inicialmente Suricata.
- Configuración de la herramienta de rotación de registros, logrotate, para gestionar archivos eve.json generados por Suricata diariamente.

3.2.4 INTEGRACIÓN CON LA HERRAMIENTA ZUI

Una vez que se culminó con la instalación, configuración y validación de la herramienta Suricata, junto con la configuración de logrotate, se prosigue con la instalación de la herramienta de visualización de los datos Zui. Para ello se debe seguir los siguientes puntos:

- Instalación y configuración de la herramienta Zui para poder visualizar los datos generados por Suricata.

- Verificación de que los archivos eve.json generados por suricata sean cargados correctamente en Zui.
- Validación del funcionamiento de Zui mediante carga de archivos que permita una lectura clara para un análisis eficiente.

3.2.5 EVALUACIÓN DEL TRÁFICO Y VALIDACIÓN

Finalmente, una vez instalado y configurado correctamente la herramienta Zui, además de la validación de visualización de datos, se prosigue con la evaluación del tráfico mediante la lectura de los archivos eve.json que genera Suricata. Para ello, se cubren los siguientes aspectos:

- Carga y procesamiento de logs (eve.json) que genera Suricata diariamente en la herramienta Zui.
- Realización consultas específicas y filtrado interactivo utilizando Zui para visualizar los datos estructurados de los archivos que se carguen.
- Análisis detallado de los comportamientos anómalos o signos de actividad maliciosa que hayan sido detectados durante las consultas realizadas.
- Generación y visualización de gráficos con Power BI para comprender de mejor manera los archivos generados de suricata

3.3 HERRAMIENTAS Y TECNOLOGÍAS

3.3.1 HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE RED (SURICATA)

Suricata es una herramienta avanzada que trabaja como sistema de detección de intrusiones (IDS) y monitoreo de tráfico de red. Tiene la capacidad de registrar eventos a base de logs del tráfico de una red para que posteriormente se pueda analizar el comportamiento del tráfico en tiempo real. Los motivos porque se escogió Suricata en el presente trabajo de titulación son los siguientes:

- Captura y análisis del tráfico en tiempo real.
- Soporte para múltiples protocolos como HTTP, DNS, LTS, etc.
- Generación de archivos históricos json detallados (eve.json) que contiene eventos relevantes como alertas, flujos.

- Compatibilidad con reglas personalizadas y predefinidas.
- Capacidad para operar en modo promiscuo, capturando todo el tráfico en una interfaz específica.

En el presente trabajo de titulación, Suricata ayuda a fortalecer el monitoreo de tráfico de red generado por las máquinas virtuales que se encuentran dentro del entorno de la empresa de estudio y así, identificar posibles patrones sospechosos o maliciosos. Además, debido a su flexibilidad, la precisión en la detección de amenazas, la capacidad de poder integrarse con otras herramientas como Zui y su soporte en entornos virtualizados lo hace ideal para el análisis de tráfico.

3.3.2 HERRAMIENTA DE VISUALIZACIÓN DE DATOS (ZUI)

Zui es una herramienta interactiva diseñada para poder visualizar y analizar volúmenes de datos grandes. En el presente trabajo de titulación se utilizó específicamente para poder interpretar los datos generados por suricata. Zui ofrece múltiples capacidades que nos ayudó con el análisis e interpretación de los archivos json. Entre las características principales de Zui se encuentran:

- Interfaz gráfica intuitiva que permite la exploración y el análisis de eventos capturados.
- Soporte nativo para archivos json. En este estudio, los archivos generados por Suricata (eve.json).
- Capacidad para filtrar mediante consultas, buscar y visualizar eventos específicos de los archivos que se carguen.
- Representación gráfica que nos ayuda a poder identificar patrones o anomalías de manera más rápida y eficiente.

La herramienta Zui es ideal para el presente trabajo de titulación ya que tiene la capacidad de procesar grandes volúmenes de datos, además, de poder cargar y procesar archivos de tipo json y mostrar los archivos generados por Suricata en formato visualmente comprensible. Por lo que necesario en el análisis diario del tráfico sin la necesidad de depender únicamente en un formato textual.

3.3.3 HERRAMIENTA DE GENERACIÓN DE GRÁFICOS (POWER BI)

Power BI es una herramienta que sirve para poder realizar análisis de datos y visualizar datos. Esta herramienta es desarrollada por Microsoft y permite transformar datos complejos en datos interactivos junto con tableros personalizados. Esta herramienta es altamente flexible ya que facilita la conexión ante diversas fuentes de archivos. Tiene la posibilidad de conectarse frente a diferentes archivos como json, bases de datos, hojas de cálculo, APIS, etc. Con Power BI los usuarios pueden importar, transformar modelar datos para crear informes dinámicos y visualizaciones interactivas que se adapten a diferentes necesidades según el contexto con el que se utilice (Saavedra, 2023).

Para el presente trabajo de titulación, se va a utilizar la herramienta Power BI para así poder importar y cargar los archivos eve.json que genera Suricata. Estos archivos generados contienen información de registros como direcciones IPs, alertas, eventos, anomalías, etc. Una vez que se carguen y se importe los archivos se van a transformar los datos para así poder generar gráficos interactivos y poder analizar los datos. Power BI es ideal para trabajar con este tipo de datos ya que permite extraer información clave y poder visualizarla gráficamente.

3.3.4 INFRAESTRUCTURA TECNOLÓGICA

La infraestructura tecnológica que fue de uso para el desarrollo del presente trabajo de titulación incluye:

- Servidor HPE DL360 G10: Un servidor robusto diseñado para poder soportar diferentes cargas virtualizadas. El servidor ofrece los recursos suficientes para poder ejecutar múltiples máquinas virtuales simultáneamente, incluyendo la máquina donde se encuentra la herramienta Suricata.
- VMware ESXi Host Client: Un hipervisor para gestionar y administrar las máquinas virtuales que se encuentren alojadas en el servidor. Además, el hipervisor tiene la capacidad para configurar las redes virtuales e interfaces compartidas necesarias para así poder realizar la captura del tráfico.
- Logrotate: Una herramienta utilizada para poder gestionar los archivos eve.json generados por suricata diariamente. Gracias a esta herramienta se puede

automatizar la rotación, comprensión y eliminación periódica de archivos antiguos, asegurando así el uso eficiente del almacenamiento.

La integración de todas estas herramientas y de estas tecnologías permitió establecer un flujo eficiente desde la captura del tráfico con Suricata hasta el análisis visual con la herramienta Zui. Esta integración tecnológica asegura un sistema funcional y eficiente para el análisis del tráfico de red dentro de este entorno controlado y virtualizado.

CAPÍTULO IV: APLICACIÓN DE LA METODOLOGÍA

4.1 PREPARACIÓN Y ANÁLISIS DEL ENTORNO DE RED

4.1.1 TOPOLOGÍA Y CONFIGURACIÓN DEL ENTORNO

El presente trabajo de titulación, para realizar el análisis del tráfico de red en la empresa que se seleccionó, se tomó a consideración la topología actual que tiene y con la que se lleva a cabo todos sus procesos. A continuación, en la figura 8 se presenta una imagen de la topología actual de la empresa.

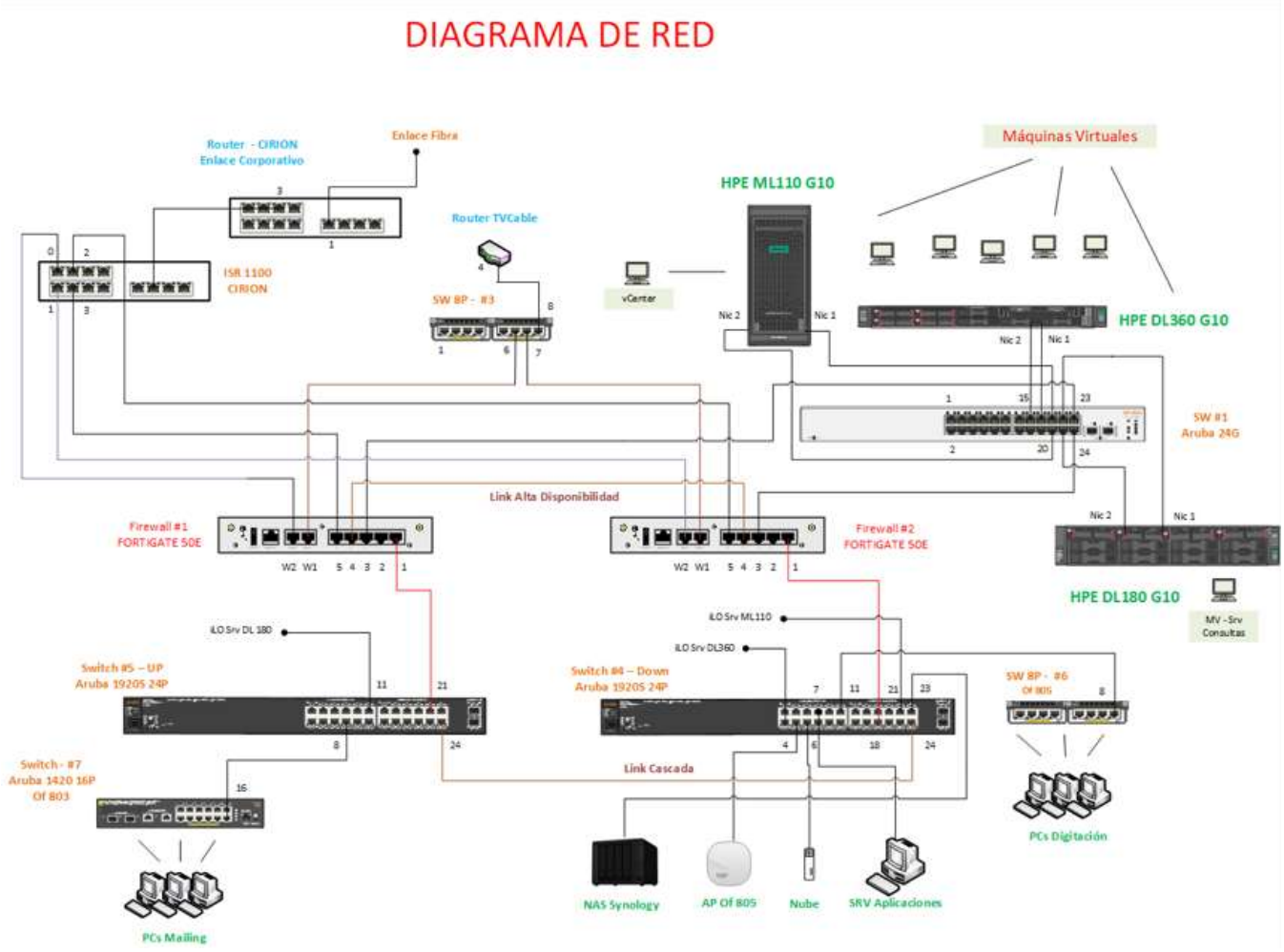


Figura 8 Diagrama de red de la empresa a selección. Fuente: Empresa seleccionada (2022)

En la figura 8, se puede observar que existe un servidor HPE DL3610 G10. Dentro de ese servidor están alojadas máquinas virtuales de diferentes clientes con las que la empresa trabaja.

El trabajo que se realiza en las máquinas virtuales es el siguiente: Cada máquina es un cliente diferentes de la empresa. Dentro de la empresa un grupo de personas, conocidas como digitadores, realizan envíos masivos de correos a los distintos clientes diariamente. La información que envían de estos correos es de los oficios. Los oficios son cartas de respuesta que se generan por las providencias judiciales que son cargadas en un portal de consultas que también maneja la empresa. Los oficios son generados por dos máquinas que de igual manera pertenece al grupo de máquinas virtuales, sin embargo, estas máquinas no tienen salida a internet ya que solo generan oficios y lo digitadores con estos oficios realizan él envió de correos masivo a cada cliente diariamente, por lo que las demás máquinas virtuales si tienen salida a internet y están en constantemente trabajo enviando y recibiendo información.

El servidor está conectado a un switch Aruba 24g (SW #1) por el cual permite la conexión hacia diferentes entornos además de su conexión hacia internet, pasando por el firewall FortiGate 50E (Firewall #2). En la figura 9 se puede observar que el servidor tiene dos puertos conectados hacia el SW#1.

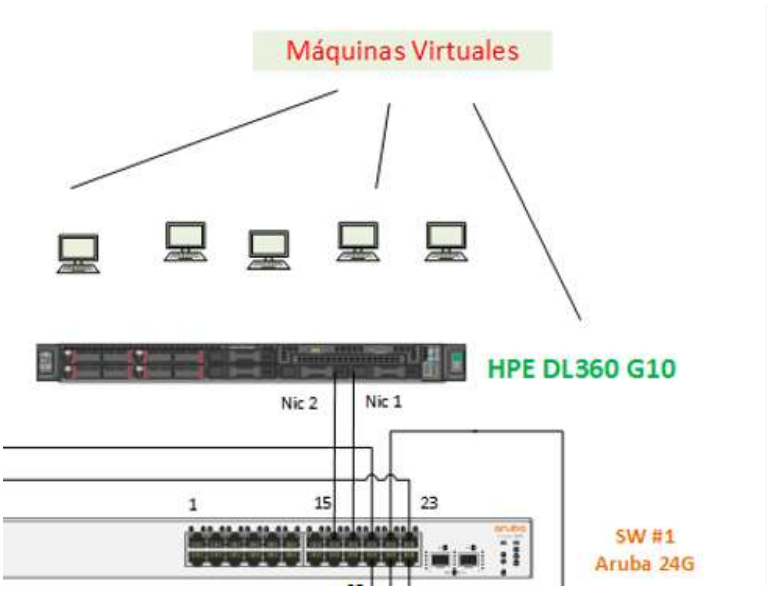


Figura 9 Conexión servidor hacia switch. Fuente: Empresa seleccionada (2022)

En la figura 10 se puede ver las diferentes máquinas virtuales están alojadas en un hipervisor, el hipervisor es de VMware ESXI Host Client. Este hipervisor sirve para poder gestionar, administrar y permite la comunicación entre la parte física (host) y las máquinas virtuales.

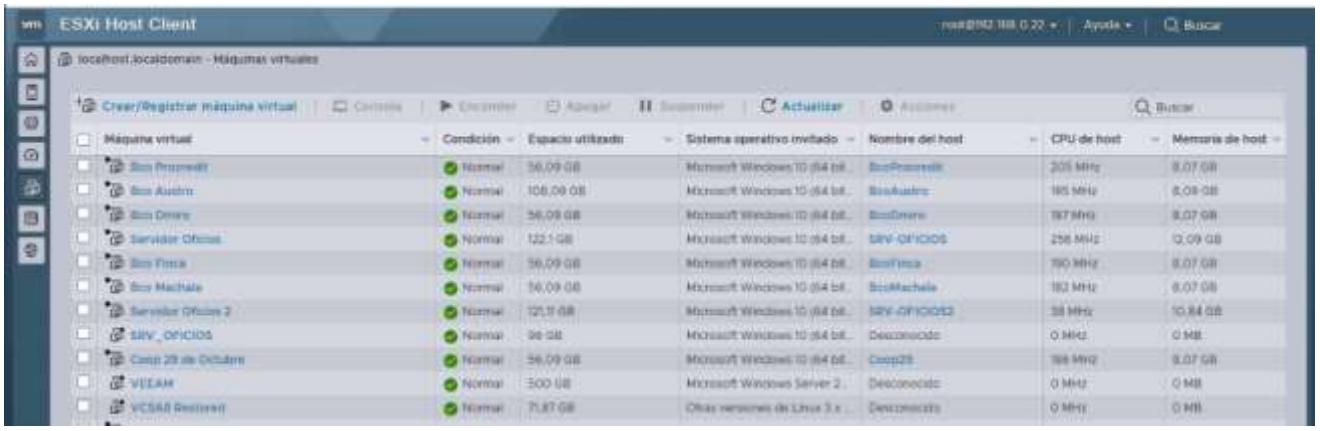


Figura 10 Máquinas virtuales alojadas en el host. Fuente: VMware ESXi Host Client (s.f)

Para que exista comunicación dentro del entorno virtualizado de las diferentes máquinas virtuales, incluyendo la máquina virtual suricata, la configuración de red interna del hipervisor VMware ESXi Host Client se encuentra como se muestra en la figura 11:

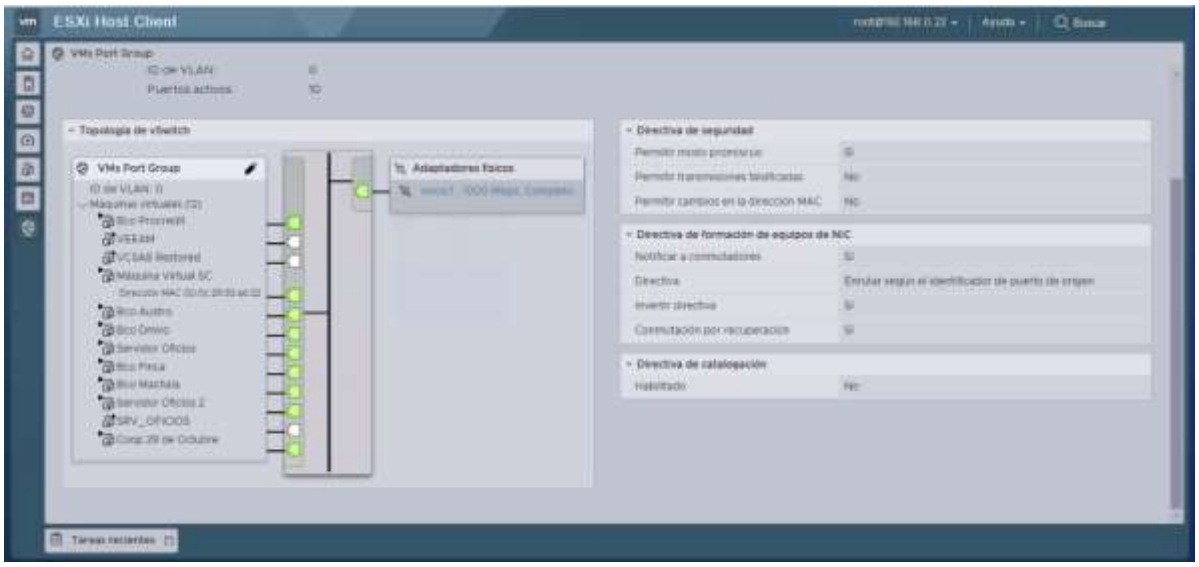


Figura 11 Topología del vSwitch. Fuente: VMware ESXi Host Client (s.f)

En la figura 11 se puede ver que, dentro de la red, está configurado un vSwitch (Virtual Switch) en donde la configuración de la topología del vSwitch incluye:

- VMs Port Group: Es el grupo de puerto asignados a las máquinas virtuales (VMs). Aquí se encuentra configurado las redes virtuales que comparten las VMs.
- Máquinas virtuales listadas: Son las diferentes máquinas virtuales conectadas al vSwitch.
- Adaptador físico: El adaptador físico conectado al vSwitch es “vmnic1”. Este adaptador es el que se muestra en la figura 9 como Nic 1.
- El modo promiscuo está activado por lo que es esencial para que la máquina con Suricata pueda capturar todo el tráfico que pasa por el vSwitch.

Dentro de este mismo entorno, se va a crear la máquina virtual donde se va a instalar la herramienta Suricata. En la figura 12 se puede observar la máquina virtual creada con el nombre “Máquina Virtual SC” para diferenciar de las otras.

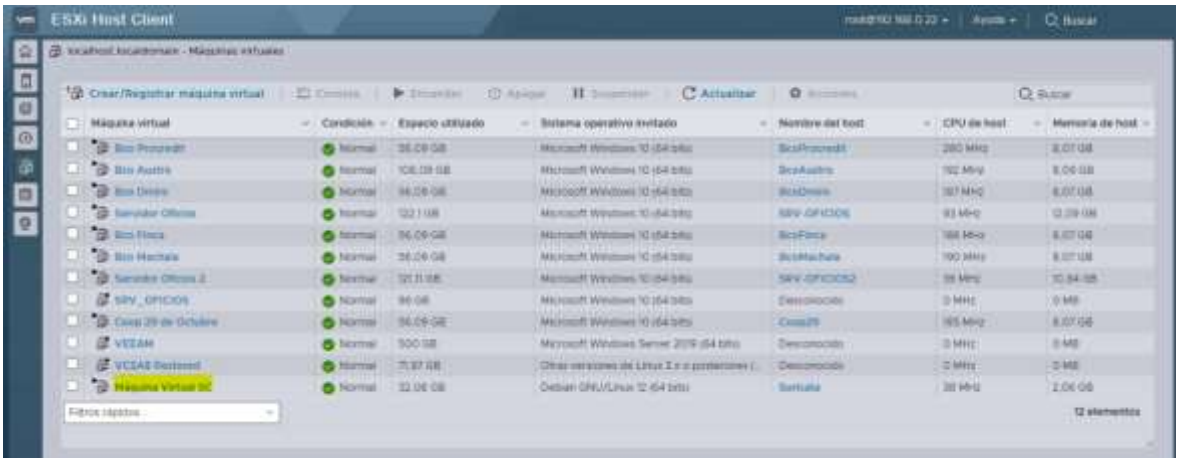


Figura 12 Creación Máquina Virtual SC. Fuente: VMware ESXi Host Client (s.f)

Para que la herramienta Suricata pueda recibir el tráfico de las distintas máquinas virtuales, se debe tomar en cuenta que la configuración de red de la máquina virtual suricata debe ser la misma a las otras máquinas, por lo que el adaptador de red va a ser el que comparten todas las máquinas VMs Port Group. Además, la IP asignada debe estar dentro del mismo rango de IPs, en este caso 192.168.0.100/24. En la figura 13 se puede ver la configuración de la MV de suricata.

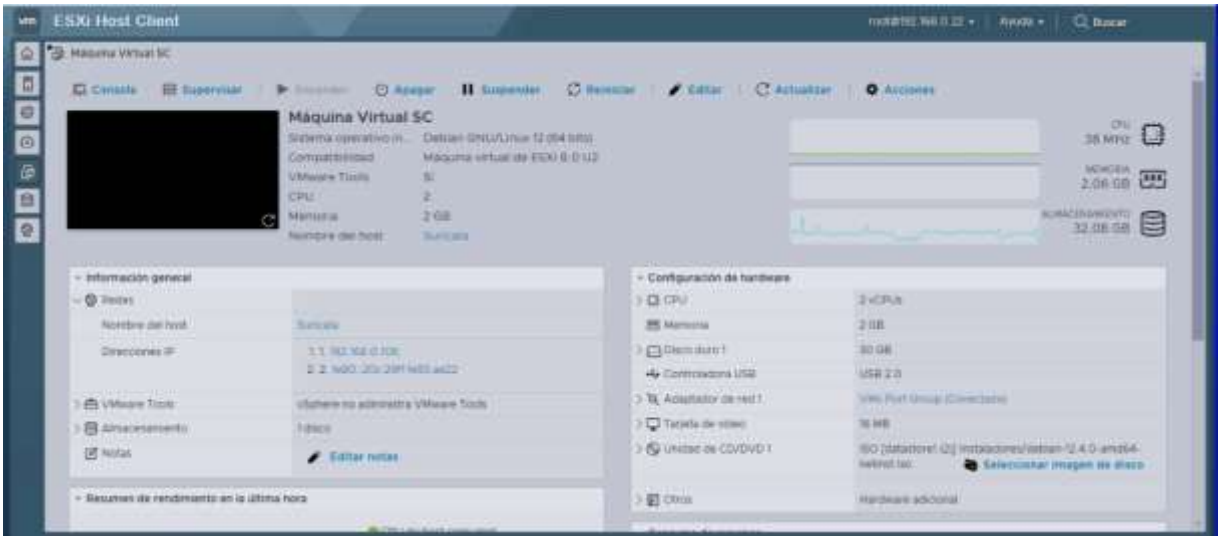


Figura 13 Configuración Máquina Virtual SC. Fuente: VMware ESXi Host Client (s.f)

Una vez ya configurado la máquina virtual Suricata, se procede con la validación de conexión ping hacia la puerta de enlace (Gateway) que comparten todas las máquinas,

la IP del Gateway es 192.168.0.99. Además, se procede con una prueba desde una de las máquinas con una conexión ping hacia la máquina virtual suricata.

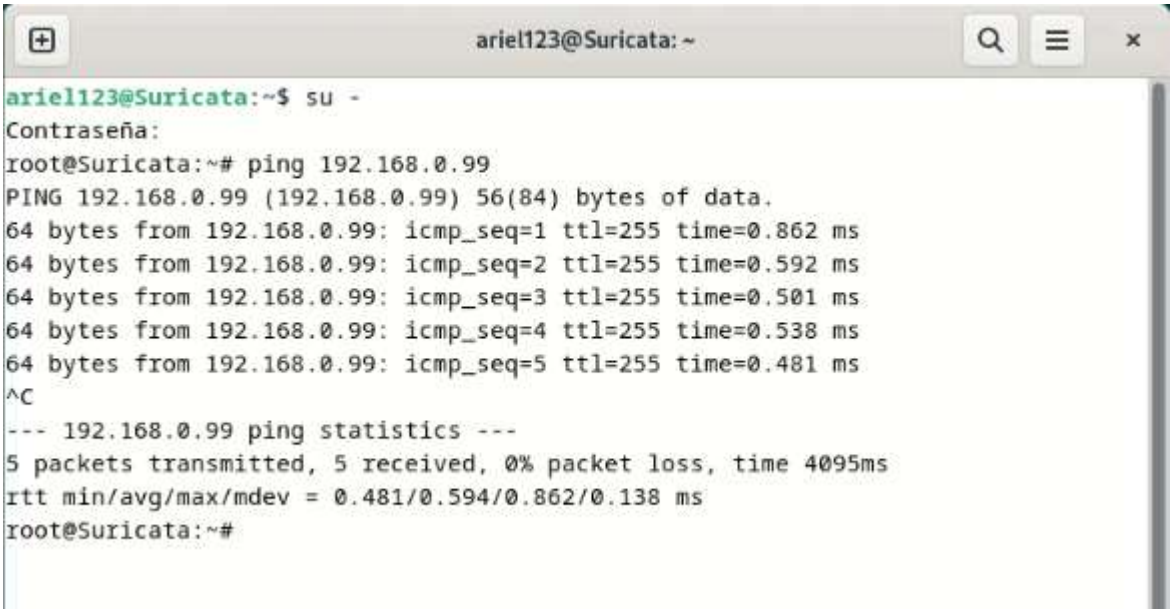


Figura 14 Ping desde la Máquina Virtual SC hacia el Gateway. Fuente: Máquina Virtual SC (s.f)

En la figura 14 se puede visualizar la conexión ping que se hace desde la máquina virtual de suricata hacia la puerta de enlace que comparten todas las otras máquinas virtuales.

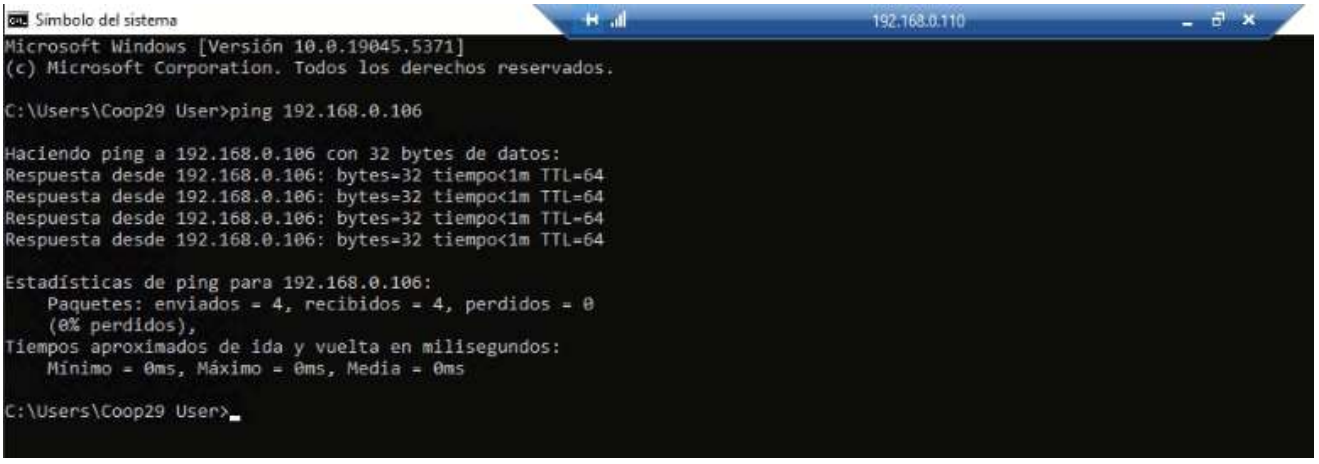


Figura 15 Ping desde otra máquina virtual hacia máquina de suricata. Fuente: VMware ESXi Host Client (s.f)

En la figura 15 se puede visualizar la conexión ping que se hace desde una de las máquinas virtuales hacia la máquina virtual suricata.

Ya teniendo conexión se puede validar que la máquina se encuentra dentro de la red, por lo que se prosigue con la instalación de la herramienta Suricata.

4.2 CONFIGURACIÓN INICIAL Y CAPTURA DEL TRÁFICO

4.2.1 INSTALACIÓN DE SURICATA

Una vez que se haya realizado el análisis y comprensión del entorno de la red, además de la creación y configuración de la máquina virtual donde se va a instalar la herramienta Suricata, se procede con la instalación y configuración de la herramienta. Se debe tomar en cuenta que el sistema operativo en el que se va a trabajar es Debian GNU/Linux 12 (64 bits).

Primero, para comenzar con la instalación se debe actualizar el sistema operativo para resolver cualquier error que pueda aparecer. En la figura 16 se puede observar el uso del comando “sudo apt update && apt upgrade -y” para actualizar el sistema operativo:

Figura 16 Actualización del sistema operativo. Fuente: Máquina Virtual SC (s.f)

Una vez finalizado, se procede a instalar las dependencias y herramientas que son necesarias y nos ayudarán a compilar y ejecutar software en sistemas Linux. En el contexto de aplicaciones como Suricata, es fundamental instalar estas dependencias y herramientas para poder dar uso. En la figura 17 se puede visualizar el uso del comando “sudo apt-get install -y libpcap-dev libpcre3-dev libyaml-dev libjansson-dev libmagic-dev zlib1g-dev pkg-config make gcc” para instalar las dependencias y herramientas necesarias.

Figura 17 Instalación de herramientas y dependencias. Fuente: Máquina Virtual SC (s.f)

Una vez instalado las dependencias y herramientas necesarias para poder trabajar con Suricata, se procede a instalar Suricata utilizando el siguiente comando "sudo apt install -y suricata". En la figura 18 se puede observar el uso del comando:

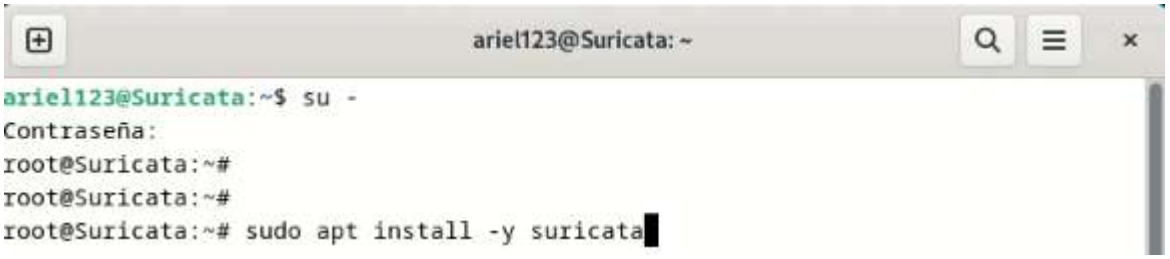


Figura 18 Instalación de suricata. Fuente: Máquina Virtual SC (s.f)

Una vez instalado la herramienta Suricata, se puede comprobar que todo este correcto verificando la versión. Para ello se utiliza el siguiente comando "suricata -V". En la figura 19 se puede ver la que versión que se instaló de suricata es la 6.0.10:

Figura 19 Verificación de la versión de suricata. Fuente: Máquina Virtual SC (s.f)

Además, se puede verificar el estado de suricata con el comando "sudo systemctl status suricata". En la figura 20 se puede visualizar que el servicio de suricata está corriendo y activo:

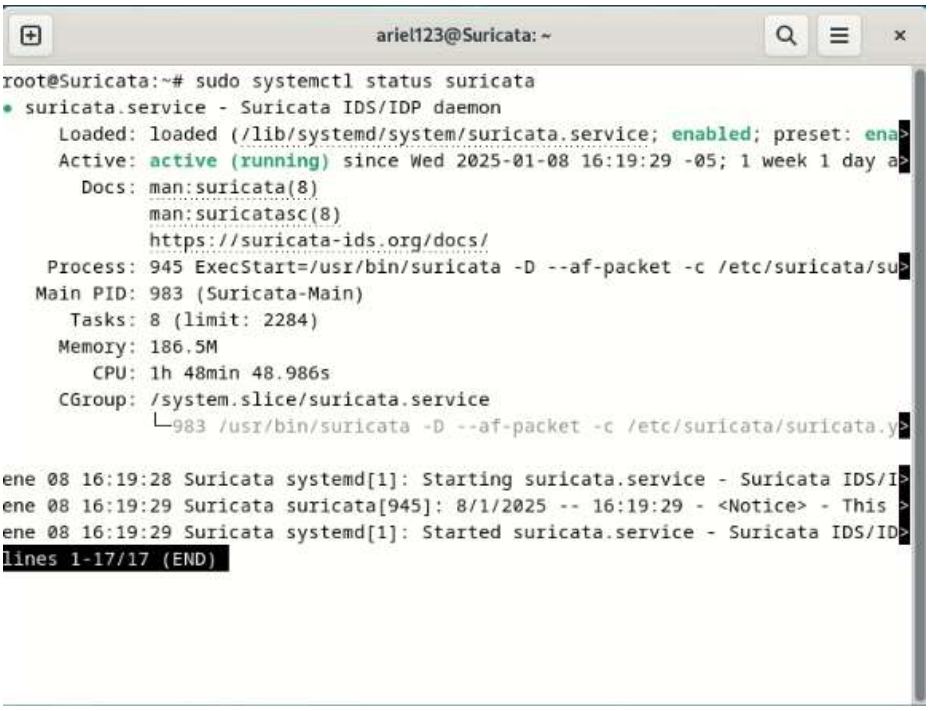


Figura 20 Verificación del estado de suricata. Fuente: Máquina Virtual SC (s.f)

4.2.2 CONFIGURACIÓN DE REGLAS

Una vez que ya se haya instalado la herramienta suricata, se debe empezar a configurar correctamente la herramienta para que pueda capturar el tráfico de las diferentes máquinas virtuales. Primero se debe conocer la interfaz de red activa por donde Suricata va a inspeccionar el tráfico de red. En la figura 21 se puede ver el uso del comando "ip link show" que nos muestra la información de las interfaces de red de la máquina:

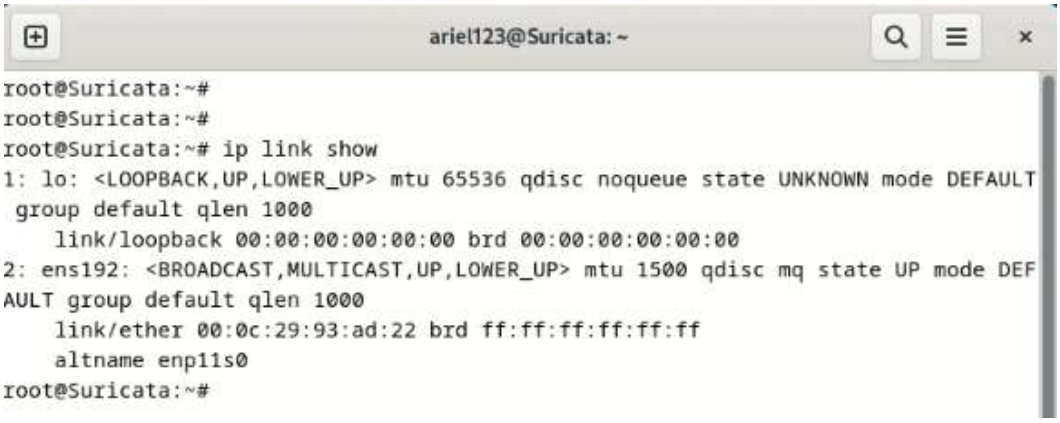


Figura 21 Comando para visualizar las interfaces de red. Fuente: Máquina Virtual SC (s.f)

Se puede observar que la interfaz activa es ens192. Una vez verificado la interfaz de red, se debe entrar al archivo suricata.yaml para poder editar la configuración. Para poder entrar al archivo de configuración se debe utilizar el comando “sudo nano /etc/suricata/suricata.yaml”

Figura 22 Archivo de configuración nano de suricata.yaml. Fuente: Máquina Virtual SC (s.f)

En la figura 22 se puede observar el archivo de configuración nano de suricata.yaml el cual nos va a permitir configurar las diferentes reglas de suricata para poder capturar el tráfico.

Dentro del archivo de configuración se debe buscar el paso 3. En el archivo de configuración se encuentra en inglés de la siguiente manera “Step 3: Configure common capture settings”

Figura 23 Configuración del archivo nano_1. Fuente: Máquina Virtual SC (s.f)

En la figura 23 dentro del archivo de configuración se puede visualizar que en la sección de interface se asigna la interfaz “ens192” ya que es la interfaz por donde suricata va a poder inspeccionar el tráfico. Los otros parámetros se dejan de la misma manera como viene por predeterminado al momento de instalar suricata.

Figura 24 Configuración del archivo nano_2. Fuente: Máquina Virtual SC (s.f)

En la figura 24 dentro del archivo de configuración se puede visualizar que la interfaz por predeterminada está asignada por “default”. Esta configuración sirve como predeterminada para las interfaces no específicas. Además, de igual manera se asigna la interfaz ens192 para capturar el tráfico utilizando libcap, que es una biblioteca para captura de paquetes.

Figura 25 Configuración del archivo nano_3. Fuente: Máquina Virtual SC (s.f)

Finalmente, en la figura 25 se puede visualizar las líneas finales del paso 3 del archivo de configuración nano de suricata.yaml. De igual manera los parámetros que se muestran no se deben aplicar ningún cambio.

Una vez realizado los cambios se guarda el archivo de configuración y se reinicia suricata con el comando “sudo systemctl restart suricata” como se muestra en la figura 26.

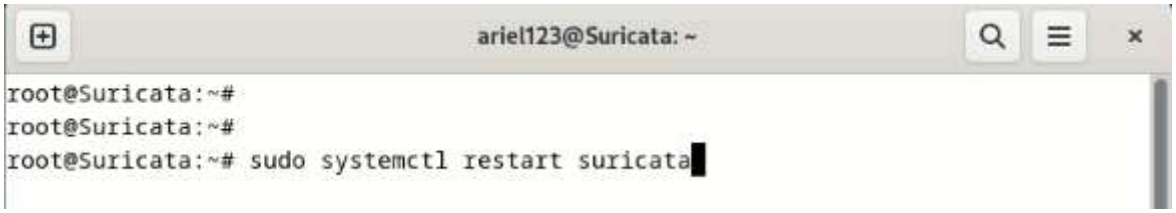


Figura 26 Reinicio del servicio suricata. Fuente: Máquina Virtual SC (s.f)

Para poder actualizar las reglas que proporcionan proveedores externos, se debe utilizar el comando “suricata-update -o /etc/suricata/rules” y así se actualiza el conjunto de reglas. En la figura 27 se puede ver la aplicación del comando:

Figura 27 Comando para actualizar las reglas. Fuente: Máquina Virtual SC (s.f)

Figura 28 Actualización de reglas desde Emergin Threats. Fuente: Máquina Virtual SC (s.f)

En la figura 28 se puede observar la actualización de las reglas de suricata. La actualización de las reglas se obtiene desde ET Emergin Threats, una plataforma gratuita que agrega las reglas de inspección al archivo /etc/suricata/rules de suricata.

Figura 29 Número de reglas actualizadas. Fuente: Máquina Virtual SC (s.f)

En la figura 29 se puede observar que se han agregado un total de 55869 reglas de las cuales se han habilitado 41746, se han removido 0 y se han modificado 0. Es importante estar actualizando las reglas de inspección en Suricata.

Finalmente, para verificar que suricata está capturando tráfico, se utiliza el comando “tail -f /var/log/suricata/fast.log” como se muestra en la figura 30:

```
root@Suricata:~# tail -f /var/log/suricata/fast.log
01/16/2025-18:18:05.379376  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.1.154:51459 -> 192.168.0.111:7680
01/16/2025-18:18:10.031415  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.0.102:52756 -> 192.168.0.111:7680
01/16/2025-18:18:45.517820  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.1.154:51460 -> 192.168.0.111:7680
01/16/2025-18:18:50.219969  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.0.102:52757 -> 192.168.0.111:7680
01/16/2025-18:19:06.038640  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.0.111:53618 -> 192.168.0.105:7680
01/16/2025-18:19:25.641142  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.1.154:51461 -> 192.168.0.111:7680
01/16/2025-18:19:30.331279  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.0.102:52758 -> 192.168.0.111:7680
01/16/2025-18:20:05.702819  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.1.154:51462 -> 192.168.0.111:7680
01/16/2025-18:20:10.456634  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.0.102:52760 -> 192.168.0.111:7680
01/16/2025-18:20:26.916454  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.0.111:53621 -> 192.168.0.105:7680
01/16/2025-18:20:45.797184  [**] [1:2027766:2] ET POLICY Windows Update P2P Activity [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP
 192.168.1.154:51464 -> 192.168.0.111:7680
```

Figura 30 Captura de tráfico de Suricata. Fuente: Máquina Virtual SC (s.f)

4.3 RECOPILACIÓN DE DATOS INICIALES

Una vez ya instalado y configurado correctamente la herramienta Suricata, se llevó a cabo la recopilación de los datos generados. Posteriormente, con los datos recopilados se realizó la visualización y análisis con la herramienta Zui.

4.3.1 GENERACIÓN DE ARCHIVOS

Suricata fue configurado para que pueda capturar el tráfico de red desde la interfaz activa en modo promiscuo, así permite monitorear todo el tráfico generado por las máquinas virtuales.

Todos los eventos capturados fueron registrados en archivos con formato json (eve.json). Estos eventos capturados constituyen la base para realizar un análisis posterior. Todos los logs generados por suricata se encuentran en el directorio predeterminado /var/log/suricata/ como se muestra en la figura 31:

Figura 31 Archivos recopilados por suricata (eve.json). Fuente: Máquina Virtual SC (s.f)

4.3.2 GESTIÓN DE ARCHIVOS CON LOGROTATE

Para poder realizar el análisis de los eventos eve.json generados por suricata, además de un control de almacenamiento y registro de logs, se procedió con la configuración de la herramienta logrotate. Logrotate es una herramienta diseñada para la administración de sistemas que generan una gran cantidad de archivos (logs). Logrotate puede automatizar tareas como rotación, compresión, eliminación y envío automático por correos de los archivos de registro, además, evita que estos archivos crezcan de manera descontrolada, ocupen demasiado espacio en el disco y afecten el rendimiento del sistema (Troan, 2019).

Para poder configurar la rotación diaria de archivos con la herramienta logrotate, primero se debe ingresar al archivo de configuración nano de logrotate con el comando "sudo nano /etc/logrotate.d/suricata" En la figura 32 se puede visualizar el uso del comando para poder ingresar al archivo de configuración.

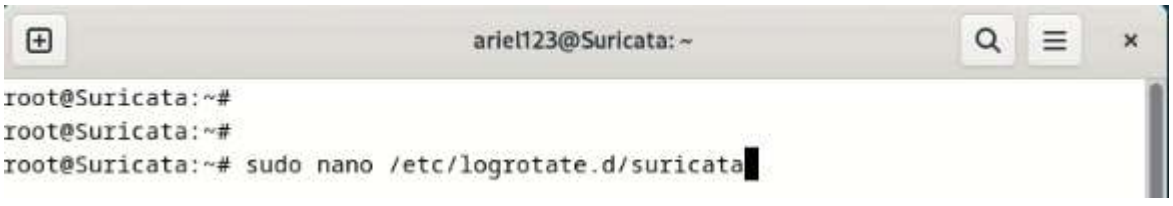


Figura 32 Comando archivo de configuración nano logrotate. Fuente: Máquina Virtual SC (s.f)

Dentro del archivo de configuración se debe aplicar la siguiente configuración como se muestra en la figura 33:

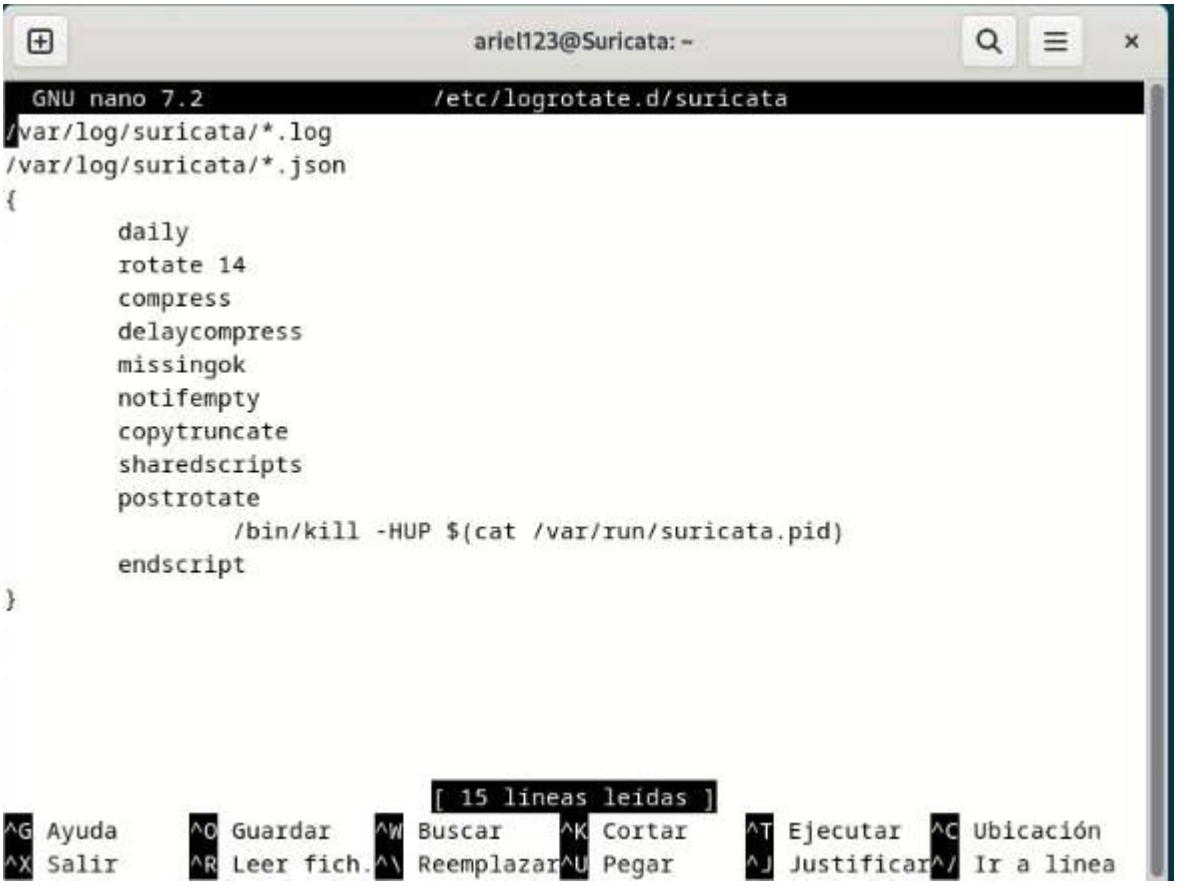


Figura 33 Archivo de configuración nano logrotate. Fuente: Máquina Virtual SC (s.f)

En la figura 33 se puede ver la configuración que se estableció de logrotate para que Suricata pueda rotar los archivos de logs diariamente. A continuación, se va a explicar las líneas del archivo de configuración para un mayor entendimiento:

‘daily’: Se asegura que los logs se roten diariamente.

‘rotate 14’: Conserva los logs de los últimos 14 días antes de eliminarlos.

‘compress’: Comprime los logs que se generan para así ahorrar espacio.

‘delaycompress’: Retrasa la comprensión hasta el siguiente ciclo de rotación. Esto sirve para evitar conflictos con procesos en curso.

‘missingok’: Evita errores si no encuentra archivos de log.

‘notifempty’: No rota archivos vacíos.

Una vez configurado el archivo nano de logrotate, se puede validar la rotación de los logs que genera suricata. En la figura 34 se puede visualizar los logs que se han generado en los últimos 10 días.

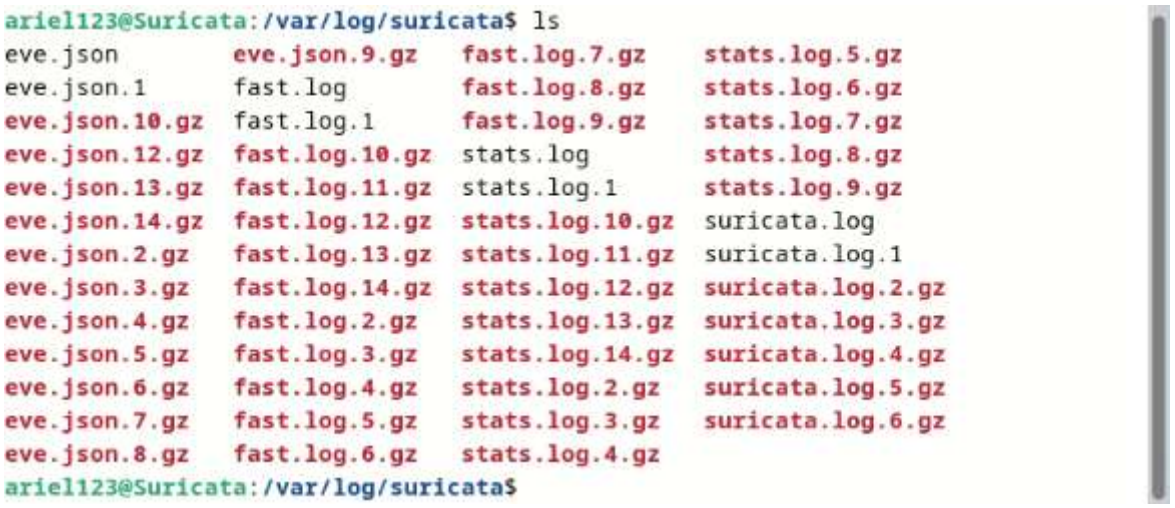


Figura 34 Archivos json que capturó suricata. Fuente: Máquina Virtual SC (s.f)

En la figura 34 se puede visualizar los archivos json que va capturando y guardando suricata en el directorio /var/log/suricata. A continuación, se va a explicar cada uno de los archivos generados por suricata.

‘eve.json’: Son los archivos json que contienen los eventos detallados detectados por Suricata.

‘fast.log’: Son archivos que contienen alertas rápidas en formato más simple y directo.

‘stats.log’: Son archivos que contiene las estadísticas del rendimiento y funcionamiento de la herramienta Suricata.

‘suricata.log’: Son los archivos principales del sistema. Registran la información general sobre la operación de Suricata.

Para la visualización y análisis de los datos con la herramienta Zui, se van a utilizar los archivos eve.json, ya que contiene los eventos detallados que han sido capturados del tráfico por la herramienta Suricata.

En la figura 34 también se puede visualizar en los archivos json una enumeración. Esta enumeración corresponde a la escritura continua, en este caso en eve.json, que realiza suricata mientras está en ejecución. La configuración de logrotate está establecida para que se renombre el archivo actual diariamente. El archivo que se está escribiendo en tiempo real es eve.json, por lo que el siguiente día, luego de completar la frecuencia establecida en la configuración de logrotate, va a pasar a ser eve.json.1. Si ya existe un archivo con el nombre eve.json.1, pues este se convierte en eve.json.2 y así sucesivamente.

Como la configuración de logrotate está establecido para comprimir los archivos rotados, los archivos más antiguos serán comprimidos como .gz como se observa en la figura 34.

4.4 VISUALIZACIÓN Y ESTRUCTRACIÓN DE DATOS DEL TRÁFICO

Para poder visualizar los datos y el tráfico capturado por Suricata, se va a instalar la herramienta “Zui” que permite la visualización de archivos json. En este caso, los archivos que se van a visualizar son los archivos generados eve.json y los datos se podrán visualizar de manera estructurada.

4.4.1 INSTALACIÓN Y CONFIGURACIÓN DE ZUI

Primero, se debe ingresar al enlace de descarga de la página oficial “https://www.brimdata.io/download/” como se muestra en la figura 35. Dentro de esta página debemos buscar el archivo .deb de Zui para poder instalar la herramienta.

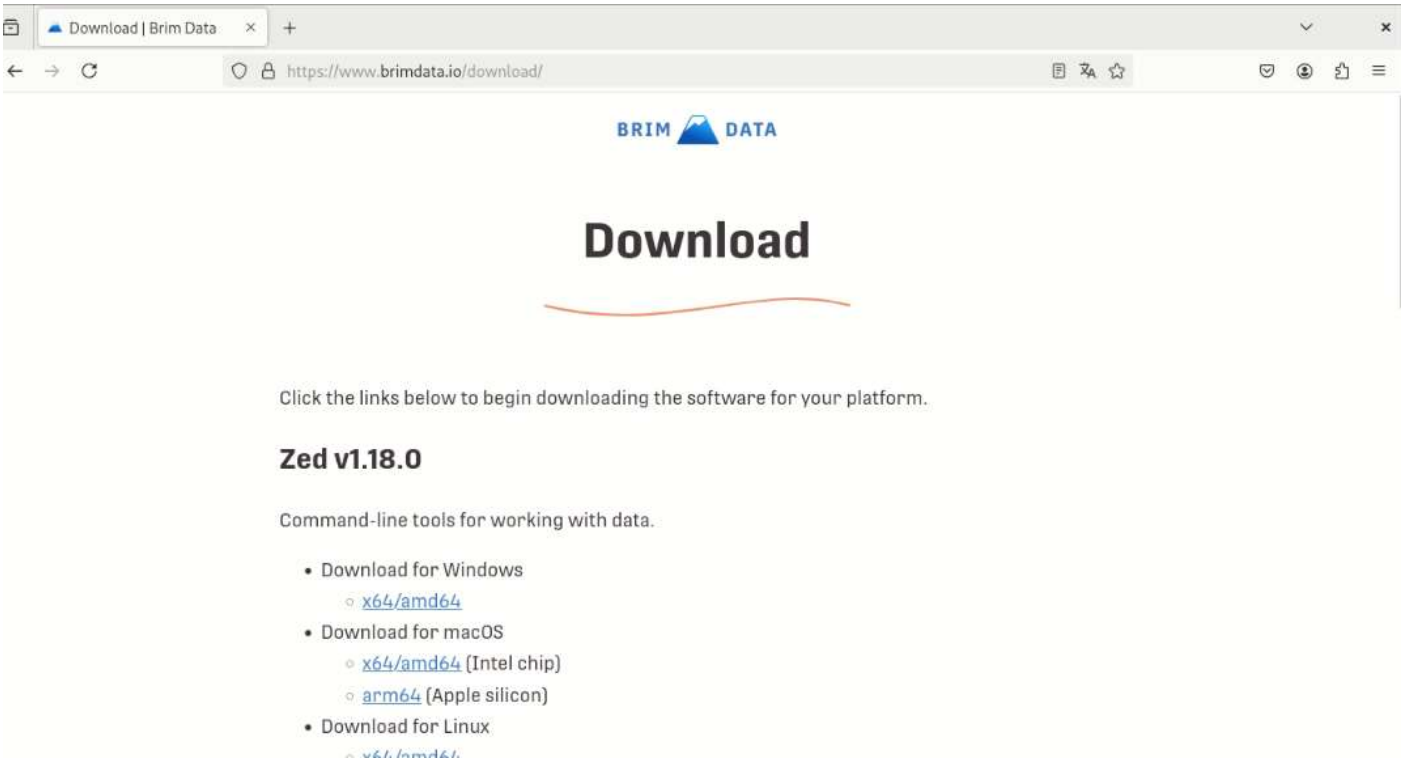


Figura 35 Página oficial para instalar Zui. Fuente: brimdata.io (s.f)

Una vez que ya se ingresó al enlace, debemos buscar el instalador de la herramienta Zui dentro de la página. Para nuestro caso debemos descargar la versión .debx64/amd64 para Ubuntu/Debian como se muestra en la figura 36.

Figura 36 Archivo .deb de descargas de Zui. Fuente: brimdata.io (s.f)

Luego de proceder con la descarga del archivo, podemos verificar la descarga en la carpeta de “Descargas” dentro de archivos como se muestra en la figura 37.

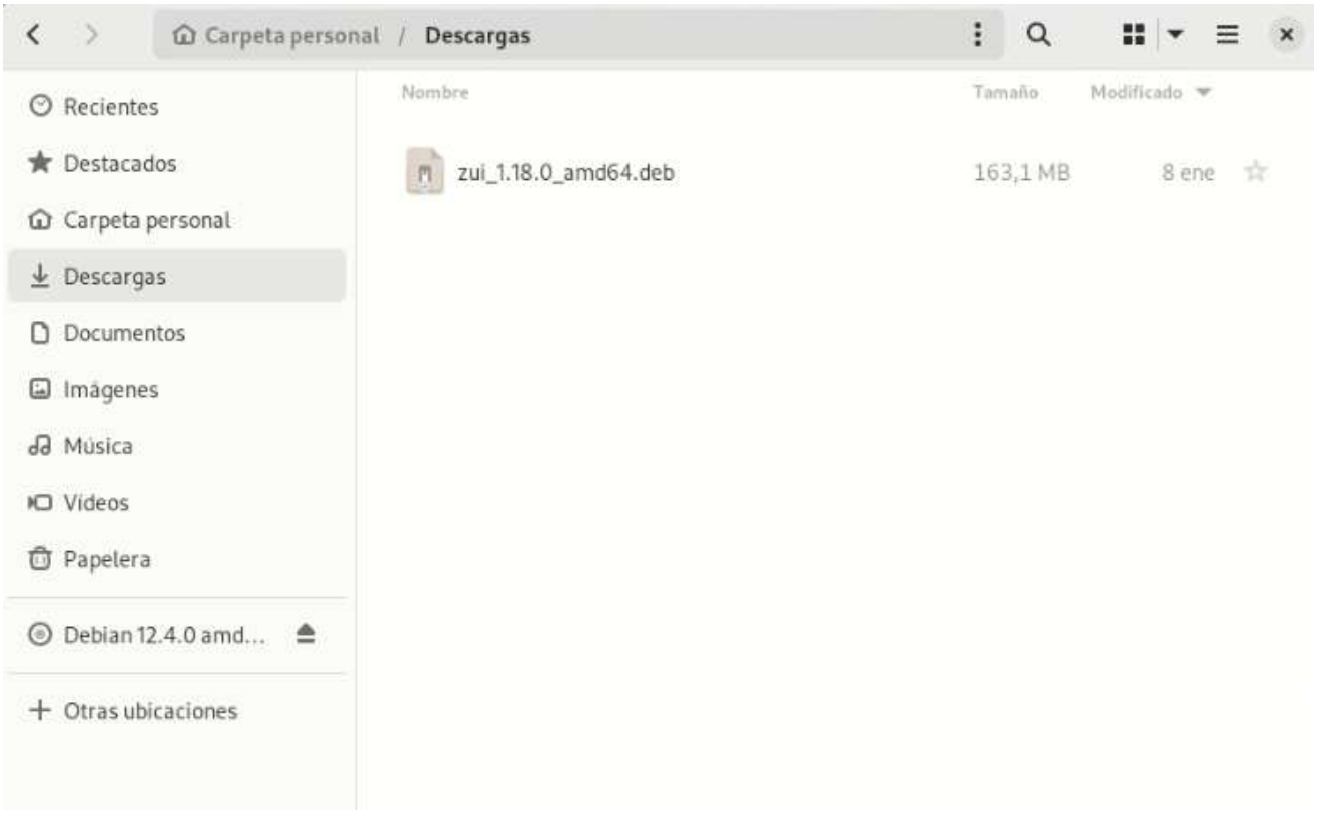


Figura 37 Carpeta Descargas. Fuente: Máquina Virtual SC (s.f))

Una vez que ya procedemos con la descarga del archivo .deb de Zui procedemos con la instalación. Para la instalación vamos a entrar en la carpeta de descargas como se muestra en la figura 38 y utilizar el comando "sudo dpkg -i zui_1.18.0_amd64.deb" para poder instalar la herramienta.

Figura 38 Comando para instalar la herramienta Zui. Fuente: Máquina Virtual SC (s.f)

Si se encuentra errores en la instalación de Zui, se puede resolver utilizando el comando “sudo apt-get install -f” como se muestra en la figura 39.

Figura 39 Comando para corregir errores durante la instalación. Fuente: Máquina Virtual SC (s.f)

Una vez ya instalado la herramienta, desde una nueva terminal vamos a ingresar el comando “zui” como se muestra en la figura 40 y así poder ingresar al menú de Zui.

Figura 40 Comando para ingresar a la herramienta Zui. Fuente: Máquina Virtual SC (s.f)

Una vez ya ejecutamos el comando “zui”, se va a poder visualizar el GUI de la herramienta Zui donde vamos a poder importar los archivos eve.json generados por suricata y así, posteriormente, visualizar y analizar los datos del tráfico de manera estructurada. En la figura 41 se puede visualizar el GUI de la herramienta.

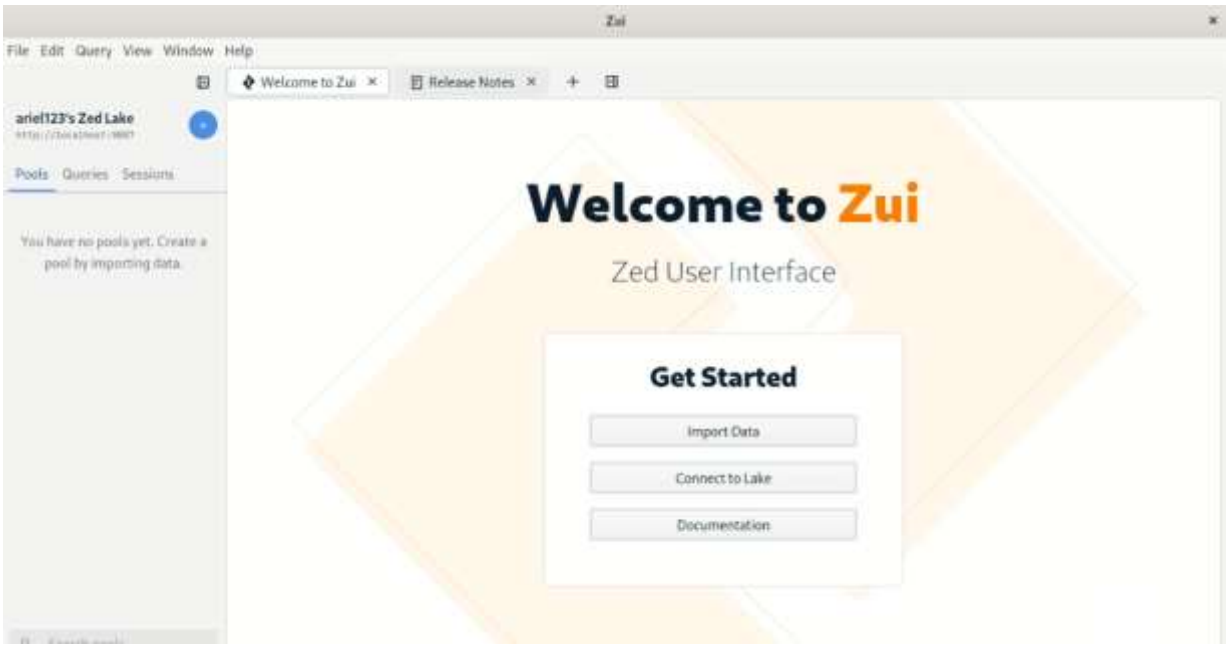


Figura 41 GUI de la herramienta Zui. Fuente: Máquina Virtual SC (s.f)

Se puede verificar que la herramienta Zui fue instalada correctamente. Seguido de la instalación, ahora se va a poder importar los archivos eve.json que genera suricata para posteriormente realizar su respectivo análisis.

4.5VALIDACIÓN DE RESULTADOS

Una vez ya finalizado y dado seguimiento de manera correcta a los pasos para la instalación de la herramienta Zui, se pudo verificar y validar la instalación. Con ello, se procede a ingresar los archivos eve.json para poder visualizar los archivos y realizar consultas.

4.5.1 VISUALIZACIÓN Y CONSULTAS EN ZUI

Primero, se debe ingresar a la GUI de la herramienta Zui, para ello, al igual como se muestra en la figura 40, debemos ingresar el comando “zui” en una terminal y de esa manera podemos ingresar al GUI de Zui. En la figura 41 se puede observar el GUI de la herramienta Zui en donde se va a importar los archivos eve.json. Una vez que ingresamos al GUI, debemos dar clic en “Import Data” como se muestra en la figura 42.

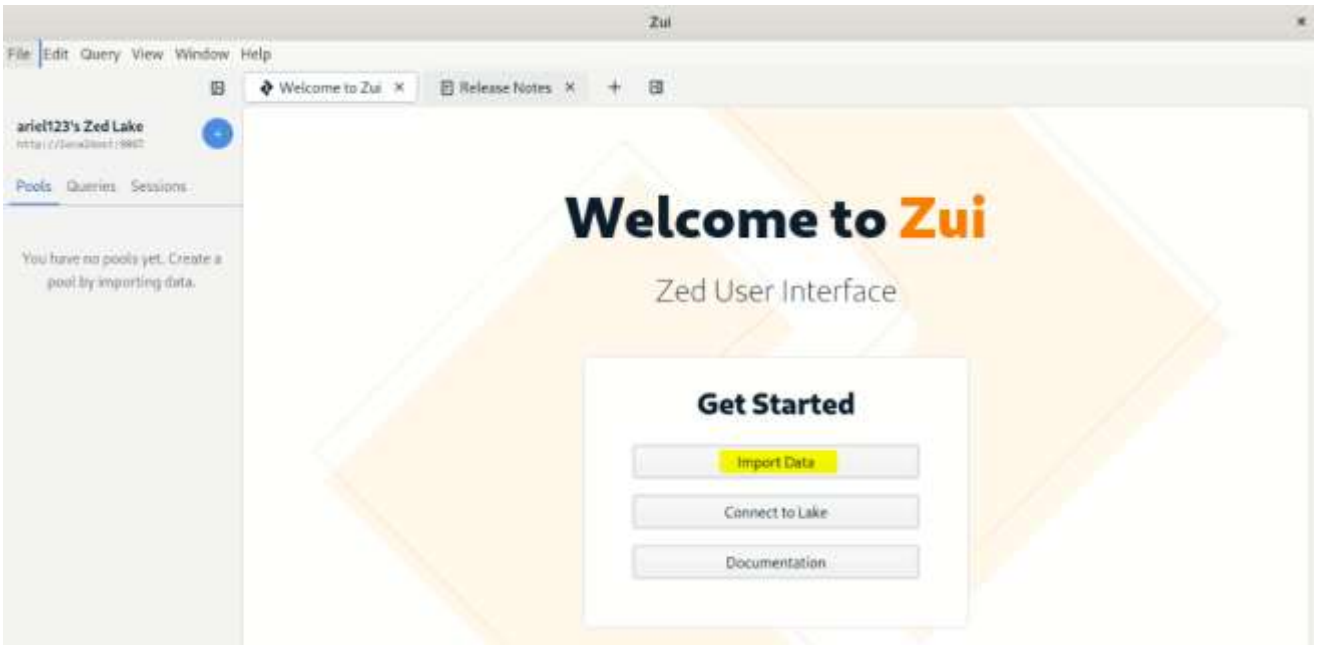


Figura 42 Selección de la opción "Import Data". Fuente: Máquina Virtual SC (s.f)

Una vez que seleccionamos la opción "Import Data", nos aparecerá en pantalla la carpeta de archivos, por lo que debemos buscar el directorio /var/log/suricata como se muestra en la figura 43. En este directorio como ya se había mencionado anteriormente, es donde se guardan los archivos eve.json que vamos a importar en Zui para realizar el análisis.

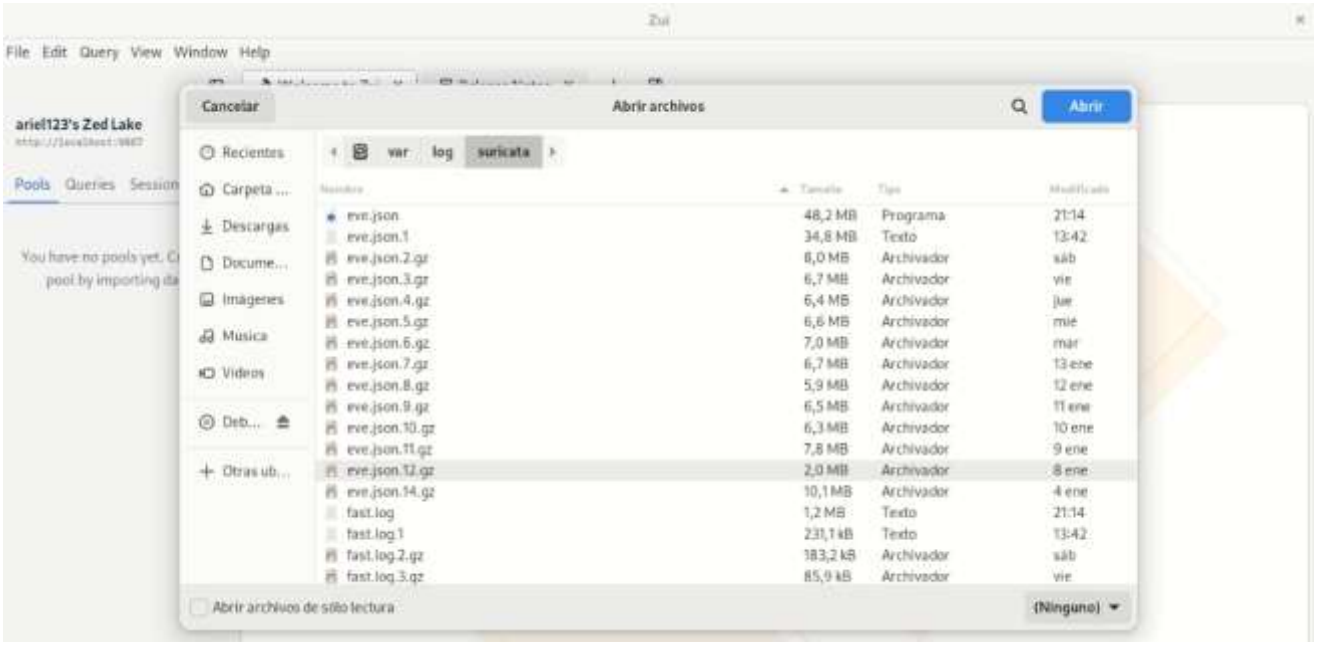


Figura 43 Selección de archivos en el directorio /var/log/suricata. Fuente: Máquina Virtual SC (s.f)

Como se puede ver en la figura 43, podemos escoger cualquier archivo que queramos visualizar y analizar en la herramienta. En este caso vamos a escoger el archivo más antiguo, que va a ser eve.json.14.gz. En la figura 44 se puede observar el resultado una vez que se escoge el archivo que deseemos analizar.

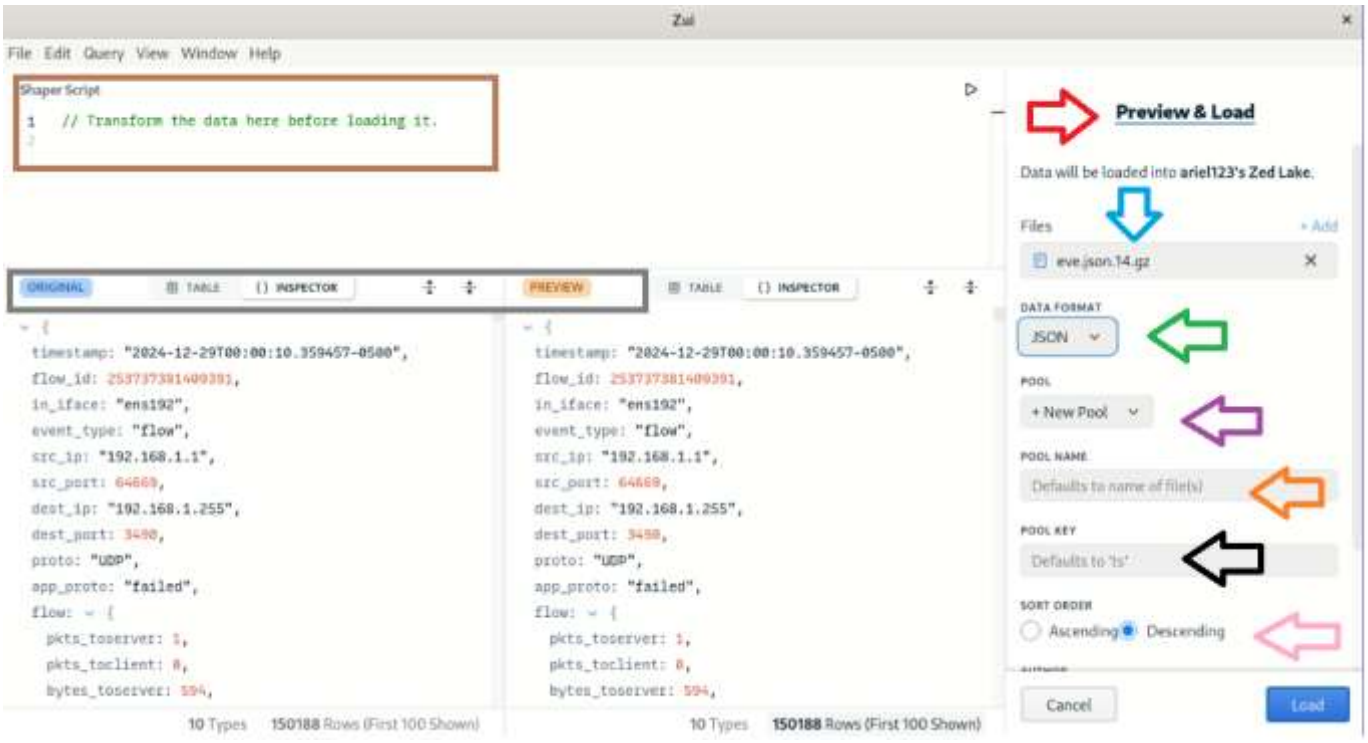


Figura 44 Sección de archivos de log Preview & Load. Fuente: Máquina Virtual SC (s.f)

Como se puede observar en la figura 44, tenemos el resultado una vez que se importa un archivo eve.json que se desee analizar. Para una mejor explicación, se han puesto figuras de colores que pueden guiar para una mejor comprensión del entorno.

- La flecha roja indica que estamos en el menú de Preview & Load. En este menú vamos a poder cargar los datos, generar consultas y además crear un “pool” o el conjunto de datos en donde se van a cargar los datos del archivo. para luego poder visualizar la información.
- En el rectángulo color marrón, es el espacio donde se puede realizar consultas y filtrar información. Se puede filtrar información de tipo de alerta, protocolo, dirección IP, etc.
- En el rectángulo color gris, se pueden visualizar dos resultados, al lado izquierdo en la sección donde dice “Original” es el espacio donde se muestra originalmente el resultado una vez que se carga archivo, en este caso el archivo eve.json.14.gz. En el lado derecho, en la sección donde dice “Preview”, se

muestra el resultado una vez que se realice una consulta en la sección de consultas.

- La flecha color celeste indica el archivo que cargamos, en este caso es el archivo eve.json.14.gz.
- La flecha color verde indica el tipo de formato del archivo. Normalmente viene con la opción “Auto-Detect”, sin embargo, debemos cambiar y asegurarnos de que este puesto con la opción JSON para que no existan errores en la carga y consulta del archivo.
- La flecha color morado indica el pool. Se puede crear un nuevo pool seleccionando la opción “ + New Pool” o usar uno existente.
- La flecha color naranja indica el nombre del pool donde se almacenarán los datos. Por defecto, va a tomar el nombre del archivo, en este caso eve.json.14.gz pero se puede personalizar.
- La flecha negra define la calve principal para indexar los datos dentro del pool. Por defecto, utiliza la clave “ts” (timestamp) el cual organiza los datos cronológicamente, pero se puede cambiar dependiendo de la estructura de datos que se requiera.
- La flecha rosa permite elegir en la manera que se van a ordenar los datos en el pool. Puede ser de manera ascendente o descendente.

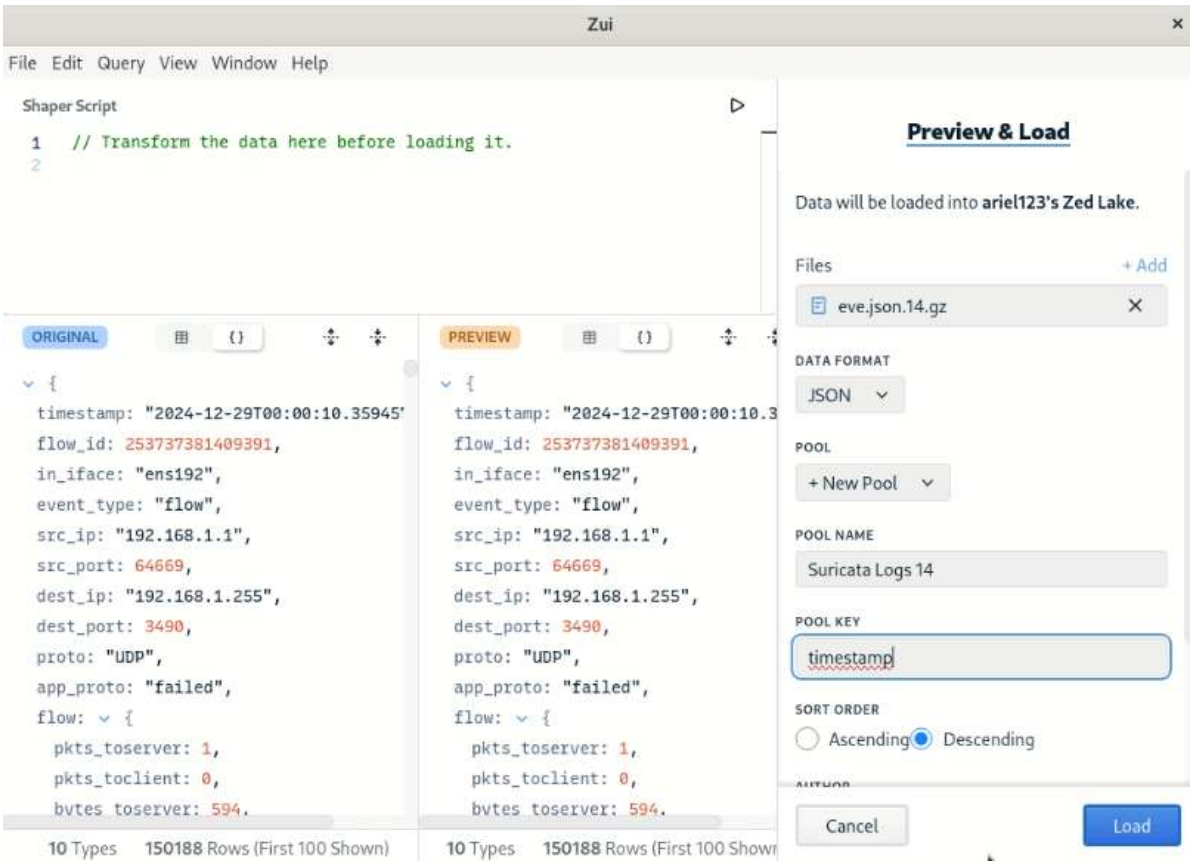


Figura 45 Configuración del pool para cargar el archivo en Preview & Load. Fuente: Máquina Virtual SC (s.f)

En la figura 45 ya asignamos los parámetros para poder crear nuestro pool. Cambiamos el formato predeterminado por JSON para evitar errores en la lectura de información, en la sección de pool se permanece la opción " + New Pool", el nombre que le asignamos es Suricata Logs 14 y en la sección de Pool Key escribimos timestamp para poder indexar los datos el cual los organiza cronológicamente. Una vez finalizado la configuración, damos clic en "Load".

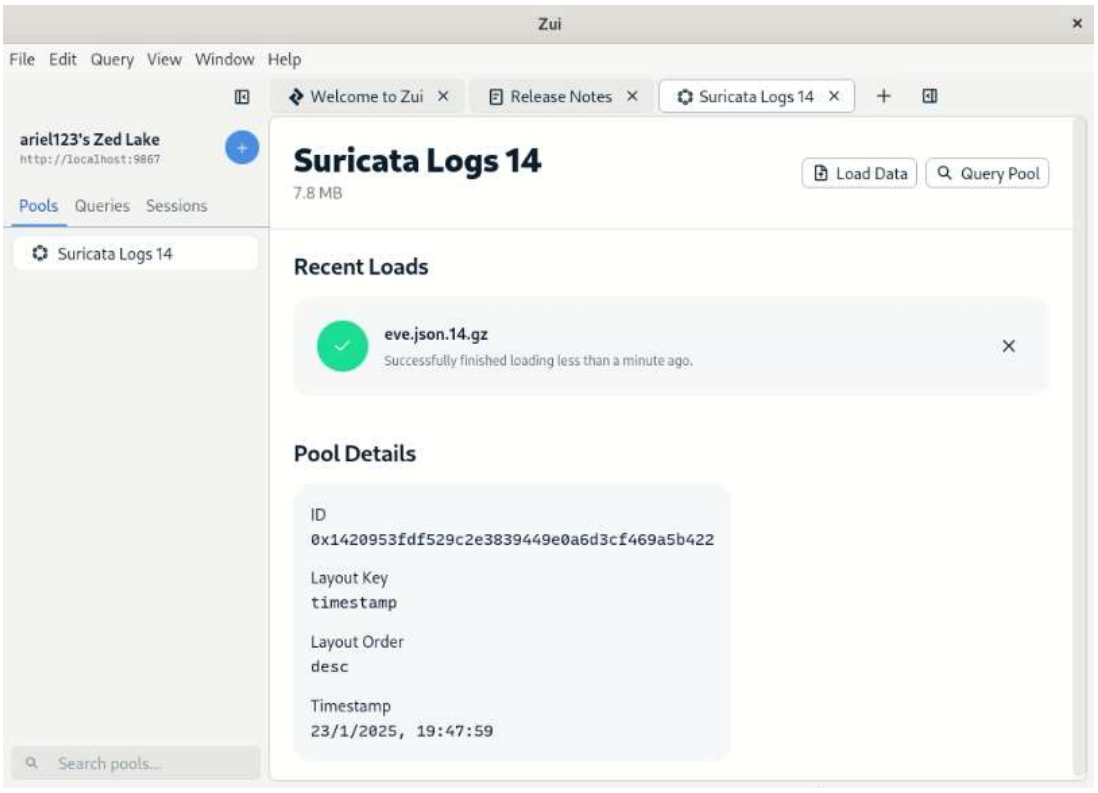


Figura 46 Pool configurado de Suricata. Fuente: Máquina Virtual SC (s.f)

Una vez ya terminado de configurar nuestro pool como se muestra en la figura 46, podemos verificar el nombre de nuestro pool, la fecha de creación y el ID. Además, ya podemos acceder a los datos y poder realizar consultas en el botón derecho al lado superior "Query Pool". Además, se pueden cargar otros archivos dentro del mismo pool en la sección "Load Data".

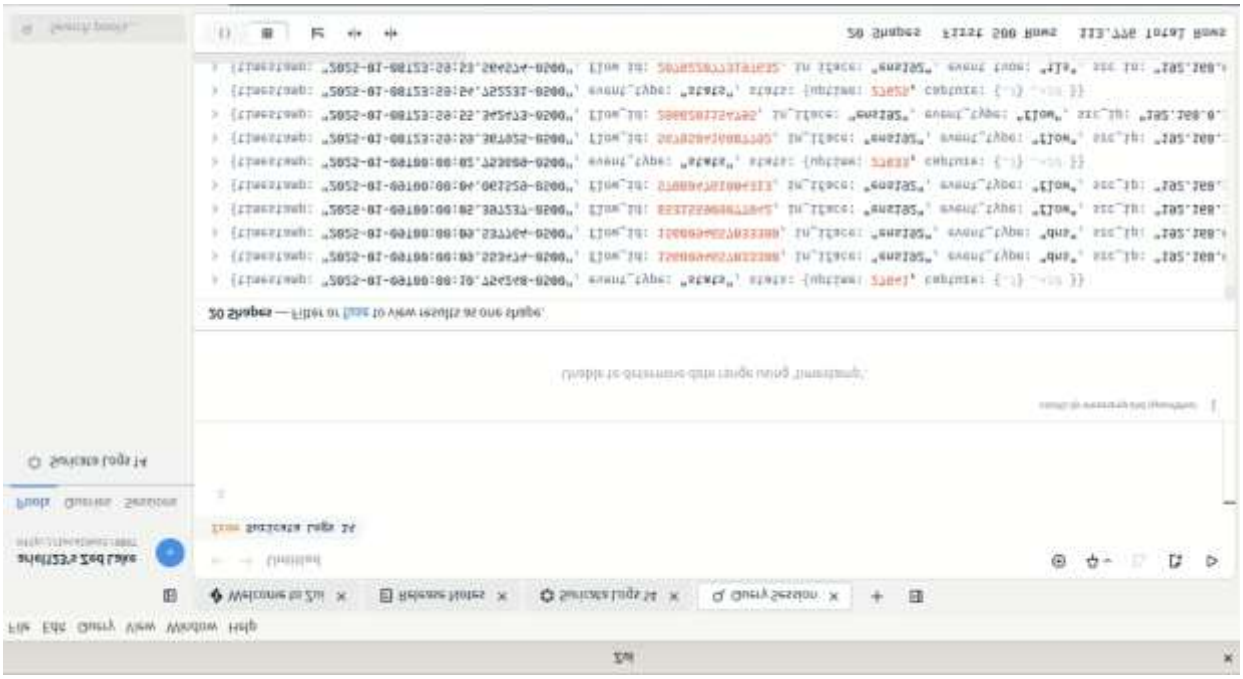


Figura 47 Muestra de consultas dentro del pool. Fuente: Máquina Virtual SC (s.f)

Finalmente, como se puede mostrar en la figura 47, una vez que cargamos los archivos, se pueden realizar consultas. Tenemos la línea de comandos en el espacio en blanco y en la parte inferior tenemos el resultado. Al momento se muestran los resultados sin realizar ninguna consulta, sin embargo, se pueden realizar consultas para filtrar información ya se por tipo de evento, IP origen, alerta, etc.

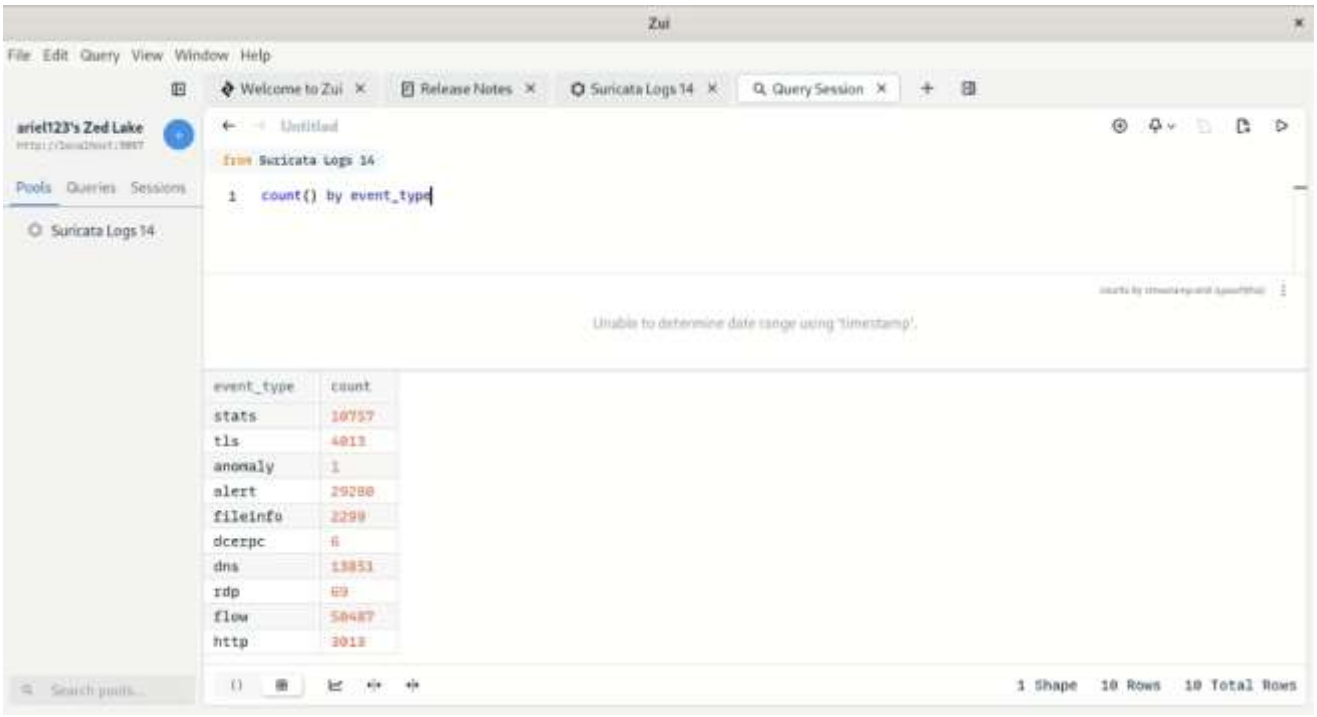


Figura 48 Consulta por tipo de evento. Fuente: Máquina Virtual SC (s.f)

Como se puede ver en la figura 48, se realizó una consulta por tipo de evento, por lo que el resultado nos va a dar los eventos que se han detectado junto al conteo. En la imagen se puede ver algunos eventos como http, Flow, alerta, etc. Con esta información se puede hacer más detallado el análisis.

CAPÍTULO V: RESULTADOS

5.1 CARGA DE DATOS EN ZUI

Dentro de este capítulo del presente trabajo de titulación, se van a visualizar los resultados y, además, se va a realizar un análisis de los mismos para poder entrar en profundidad los archivos generados diariamente por la herramienta Suricata.

Para comenzar, como se puede visualizar en la figura 49, tenemos los archivos eve.json generados por Suricata. Estos archivos contienen los datos de la captura del tráfico que realizó la herramienta diariamente. Para la visualización de datos, vamos a cargar en la herramienta Zui los archivos generados que tengan los nombres desde eve.json.13.gz hasta eve.json.7.gz.

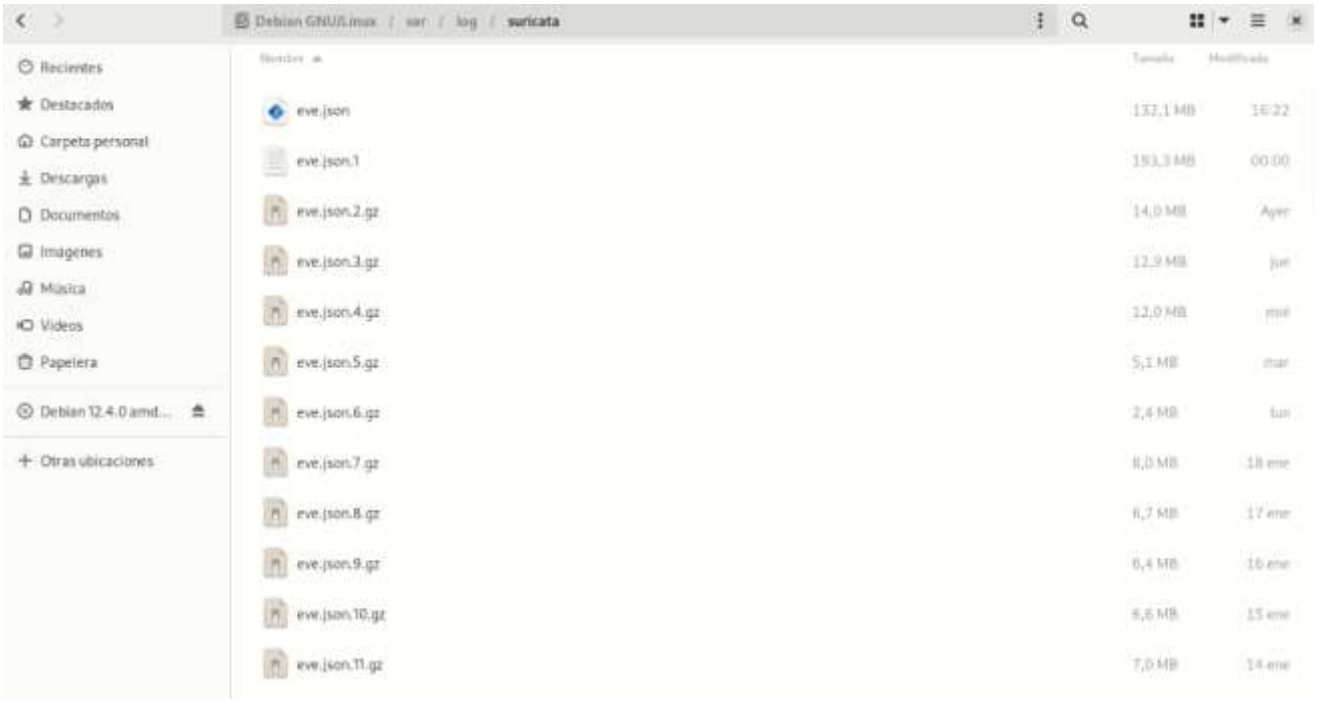


Figura 49 Muestra de archivos eve.json. Fuente: Máquina Virtual SC (s.f)

Como se puede ver en la figura 50, cargamos los archivos eve.json que tengan el nombre desde eve.json.13.gz hasta eve.json.7.gz ordenados de forma descendente y asignamos estos archivos nuestro nuevo pool de datos llamado “Logs Suricata”. Una vez cargados, damos clic en “Load”

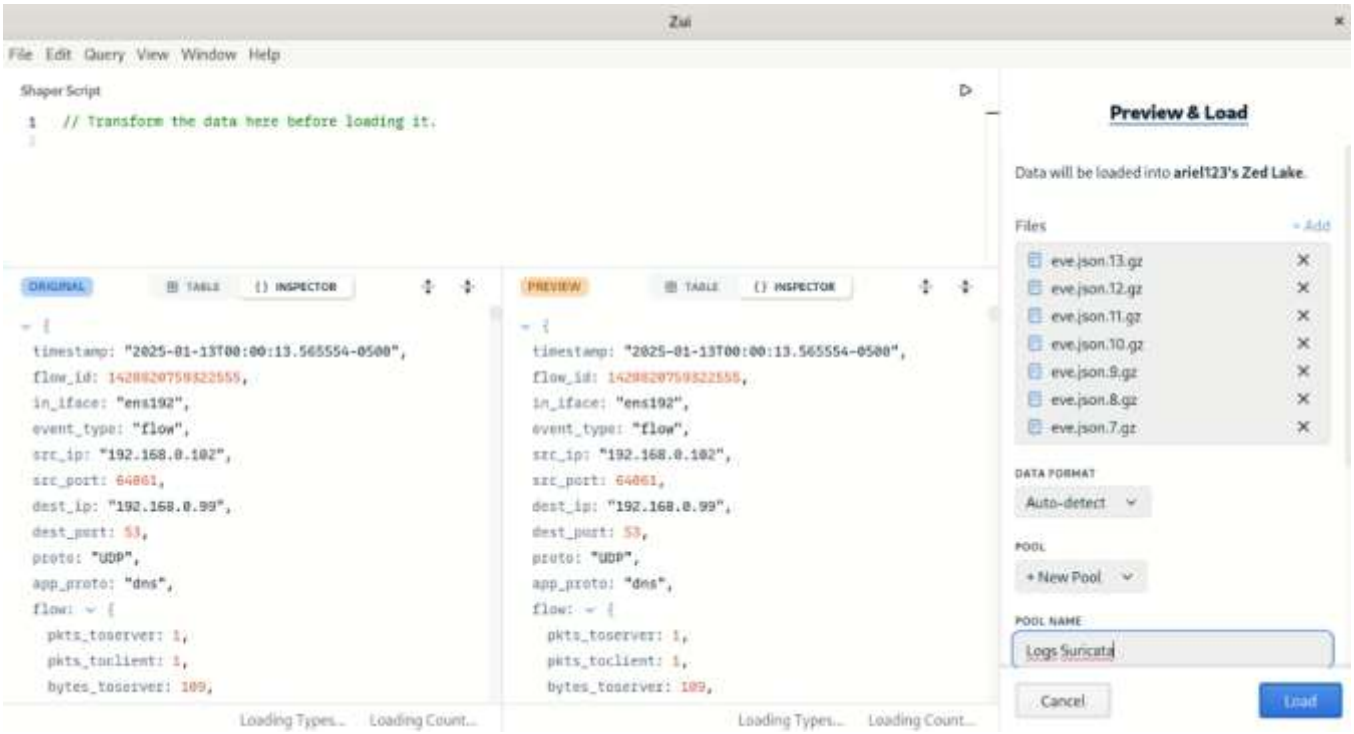


Figura 50 Carga de archivos a un nuevo pool "Logs Suricata". Fuente: Máquina Virtual SC (s.f)

En la figura 51 se puede visualizar que ya se cargó el pool de datos con el nombre de "Logs Suricata". Además, se puede ver que están cargados todos los archivos que deseemos visualizar y analizar, por lo que damos en el botón "Query Pool" para así realizar nuestras consultas.

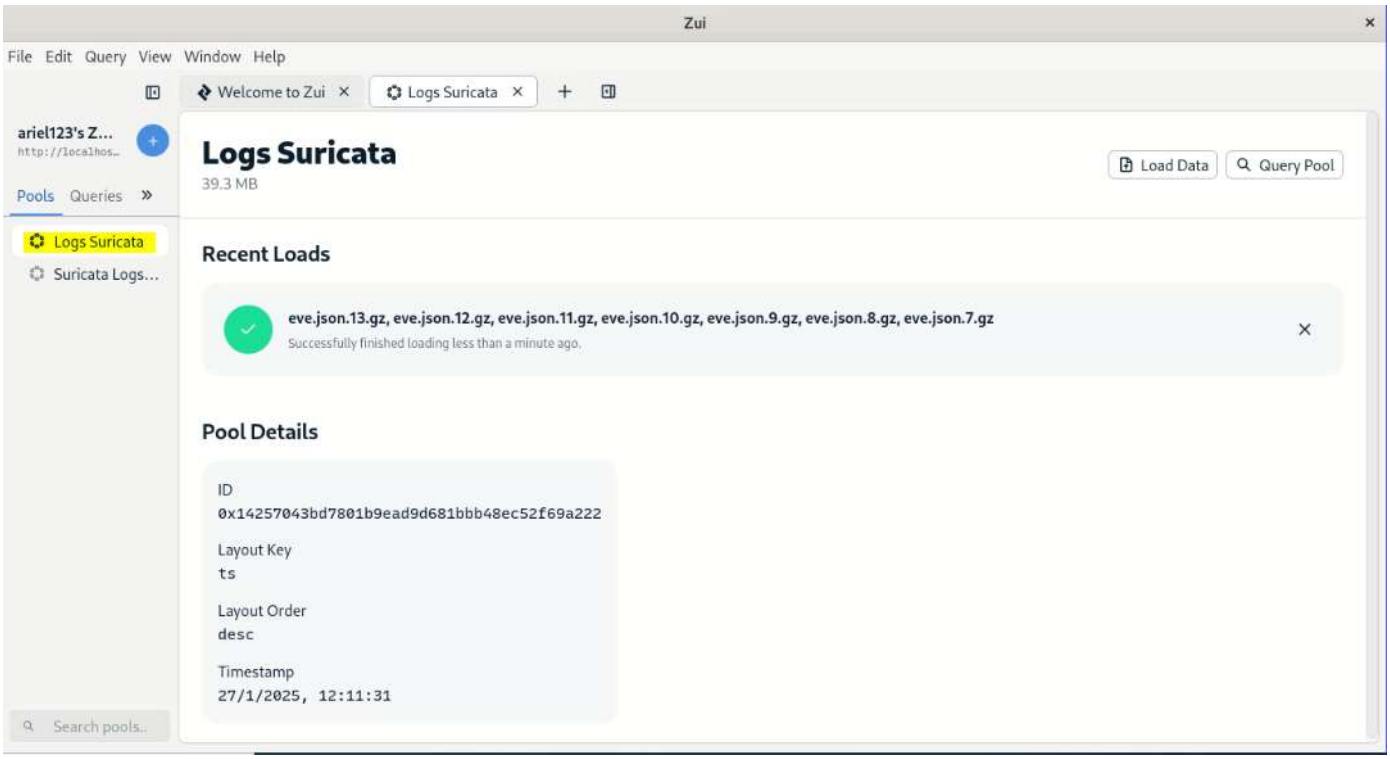


Figura 51 Carga de archivos a un nuevo pool "Logs Suricata". Fuente: Máquina Virtual SC (s.f)

Como se puede ver en la figura 52, una vez que cargamos nuestros archivos eve.json, tenemos en pantalla todos los datos listos para poder realizar consultas y poder realizar el análisis de los datos.

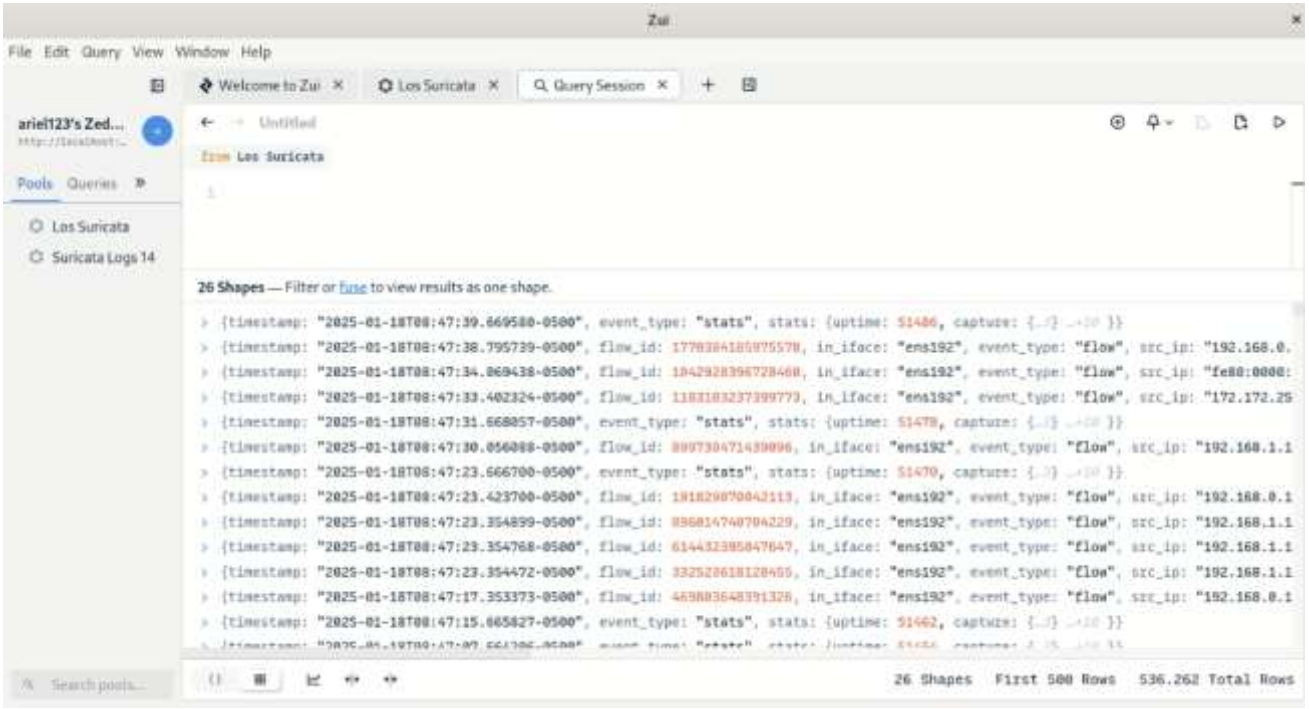


Figura 52 Datos listos para realizar consulta. Fuente: Máquina Virtual SC (s.f)

Una vez ya cargados los datos, se procede a realizar las diferentes consultas que nos permite hacer la herramienta Zui. El lenguaje que utiliza es tipo "Zed Query Language". Es un lenguaje similar a SQL diseñado para trabajar con datos estructurados, semiestructurados y no estructurados con capacidades más extendidas para manejar datos más complejos.

5.2 MUESTRA DE CONSULTAS REALIZADAS EN ZUI

Zui es una herramienta con múltiples capacidades para realizar consultas en lenguaje tipo Zed. A continuación, se van a realizar consultas para filtrar los datos por tipo de evento, filtrar por IP origen y destino, contar eventos por tipo asignado, agrupar eventos, por ejemplo, agrupar eventos de tipo alerta y asociar con su IP origen y destino, y buscar patrones específicos. Además, se van a demostrar algunas funciones adicionales que tiene la herramienta como el uso de "Fuse" para combinar resultados.

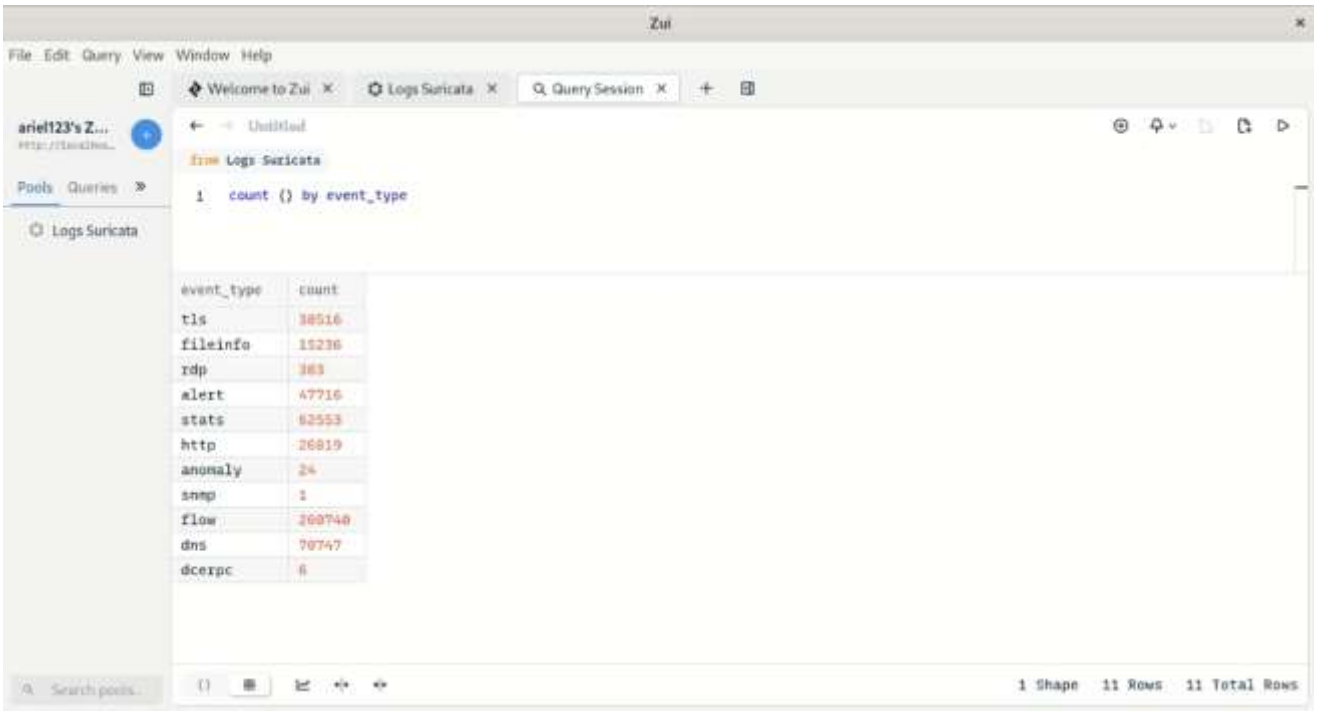


Figura 53 Búsqueda por tipo de eventos. Fuente: Máquina Virtual SC (s.f)

Para comenzar, como se puede visualizar en la figura 53, se va a empezar a contar los tipos de eventos que se encontraron en los archivos eve.json. A continuación, se va a realizar una explicación de cada evento:

- Anomaly: Los eventos de tipo “anomaly” se generan cuando suricata detecta anomalías en el tráfico de red.
- Fileinfo: Los eventos tipo “fileinfo” son generados cuando contienen información sobre archivos detectados en el tráfico de red.
- Alert: Los eventos tipo “alert” son eventos generados cuando suricata identifica actividades sospechosas o maliciosas basadas en reglas predefinidas cómo las reglas actualizadas de Emerging Threats.
- Rdp: Estos eventos están relacionados con el protocolo Remote Desktop Protocol (RDP) el cual suricata genera eventos de conexiones RDP.
- Flow: Los eventos de tipo “flow” están relacionados a flujos de conexión entre dos puntos finales o de hosts. Incluye información sobre IP origen, destino, protocolo (TCP/UDP), duración de flujo y cantidad de datos transferidos.

- Http: Estos eventos contienen información sobre tráfico http que genera suricata.
- Dns: Los eventos tipo “dns” se generan cuando registran consultas y respuestas DNS que se observan en la red.
- Tls: Los eventos “tls” recopilan información sobre conexiones TLS/SSL.
- Snmp: Los eventos “snmp” están relacionados con el tráfico del protocolo Simple Network Management Protocol.
- Dcerpc: Los eventos de tipo “dcerpc” están relacionados con el protocolo Distributed Computing Environment / Remote Produce Calls. Este protocolo es utilizado en sistemas Windows para comunicación entre servidores.
- Stats: Los eventos “stats” contienen estadísticas generales sobre el rendimiento y además el funcionamiento de Suricata.

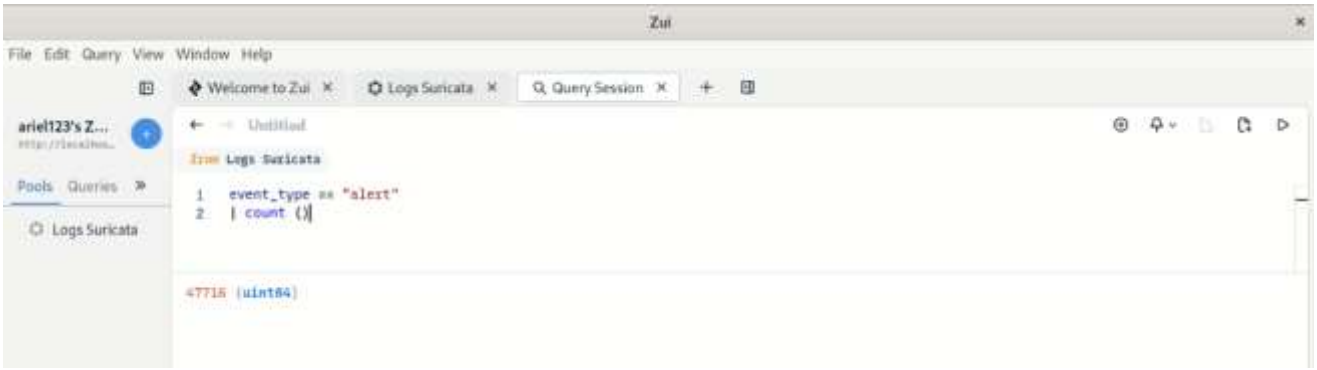


Figura 54 Búsqueda de eventos tipo “alert”. Fuente: Máquina Virtual SC (s.f)

Luego de ver el número de eventos capturados según su tipo, nos vamos a concentrar específicamente en los eventos que sean de tipo “alert”. En la figura 54 se pueden visualizar la consulta que se realiza para contar número de eventos de tipo “alert” que se encontraron en todos los datos capturados. En total se encontraron 47716 alertas como muestra la figura.

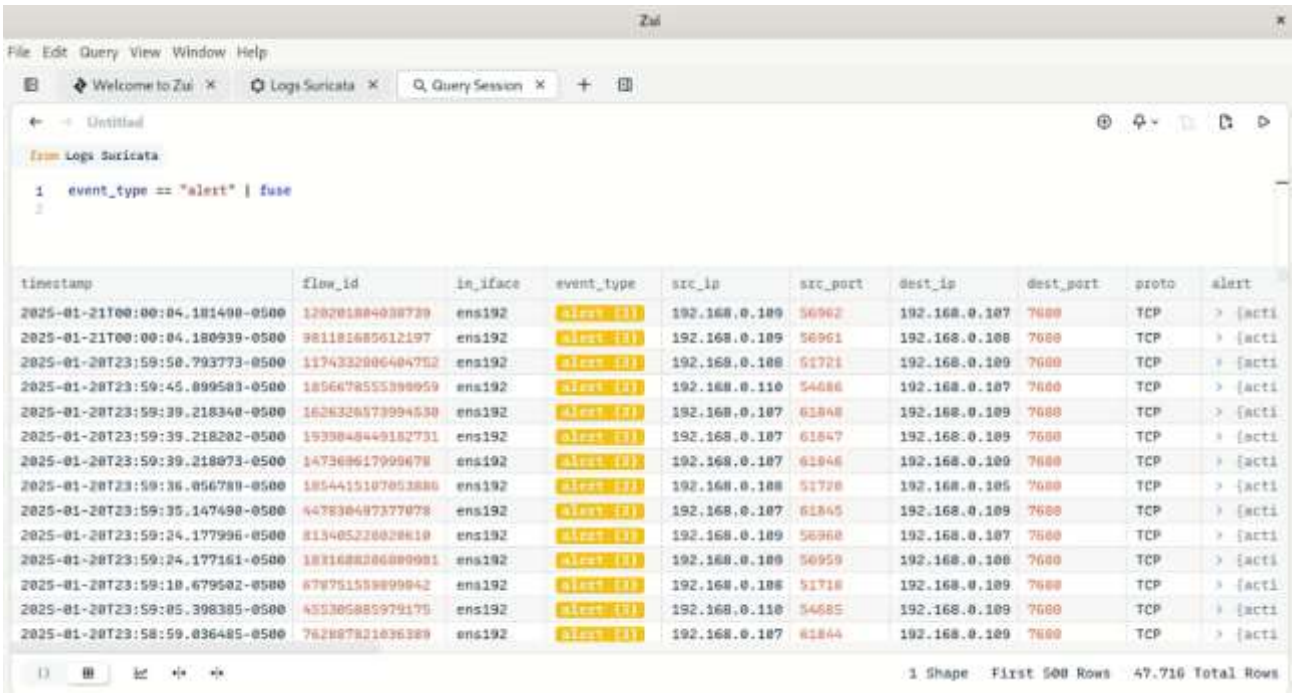


Figura 55 Uso de la función "Fuse". Fuente: Máquina Virtual SC (s.f)

Como se puede visualizar en la figura 55, se puede utilizar la función "Fuse" que permite combinar los resultados y mostrar de manera de tabla para realizar un análisis más detallado. También se pueden observar que el número de filas es el mismo número de los eventos de tipo "alert" en este caso 51688. Además, se puede ver la severidad que en este caso es tipo 3 y de color amarrillo, quiere decir, que la severidad es de media.

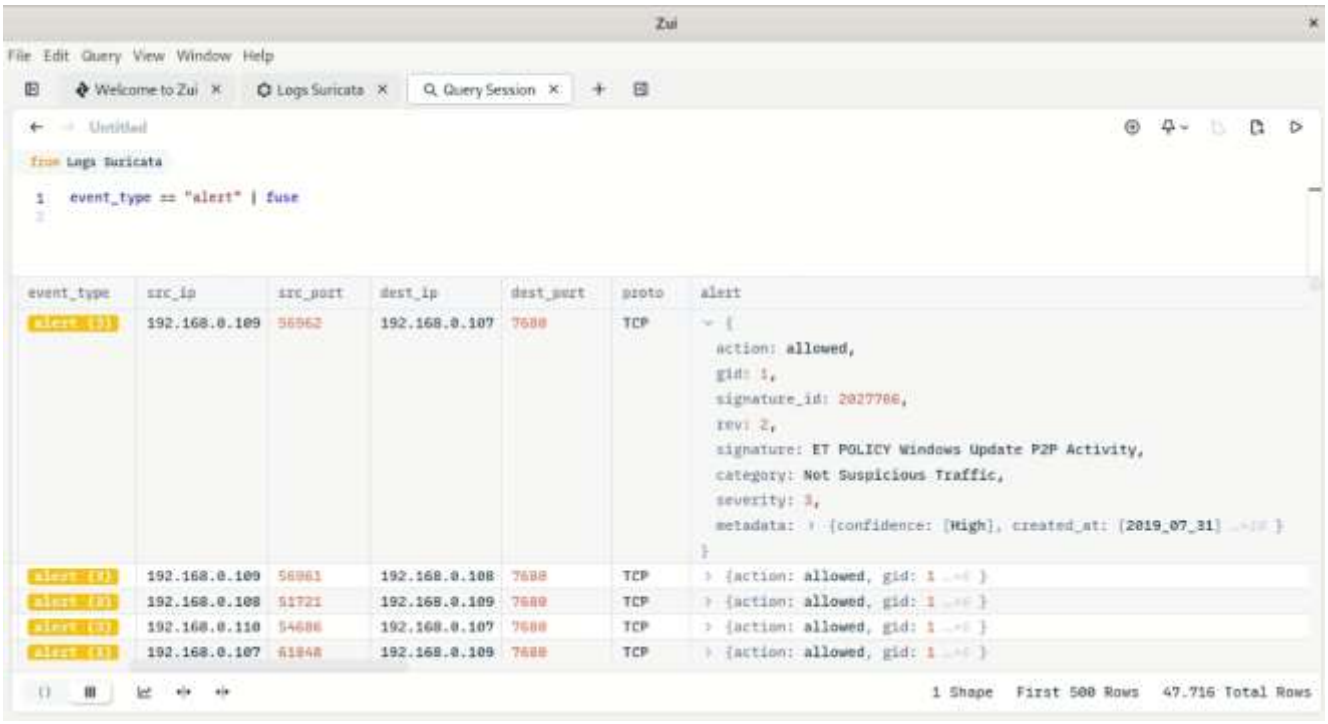


Figura 56 Despliegue de la cabecera alert. Fuente: Máquina Virtual SC (s.f)

Como se puede ver en la figura 56, de uno de los logs registrados con un evento de tipo alerta, se puede desplegar para poder verificar más información. Se puede visualizar que el tráfico fue permitido, la categoría detecta no tráfico sospechoso y la severidad es de tipo 3, es decir severidad media que no requiere investigación profunda.

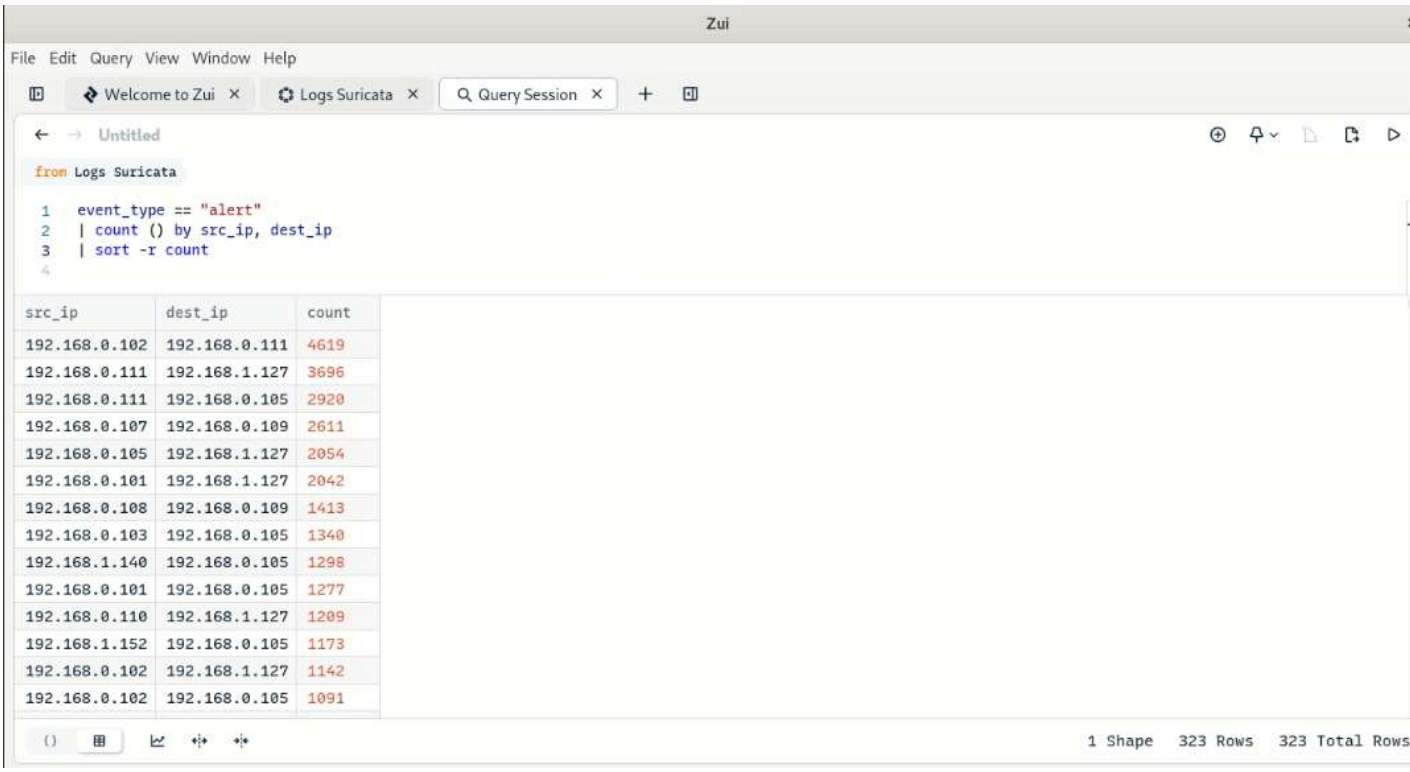


Figura 57 Consulta por tipo de IP origen. Fuente: Máquina Virtual SC (s.f)

Como se puede visualizar en la figura 57, se realizó una consulta que permite saber cuál es la IP origen con el mayor número de eventos tipo “alert” y al mismo tiempo la IP destino asociado con el mayor número de eventos tipo “alert”. En este caso, se muestra que el mayor número de eventos tipo alert provienen de la IP origen 192.168.0.102 a la IP destino 192.168.0.111 con 4619 eventos en total.

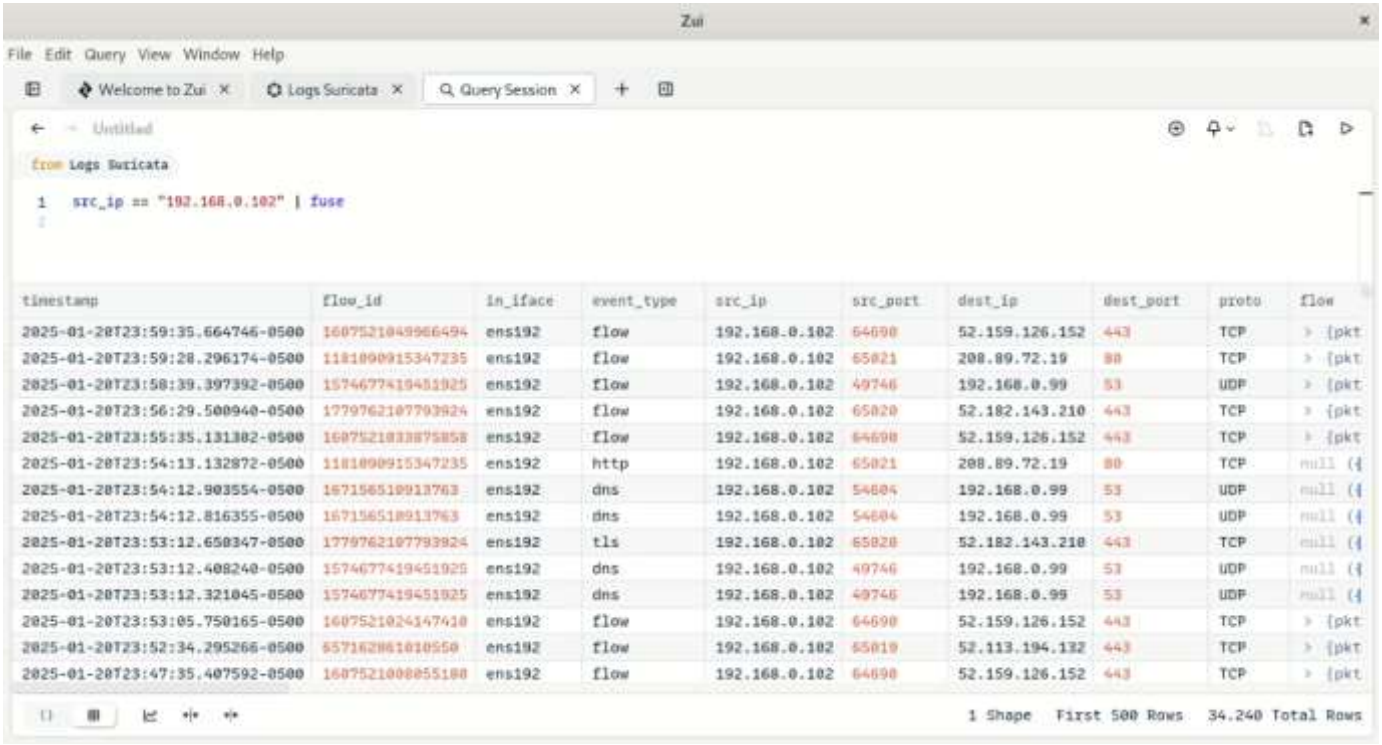


Figura 58 Consulta por IP Origen. Fuente: Máquina Virtual SC (s.f)

En la figura 58 se puede ver que se realizó la consulta para que se muestre por IP origen. En este caso se filtró la IP origen con mayor número de alertas como se mostró en la figura 5 y se puede ver el puerto destino al que se conectó, la IP destino y el protocolo.

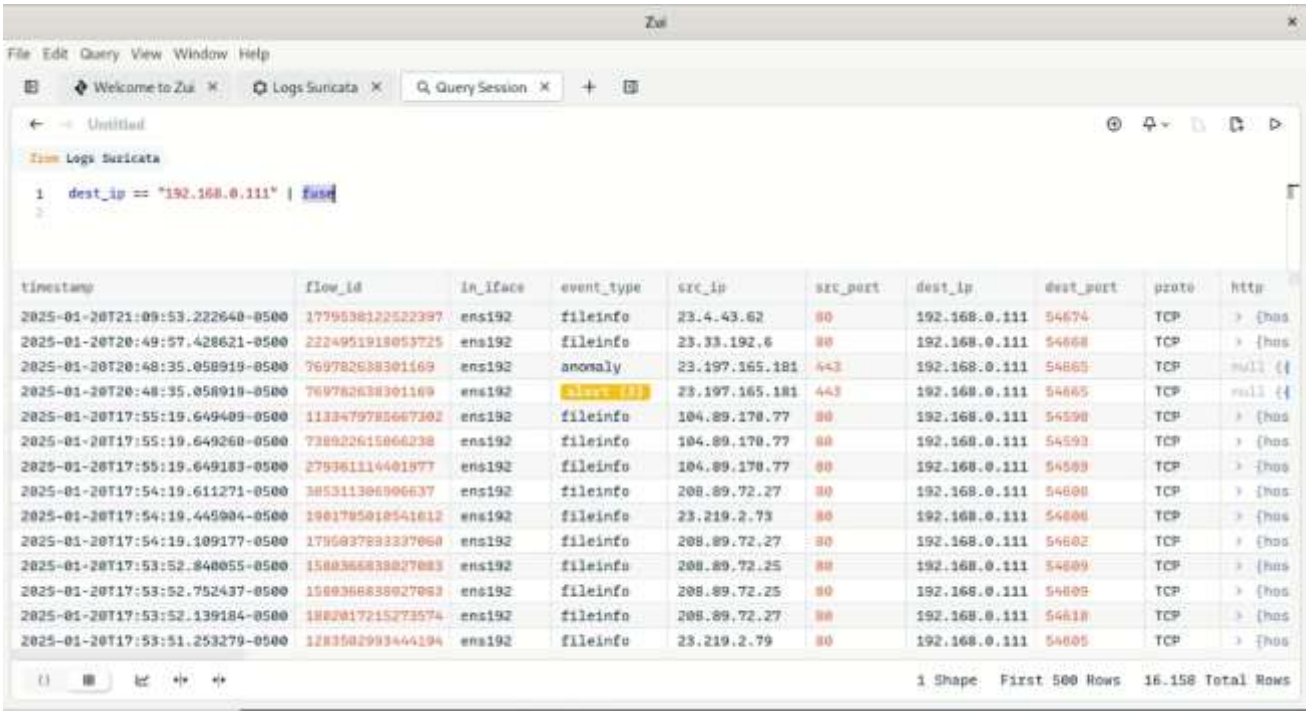


Figura 59 Consulta por IP Destino. Fuente: Máquina Virtual SC (s.f)

En la figura 59, de igual manera como se puede observar, se filtró la búsqueda por la IP destino con mayor número de alertas registradas. En este caso además se puede visualizar el tipo de evento y como se muestra en la figura 59, existe una alerta por lo que se puede realizar un seguimiento desde la IP origen que registra. Además, presenta de igual manera información como protocolo, puerto destino, etc.

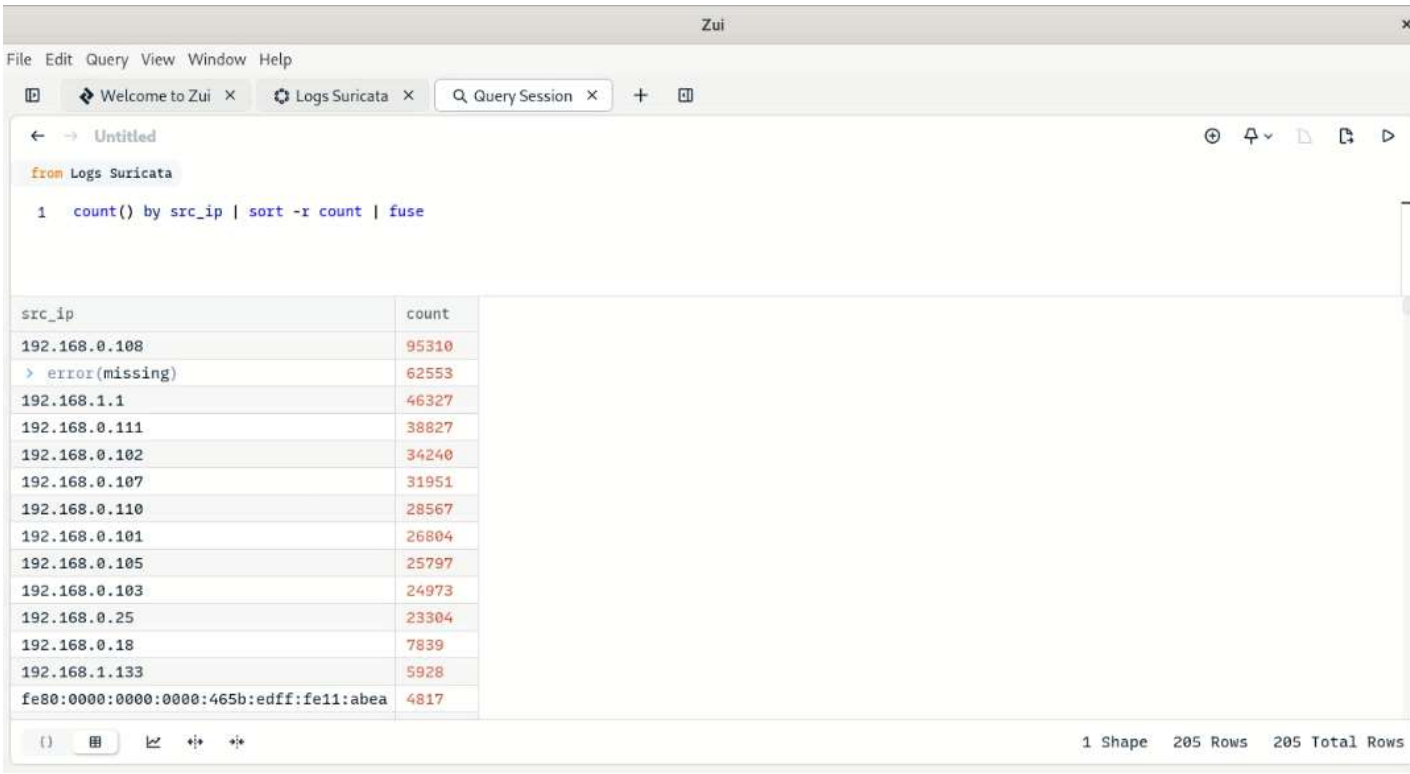


Figura 60 Consulta por IP Origen. Fuente: Máquina Virtual SC (s.f)

Como se puede ver en la figura 60, se realizó una consulta para poder ver en la tabla todas las direcciones IP origen más activas o que generaron más tráfico. Está ordenado de forma ascendente desde la IP que generó más tráfico el cual fue la 192.168.0.108 y así sucesivamente. Esta información nos puede servir para saber que IP origina más tráfico y las conexiones de esa IP.

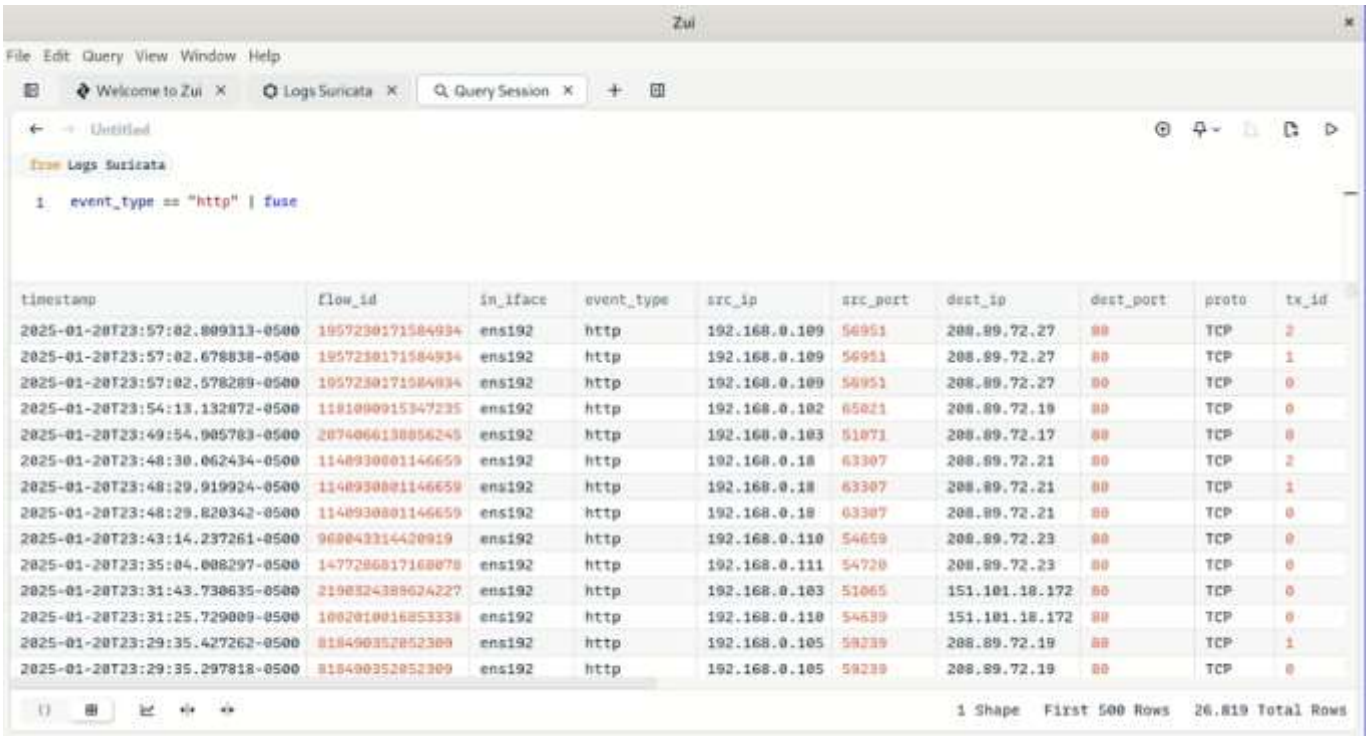


Figura 61 Consulta por tipo de evento "http". Fuente: Máquina Virtual SC (s.f)

En la figura 61, se realizó una consulta para que pueda dar todos los resultados de conexiones de tipo "http". Se decidió realizar esta consulta en la herramienta ya que como se pudo ver en la figura 53, en total se contaron 26819 eventos de tipo http, por lo que una mayoría de eventos registrados se concentraron en el uso de este protocolo.

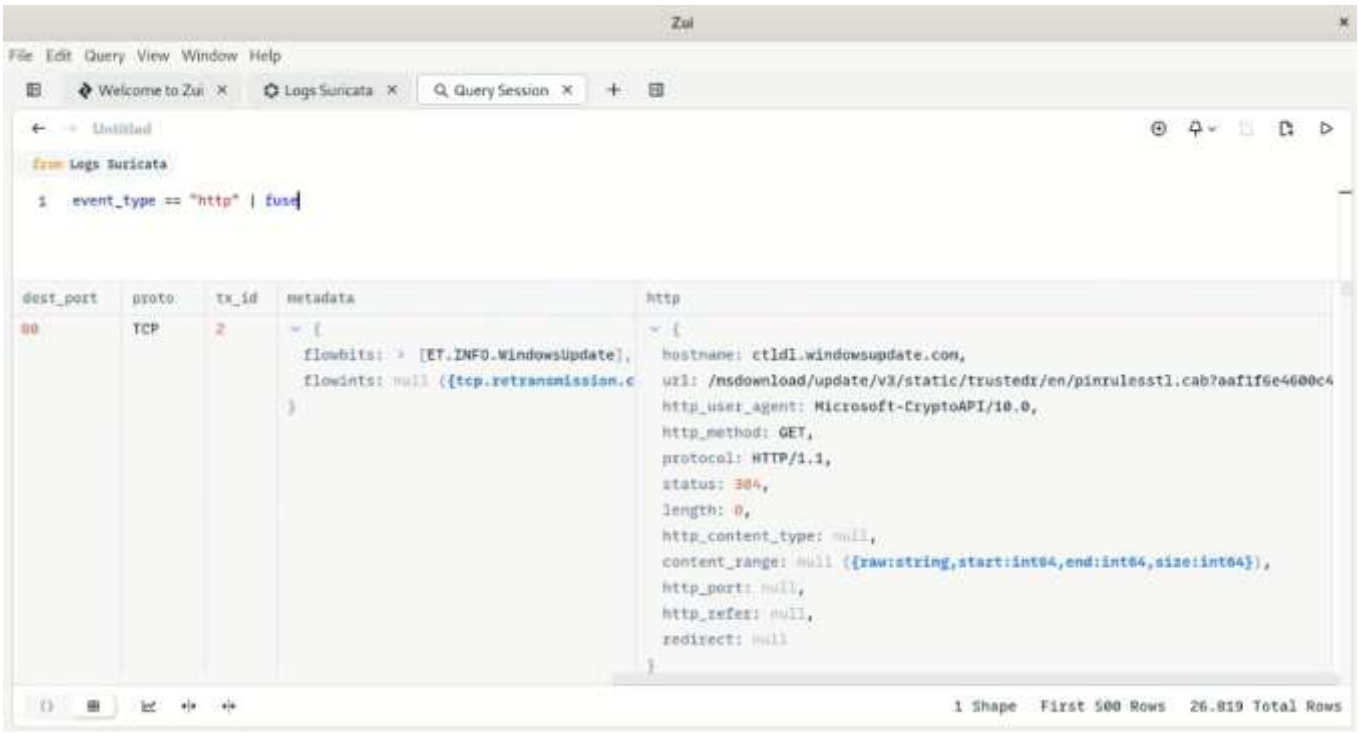


Figura 62 Despliegue de la cabecera http. Fuente: Máquina Virtual SC (s.f)

Como se puede ver en la figura 62, se realizó un despliegue de uno de los logs que se filtró por tipo de evento http. En la cabecera se puede ver la información como el hostname al que se conectó, la URL, el método que realizó, etc. Con esta información al momento de encontrar una alerta crítica que requiera un seguimiento, se puede especificar a profundidad el protocolo con el que se conectó y la información del mismo.

5.3 MUESTRA DE GRÁFICOS CON POWER BI

Además de la herramienta Zui, se pueden utilizar otras herramientas para visualizar los datos capturados por suricata. Gracias a que suricata captura y guarda los registros diariamente con un formato .json, lo hace compatible en su lectura para múltiples herramientas donde se pueda visualizar datos y generar gráficos más específicos.

Power BI es una herramienta completa para poder importar datos. Su flexibilidad para importar archivos con formato .json es ideal para así poder filtrar, generar y visualizar gráficos más específicos sobre datos del tráfico generado.

A continuación, se va a presentar desde la carga de datos en la herramienta Power BI del archivo que se va a cargar, hasta la muestra de los gráficos que se pueden realizar. Para ello, se va a utilizar un archivo eve.json y se va a cargar en la herramienta Power BI.

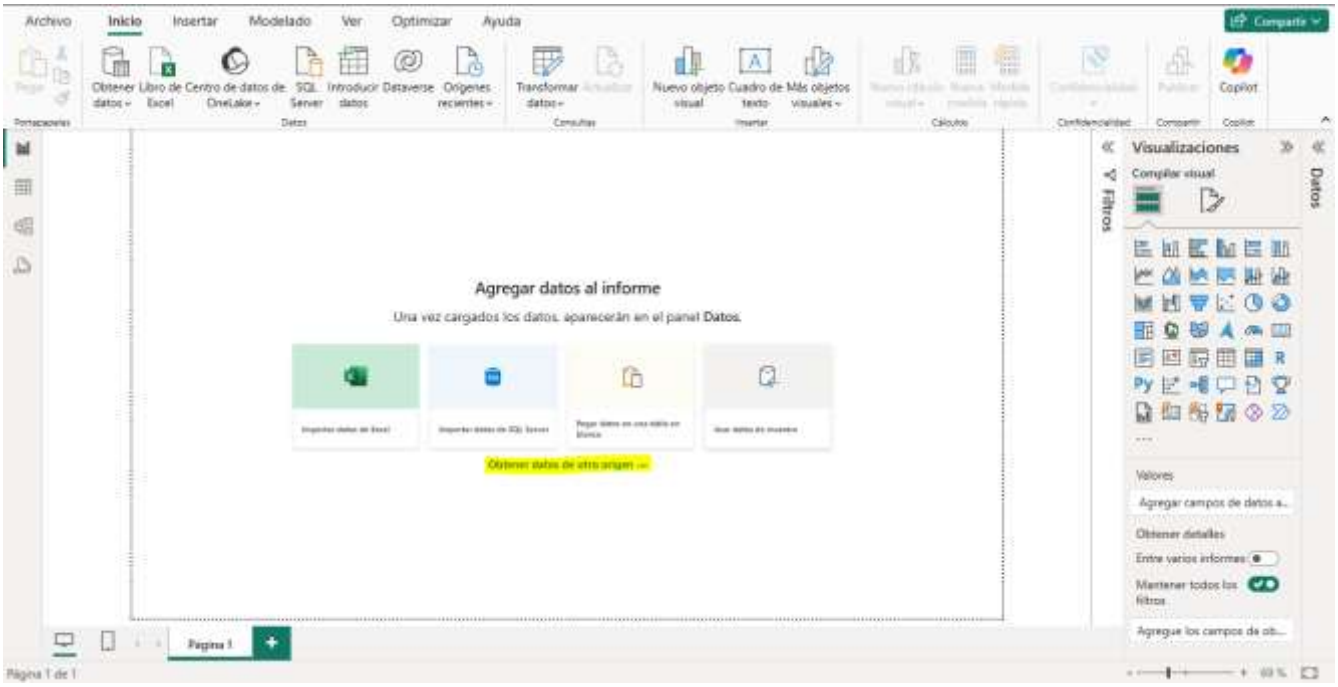


Figura 63 Carga de archivos eve.json en Power BI. Fuente: Power BI (s.f)

Como se puede ver en la figura 63, una vez dentro de la herramienta Power BI, debemos ubicarnos en la sección “Obtener datos de otro origen” y así buscar los archivos eve.json. Debemos tener en cuenta que suricata genera archivos eve.json numerados y comprimidos, por ello, se deben comprimir y verificar que tengan su extensión .json.

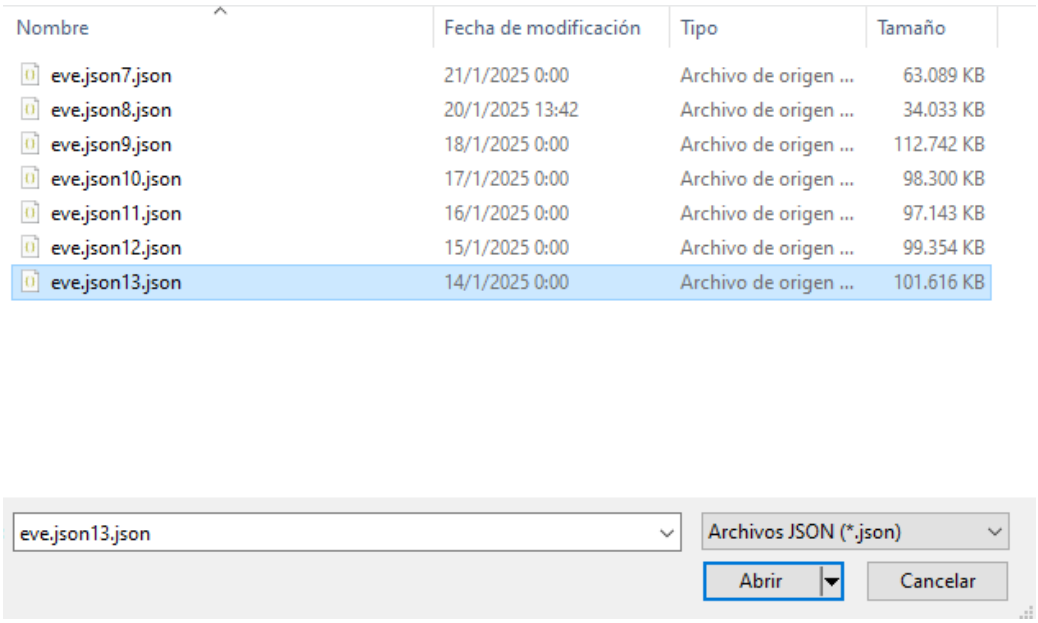


Figura 64 Carga de archivos eve.json13.json Fuente: Administrador de Archivos (s.f)

Ahora bien, se debe ubicar los archivos eve.json que se van a cargar. Para este contexto, se va a utilizar el archivo con el nombre eve.json13.json como se muestra en la figura 64.

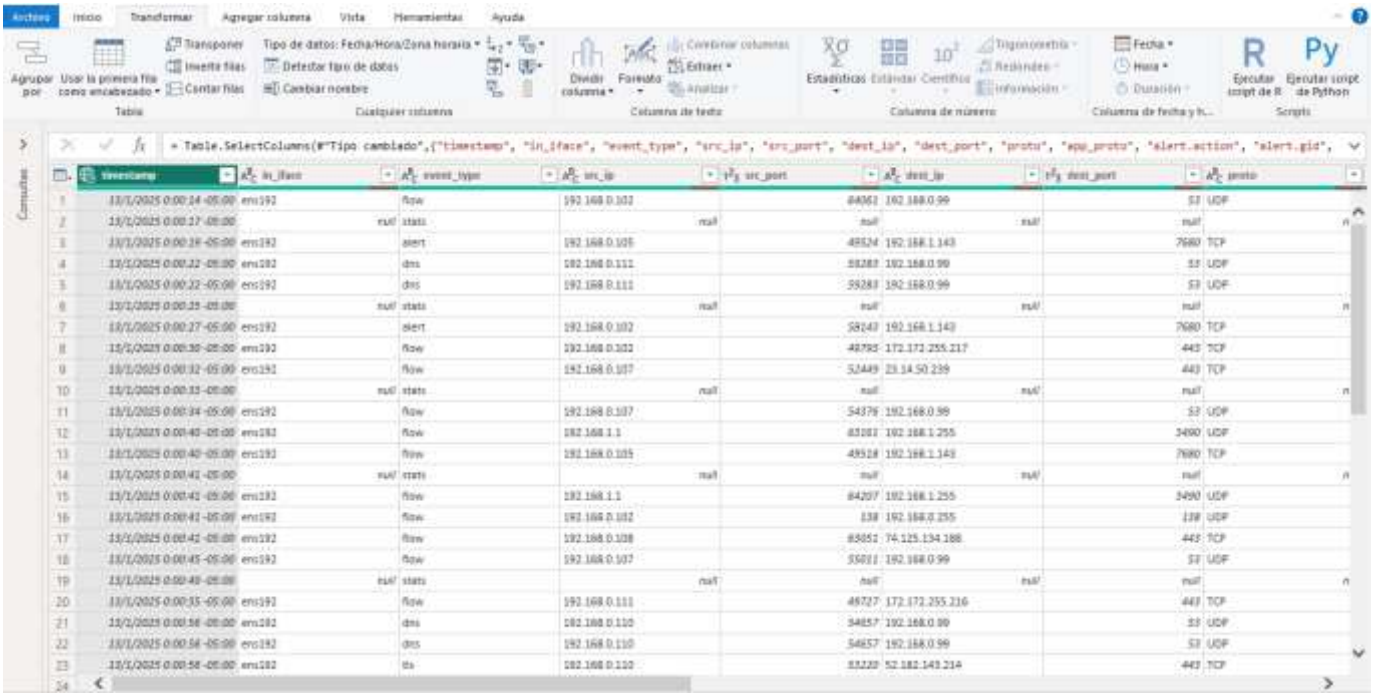


Figura 65 Carga de columnas en Power BI. Fuente: Power BI (s.f)

Una vez que cargamos el archivo se puede visualizar los datos en diferentes columnas como se observa en la figura 65. En las columnas se pueden observar la fecha y hora del evento, IP origen, IP destino, puerto origen, destino, protocolo y evento.

Con estas columnas se puede trabajar para agruparlas y así poder generar diferentes gráficas dinámicas con un análisis previo dependiendo del enfoque que se quiera lograr.

- **Frecuencia de eventos por tipo (event_type):**

El primer gráfico que se va a realizar va a ser un gráfico de barras agrupadas el cual muestre cuentos eventos existen por tipo.

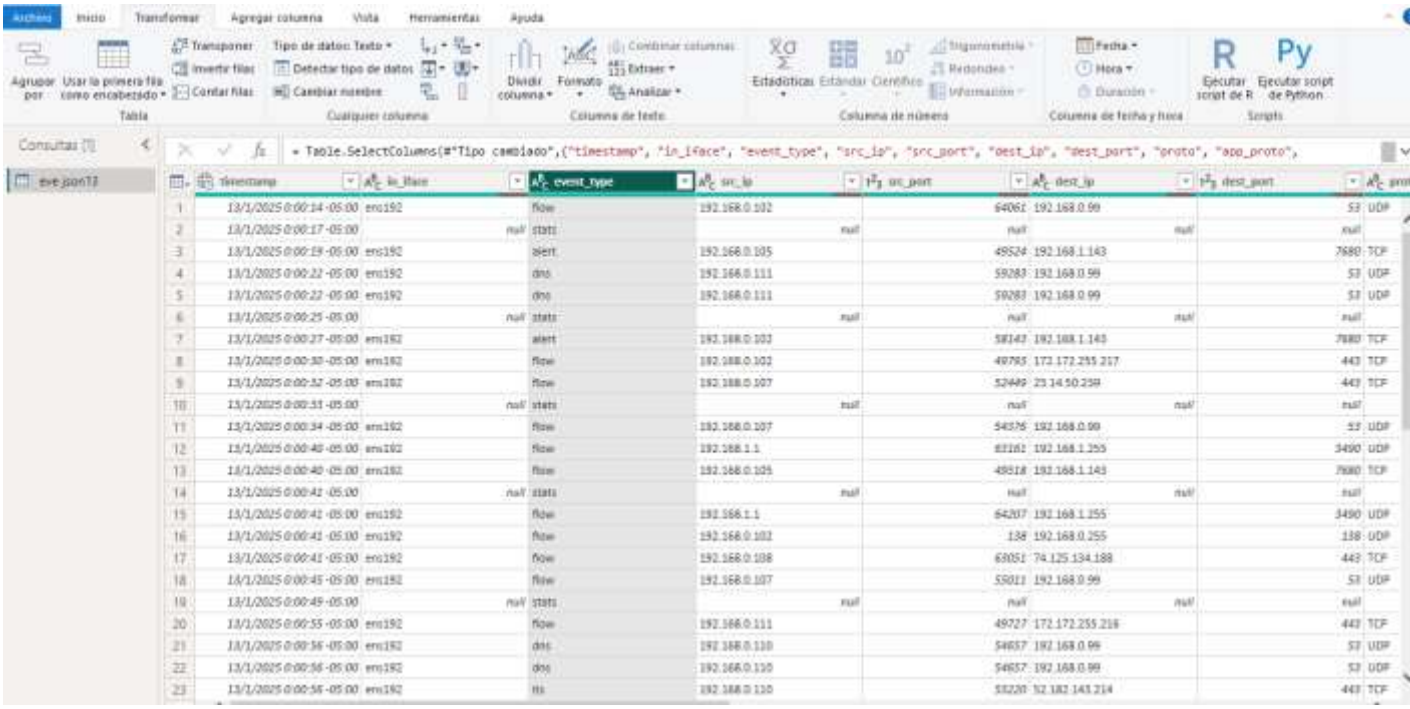


Figura 66 Carga de archivos eve.json13.json. Fuente: Power BI (s.f)

Para poder realizar el gráfico de barras, se va a seleccionar la columna event_type como se muestra en la figura 66. Una vez seleccionada la columna, vamos al menú superior en la sección “Transformar” y escogemos la opción “Agrupar por”.

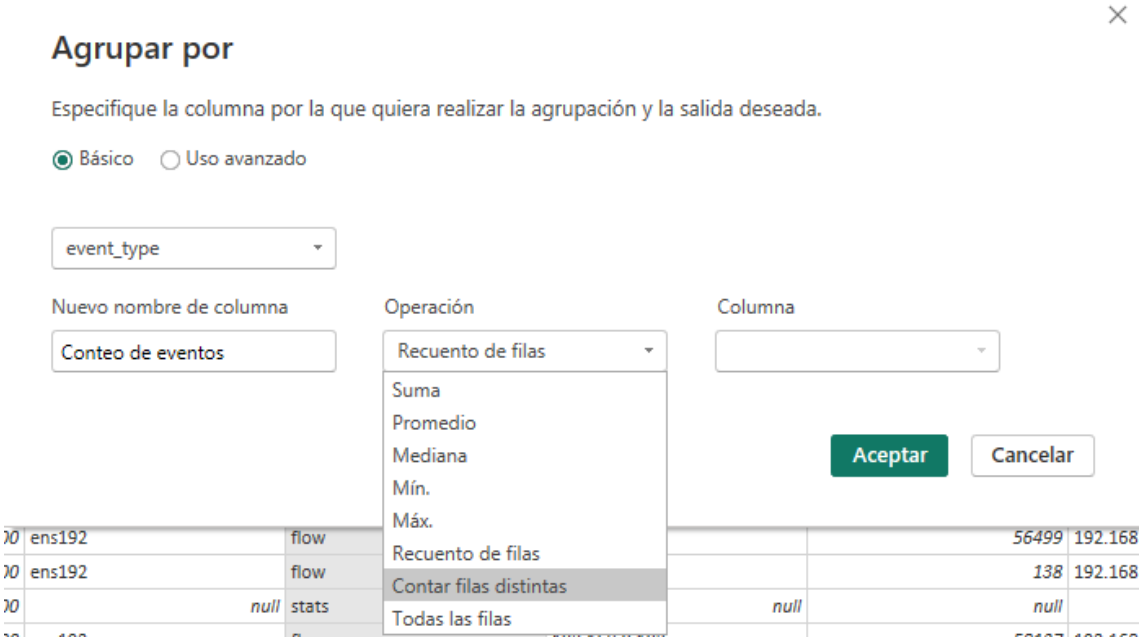


Figura 67 Agrupar por event_type .Fuente: Power BI (s.f)

Una vez seleccionada la opción "Agrupar por", como se observa en la figura 67, vamos a darle un nombre a la nueva columna que se va a generar, en este caso con el nombre "Conteo de eventos". Luego, en la sección de Operación, vamos a escoger la opción "Recuento de filas" para que así pueda contar los registros que hay en cada grupo. Una vez configurado la opción damos clic en Aceptar.

Figura 68 Resultado agrupación por event_type. Fuente: Power BI (s.f)

Como se puede observar en la figura 68, se agruparon los datos correctamente y se cargaron mostrando la nueva tabla con la que se va a dar uso para generar el gráfico de barras. Se puede observar el número de eventos clasificado por tipo de eventos. Podemos ver que en este archivo se observan 7894 alertas. Una vez que se cargue la tabla cerramos y aplicamos los cambios para que los datos se carguen al nuevo modelo de Power BI.

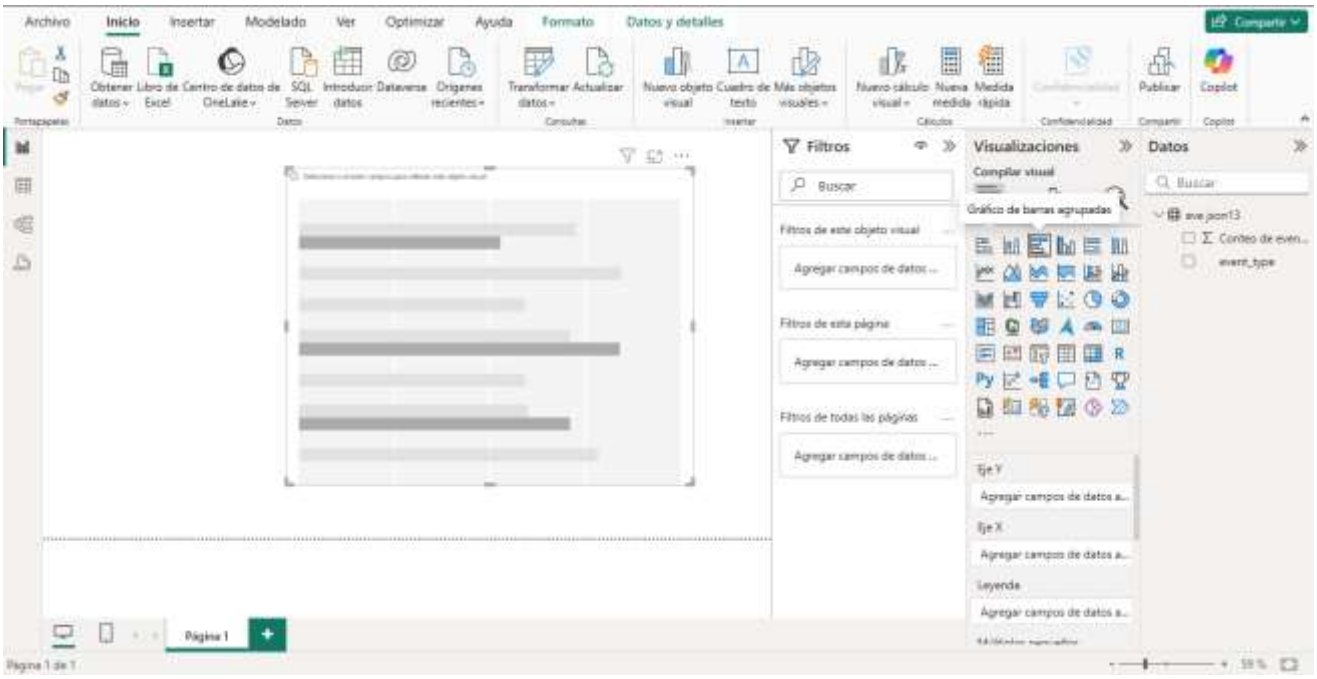


Figura 69 Carga del gráfico de barras agrupadas. Fuente: Power BI (s.f)

Una vez que cree el nuevo modelo de Power BI con los nuevos datos, se va a escoger el gráfico de barras agrupada en el panel de visualizaciones y se va a arrastrar a la página del informe como se puede observar en la figura 69. Una vez ya con el gráfico se van a escoger las columnas “event_type” en el eje de categorías y la columna “Conteo de eventos” en el campo de valores.

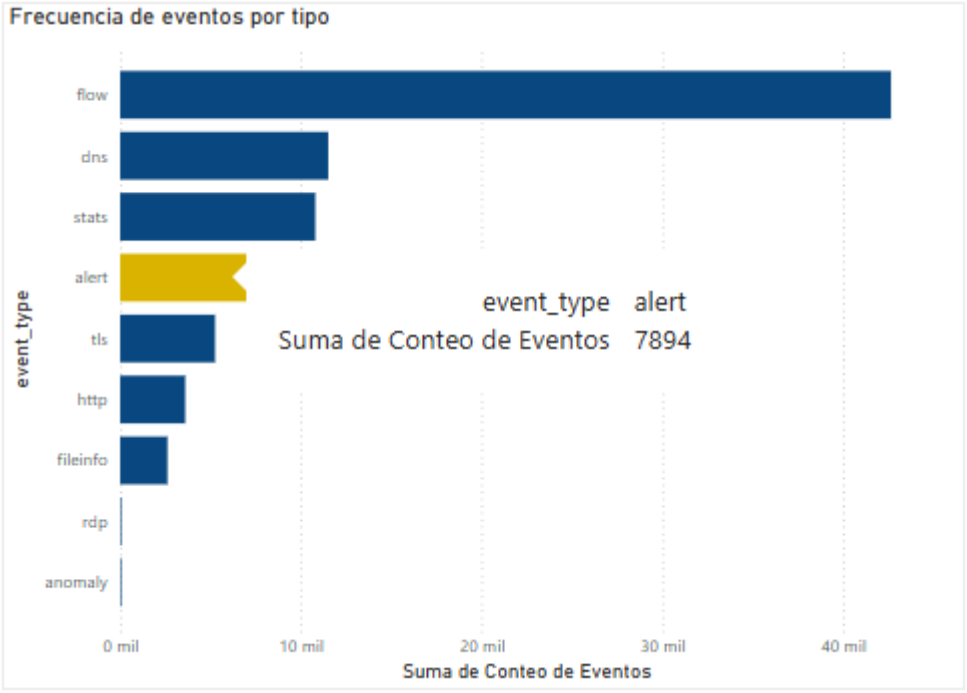


Figura 70 Gráfico de barras agrupado por tipo de evento. Fuente: Power BI (s.f)

Finalmente, como se puede observar en la figura 70, el gráfico de barras muestra las frecuencias de tipos de evento (event_type) con sus categorías en el eje "Y" y el conteo de cada categoría en el eje "X". Además, se muestra una etiqueta con el conteo total de eventos de tipo "alert", en este caso es de 7894. Cabe recalcar que las alertas generadas son de tipo medio o de tipo 3 por lo que se categoriza como tráfico no sospechoso.

- **Direcciones IP más frecuentes (src_ip):**

El segundo gráfico que se va a realizar va a ser un gráfico con las direcciones IP más activas o que generaron más conexiones.

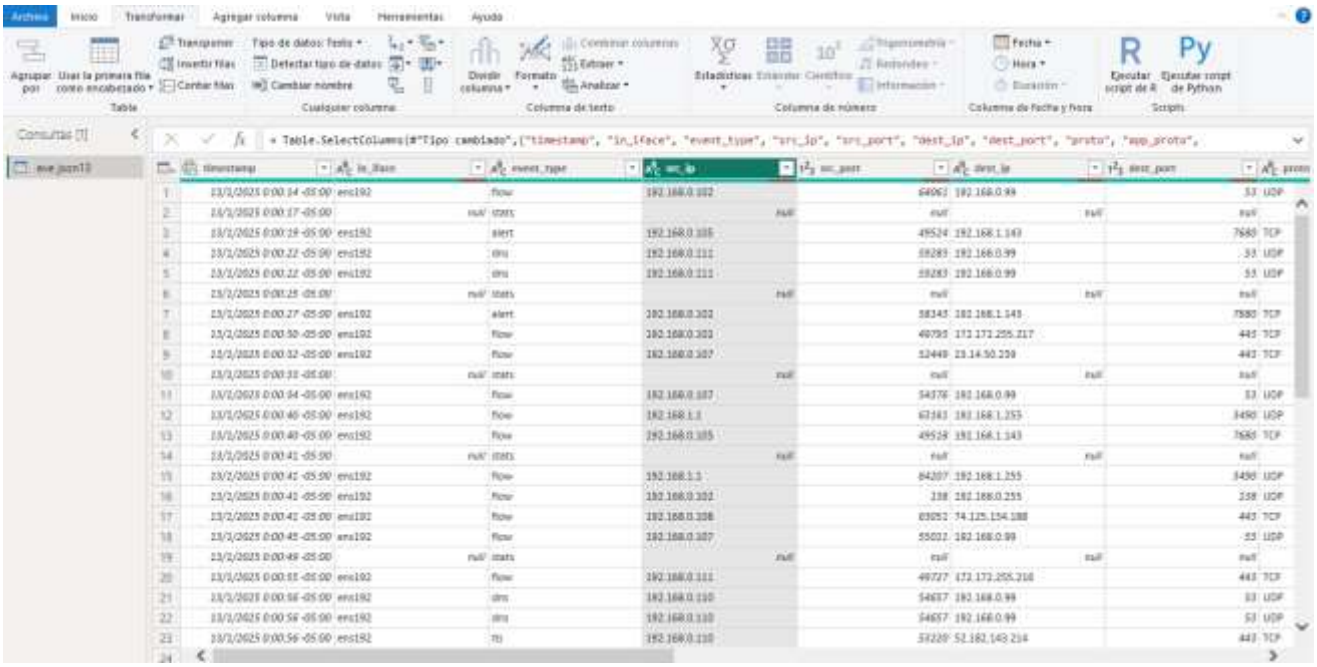


Figura 71 Carga de archivos eve.json13.json_2. Fuente: Power BI (s.f)

Para comenzar, se va a cargar el archivo eve.json13.json y se va a seleccionar la columna de IP origen (scr_ip) como se muestra en la figura 71. Una vez que se selecciona la columna src_ip, vamos a la sección de “Transformar” y damos clic en la opción “Agrupar por”

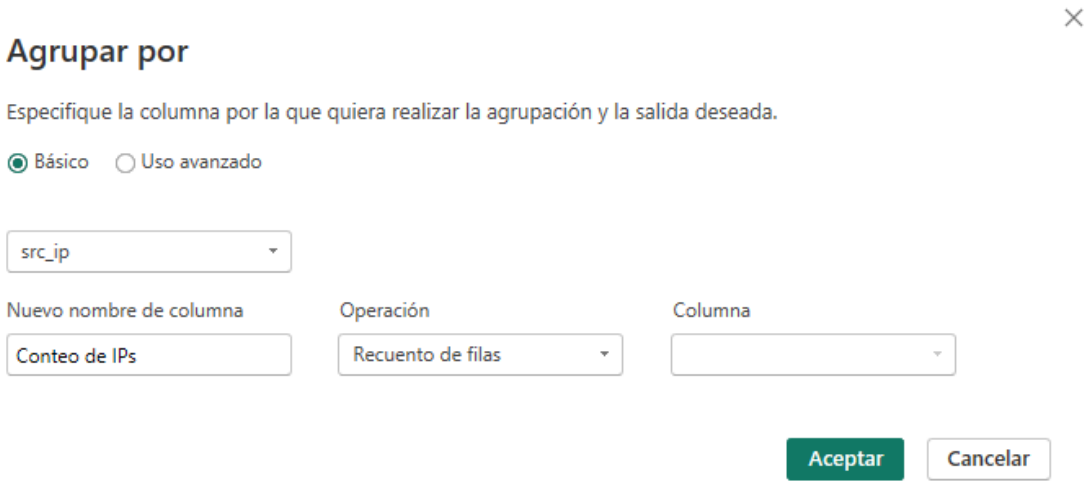
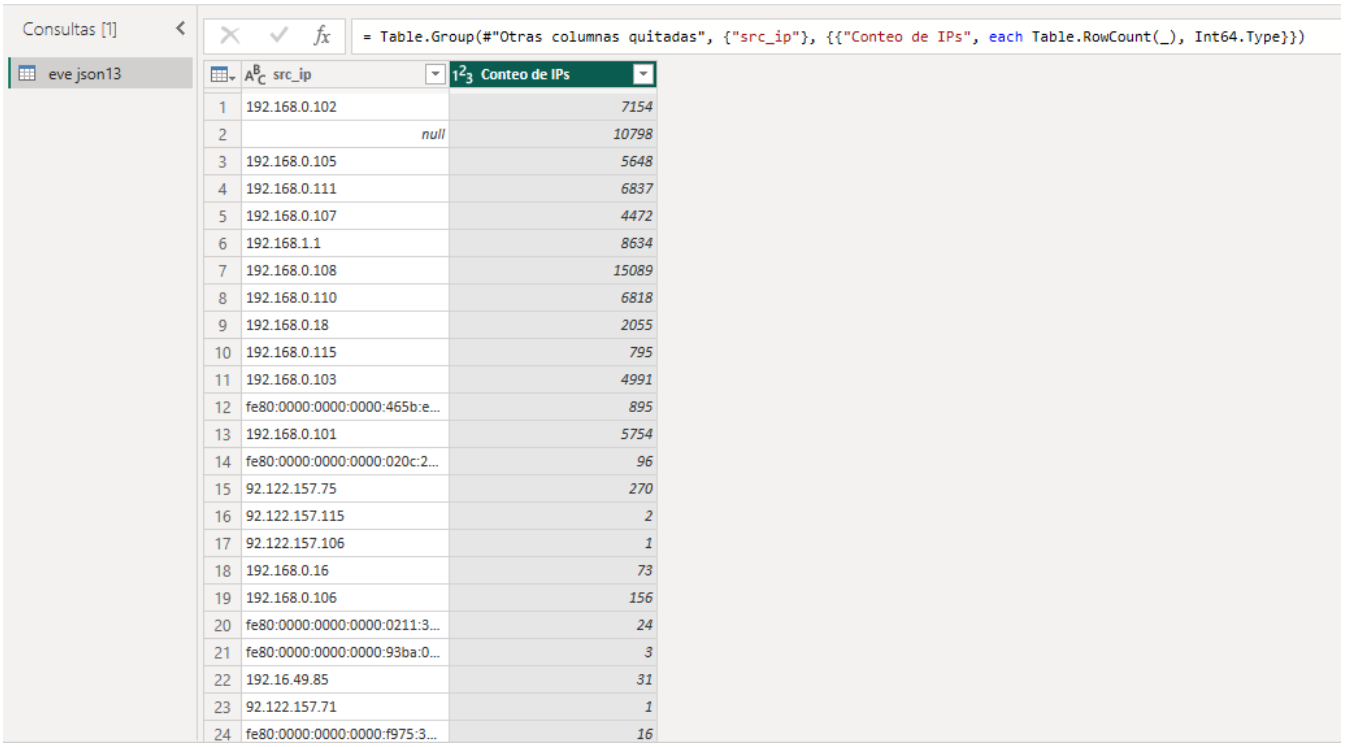


Figura 72 Agrupar por scr_ip. Fuente: Power BI (s.f)

Luego de seleccionar la opción, se va a dar nombre a la nueva columna. Como se puede ver en la figura 72, se da el nombre de “Conteo de IPs. Luego, en la sección de Operación, vamos a escoger la opción “Recuento de filas” para que así pueda contar los registros que hay en cada grupo. Una vez configurado la opción damos clic en Aceptar.



	src_ip	Conteo de IPs
1	192.168.0.102	7154
2	null	10798
3	192.168.0.105	5648
4	192.168.0.111	6837
5	192.168.0.107	4472
6	192.168.1.1	8634
7	192.168.0.108	15089
8	192.168.0.110	6818
9	192.168.0.18	2055
10	192.168.0.115	795
11	192.168.0.103	4991
12	fe80:0000:0000:0000:465b:e...	895
13	192.168.0.101	5754
14	fe80:0000:0000:0000:020c:2...	96
15	92.122.157.75	270
16	92.122.157.115	2
17	92.122.157.106	1
18	192.168.0.16	73
19	192.168.0.106	156
20	fe80:0000:0000:0000:0211:3...	24
21	fe80:0000:0000:0000:93ba:0...	3
22	192.16.49.85	31
23	92.122.157.71	1
24	fe80:0000:0000:0000:f975:3...	16

Figura 73 Resultado de agrupación por scr_ip. Fuente: Power BI (s.f)

Como se puede ver el resultado en la figura 73, tenemos el conteo total de IPs que son más frecuentes o activas. Se puede observar que la IP con más frecuencia proviene de la dirección 192.168.0.108 con un total de 15089 conexiones. Con esta nueva columna, podemos realizar un gráfico para visualizar de mejor manera los datos dentro del nuevo modelo de Power BI.

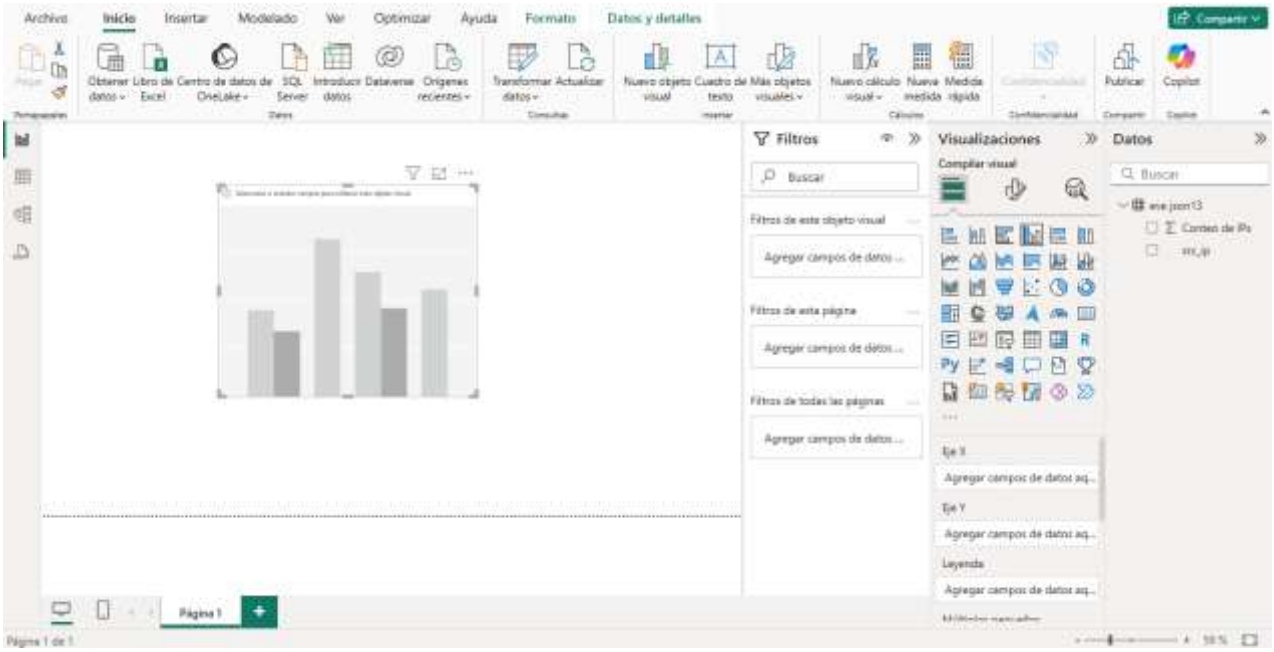


Figura 74 Carga de gráfico de columnas agrupadas. Fuente: Power BI (s.f)

Dentro de la pestaña de Power BI, se va a escoger el gráfico de columnas agrupadas que se encuentra en la parte derecha en la sección de “Visualizaciones”. Escogemos el gráfico y lo arrastramos a la página del informe como se puede ver en la figura 74. Luego, seleccionamos las columnas “scr_ip” y “Conteo de IPs” para así poder generar el gráfico

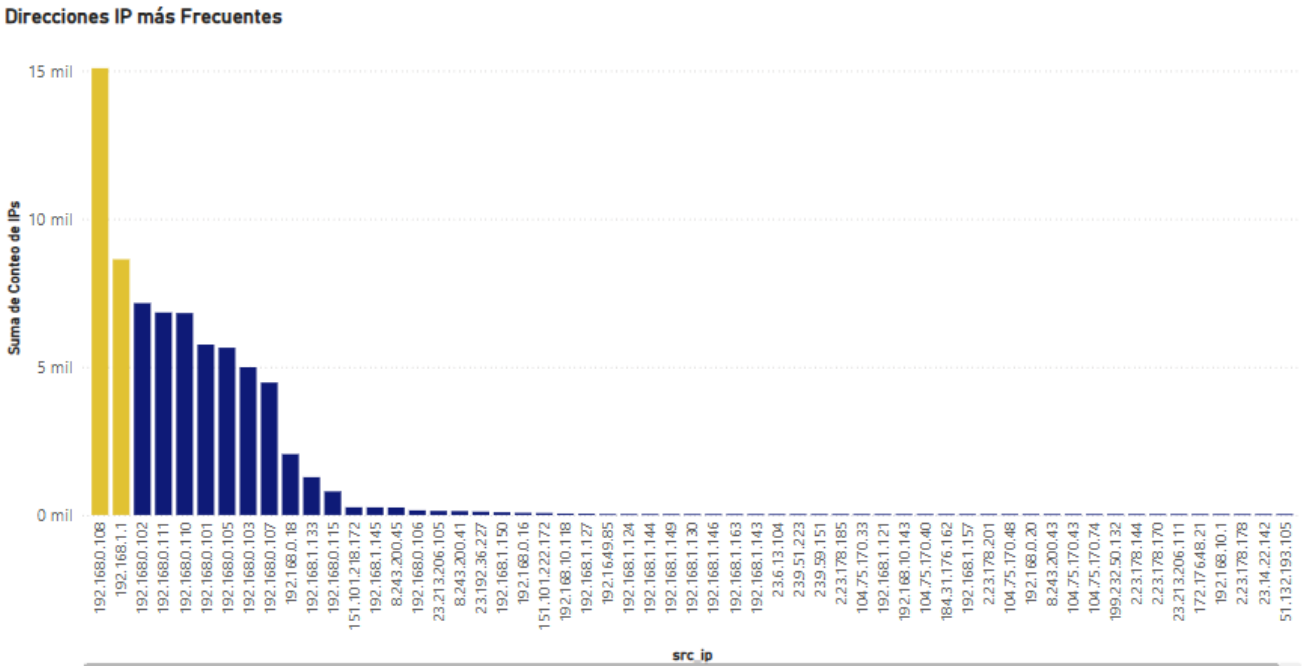


Figura 75 Gráfico de columnas agrupado por IP origen. Fuente: Power BI (s.f)

Finalmente, en la figura 75, se puede observar el gráfico de columnas agrupado por IP origen. En el eje “X” se puede observar que se encuentran las direcciones IP de origen y en el eje “Y” se encuentra la suma de conteos total por IP. Además, se puede observar la etiqueta que muestra la IP con mayor frecuencia o que tiene un mayor número de conexiones. En este caso es la IP 192.168.0.108 con un total de 15089 conexiones.

- **Alertas por fecha y hora (timestamp):**

El tercer gráfico que se va a realizar va a ser un gráfico de líneas para poder analizar cómo varían las alertas con el tiempo.

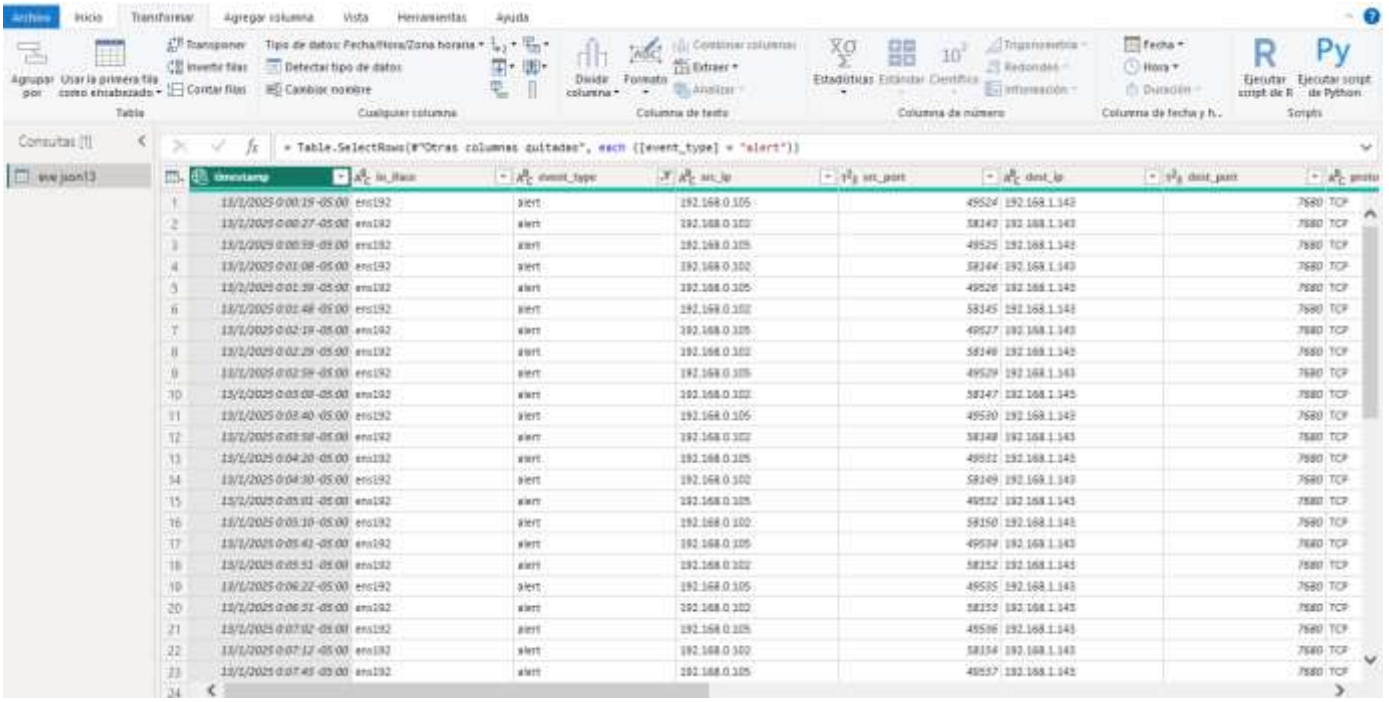


Figura 76 Carga de archivos eve.json13.json_3. Fuente: Power BI (s.f)

Como se puede ver en la figura 76, primero se deben cargar los datos del archivo con el cual vamos a generar el gráfico. En este caso, utilizaremos el archivo eve.json13.json. En este caso vamos a analizar las alertas y su variación con el tiempo, para ello vamos a filtrar en “event_type” la categoría “alert”. Además, vamos a seleccionar la columna “timestamp” que va a servir para poder agrupar la fecha y hora y el conteo de alertas generadas.

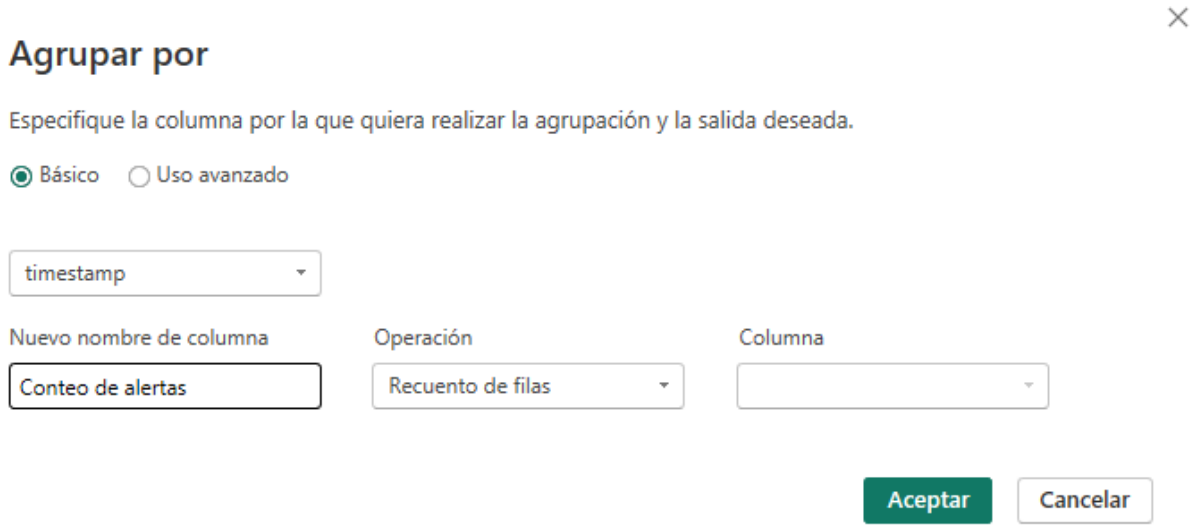
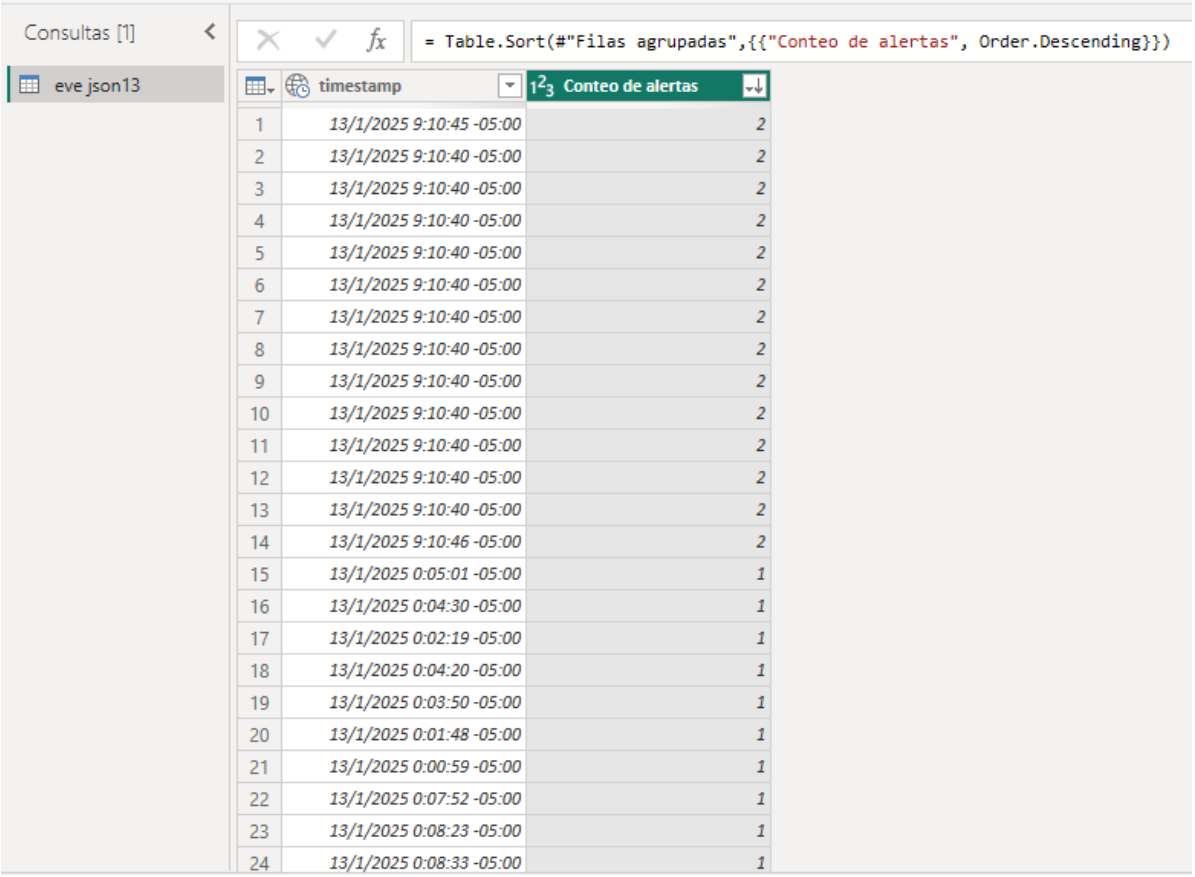


Figura 77 Agrupar por timestamp. Fuente: Power BI (s.f)

Una vez que seleccionamos la columna “timestamp”, vamos a la sección “Agrupar por” como se muestra en la figura 77. En la sección vamos a escoger la columna timestamp, vamos a darle el nombre de la nueva columna como “Conteo de alertas” y en operación vamos a seleccionar “Recuento de filas” para que cuente cada alerta generada.



	timestamp	Conteo de alertas
1	13/1/2025 9:10:45 -05:00	2
2	13/1/2025 9:10:40 -05:00	2
3	13/1/2025 9:10:40 -05:00	2
4	13/1/2025 9:10:40 -05:00	2
5	13/1/2025 9:10:40 -05:00	2
6	13/1/2025 9:10:40 -05:00	2
7	13/1/2025 9:10:40 -05:00	2
8	13/1/2025 9:10:40 -05:00	2
9	13/1/2025 9:10:40 -05:00	2
10	13/1/2025 9:10:40 -05:00	2
11	13/1/2025 9:10:40 -05:00	2
12	13/1/2025 9:10:40 -05:00	2
13	13/1/2025 9:10:40 -05:00	2
14	13/1/2025 9:10:46 -05:00	2
15	13/1/2025 0:05:01 -05:00	1
16	13/1/2025 0:04:30 -05:00	1
17	13/1/2025 0:02:19 -05:00	1
18	13/1/2025 0:04:20 -05:00	1
19	13/1/2025 0:03:50 -05:00	1
20	13/1/2025 0:01:48 -05:00	1
21	13/1/2025 0:00:59 -05:00	1
22	13/1/2025 0:07:52 -05:00	1
23	13/1/2025 0:08:23 -05:00	1
24	13/1/2025 0:08:33 -05:00	1

Figura 78 Agrupar por timestamp. Fuente: Power BI (s.f)

Como se puede ver el resultado en la figura 78, tenemos el conteo total de las alertas generadas por la fecha y hora. Se puede ver que la hora pico donde se registró más de una alerta fue entre las 09:10h del día 13 de enero del 2025. Con esta nueva columna, podemos realizar un gráfico para visualizar de mejor manera los datos dentro del nuevo modelo de Power BI.

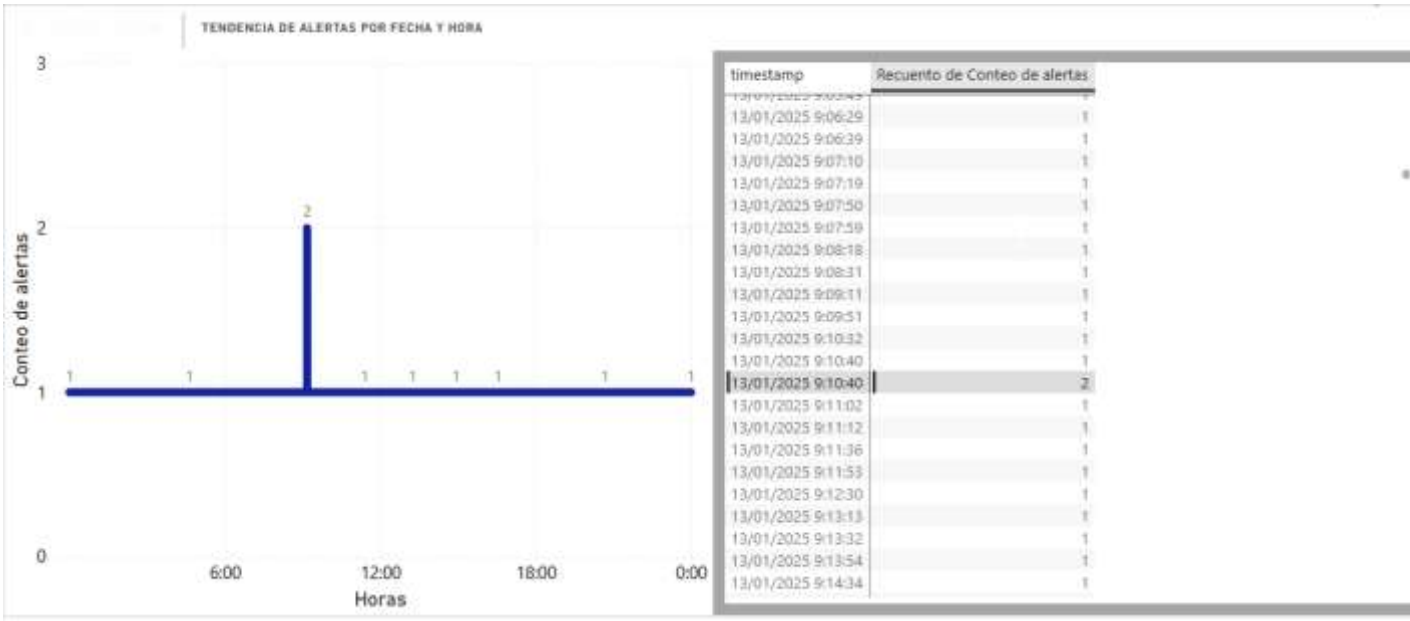
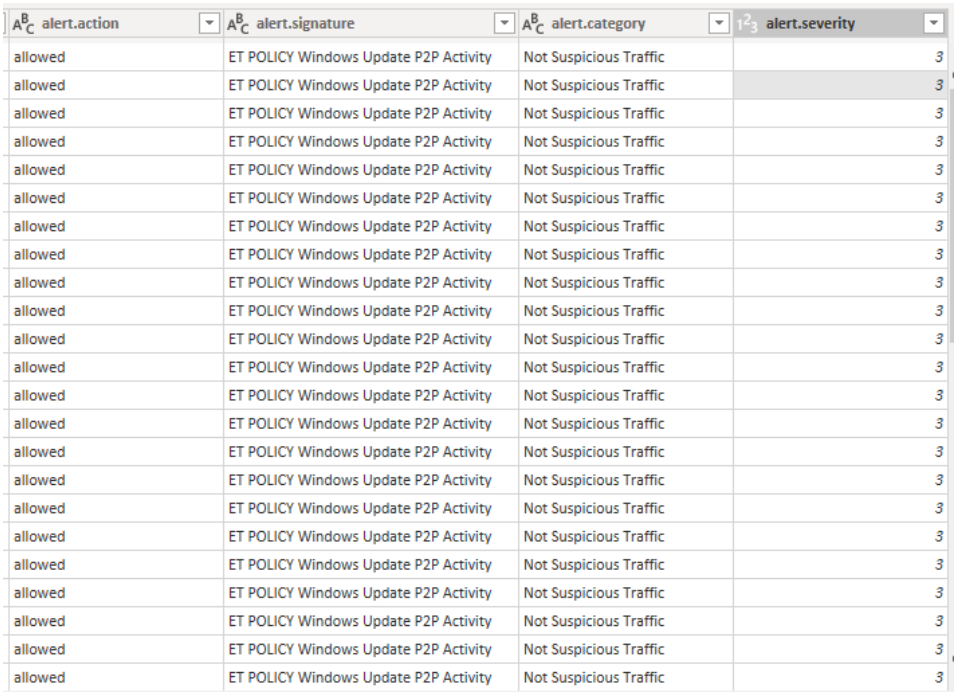


Figura 79 Tendencia de alertas por fecha y hora. Fuente: Power BI (s.f)

Una vez que se cargan los resultados en el nuevo modelo de Power BI vamos a seleccionar el gráfico de líneas. Dentro del gráfico de líneas vamos a cargar en el eje X la columna “timestamp” donde registra las horas y la fecha. En el eje Y vamos a cargar la columna “recuento de conteo de alertas” el cual registra el número de alertas por hora.

Como resultado tenemos en la figura 79 el gráfico de líneas ya generado y al lado derecho una tabla donde muestra de igual manera la columna timestamp, donde se marcan las horas registradas y también la columna reconteo de alertas, donde muestra el número de alertas registrado a esa hora. Además, se puede ver que exactamente a las 09:10:40h del día 13 de enero del año 2025, se registró el pico más alto de alertas generadas que fueron 2.



alert.action	alert.signature	alert.category	alert.severity
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3
allowed	ET POLICY Windows Update P2P Activity	Not Suspicious Traffic	3

Figura 80 Registro de alertas generadas en el archivo eve.json13.json. Fuente: Power BI (s.f)

Para saber qué tipo de alertas se generaron, en la figura 80 se muestra el tipo de alerta, en este caso fue de una actualización de Windows “ET POLICY Windows Update P2P Activity”. Se registró en la categoría como tráfico no sospechoso y en severidad se puede ver que es de tipo 3, es decir, significa de tipo mediano.

- **Distribución por protocolos (event_type):**

El último gráfico que se va a realizar va a ser un gráfico circular con la proporción de los eventos DNS, TLS, alertas, etc.

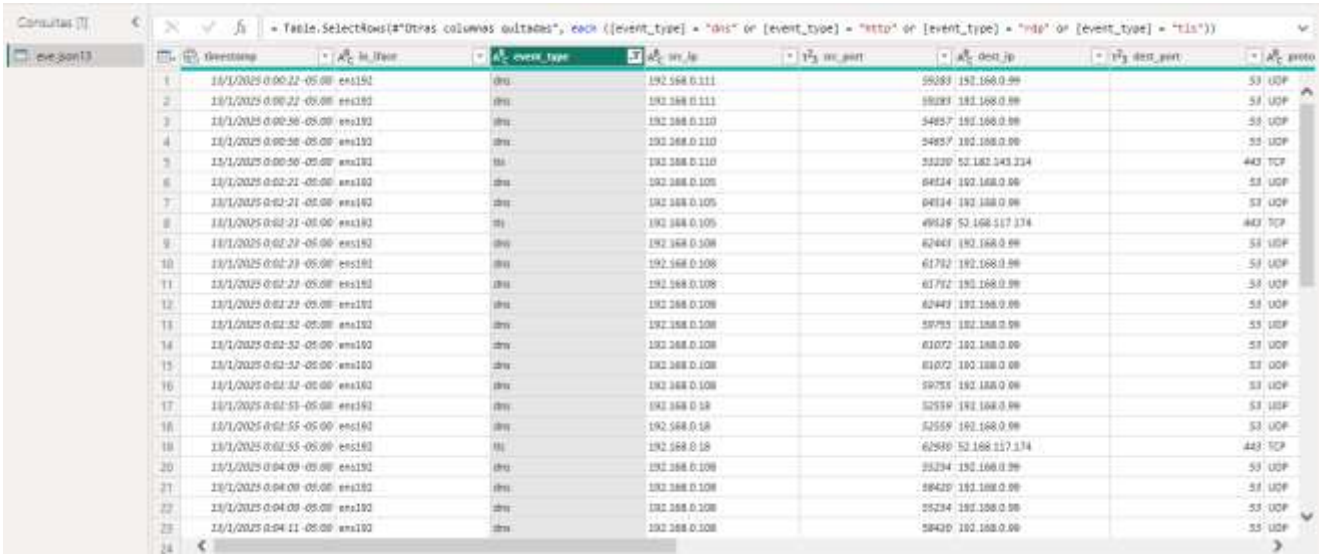


Figura 81 Carga de archivos eve.json13.json_4. Fuente: Power BI (s.f)

Para poder generar el gráfico de tipo pastel, primero debemos cargar los datos del archivo eve.json13.json como se puede ver en la figura 81. Una vez que cargamos los archivos, en la columna “event_type” debemos seleccionar los eventos que sean protocolos, en este caso van a ser: dns; tls; http; rdp. Una vez que seleccionamos los datos, debemos ir a la sección “Agrupar por” para así agrupar los datos y realizar el conteo.

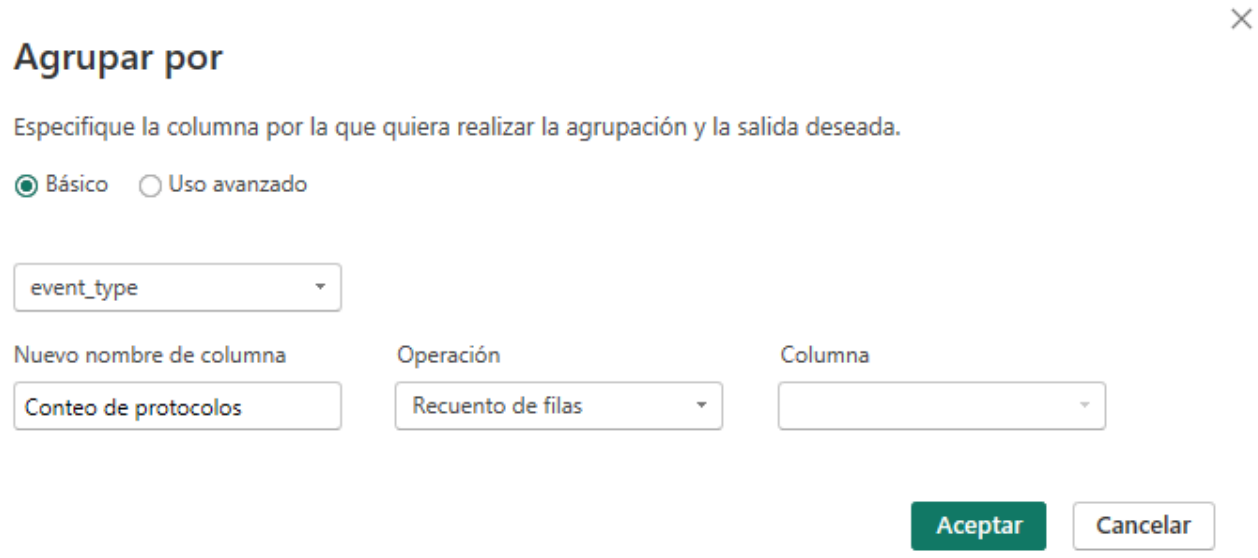


Figura 82 Agrupación por event_type conteo de protocolos. Fuente: Power BI (s.f)

Como se puede ver en la figura 82, una vez dentro de la sección “Agrupar por”, vamos a escoger los datos que queremos que agrupe la herramienta, en este caso va a ser “event_type”. Luego vamos a darle un nuevo nombre donde a la nueva columna agrupada como “Conteo de protocolos” y en operación escogemos “Recuento de filas” para que pueda contar cada evento registrado.

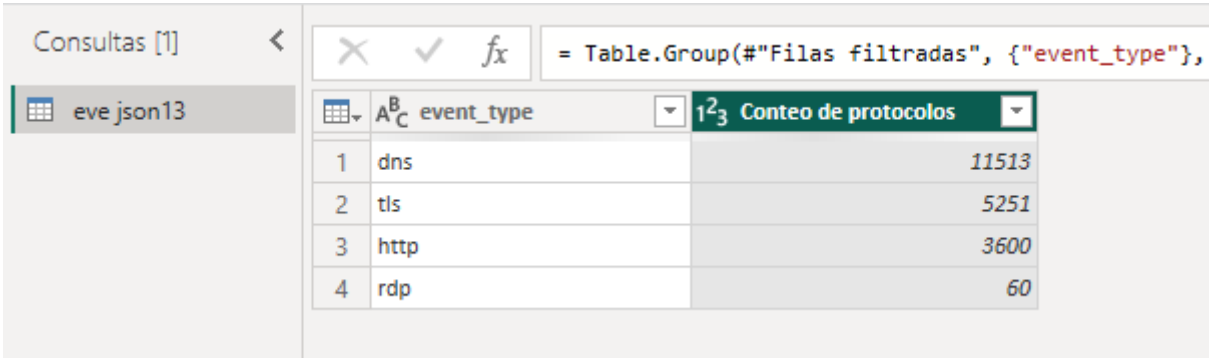


Figura 83 Resultado de protocolos y el conteo de cada uno. Fuente: Power BI (s.f)

Como se puede ver en la figura 83, tenemos el resultado de la nueva columna una vez que agrupamos los datos. Se puede ver que el protocolo más utilizado es DNS con 11513 registros. Con la nueva columna aplicamos y guardamos los cambios para así crear nuestro nuevo modelo de Power BI y poder realizar el gráfico.

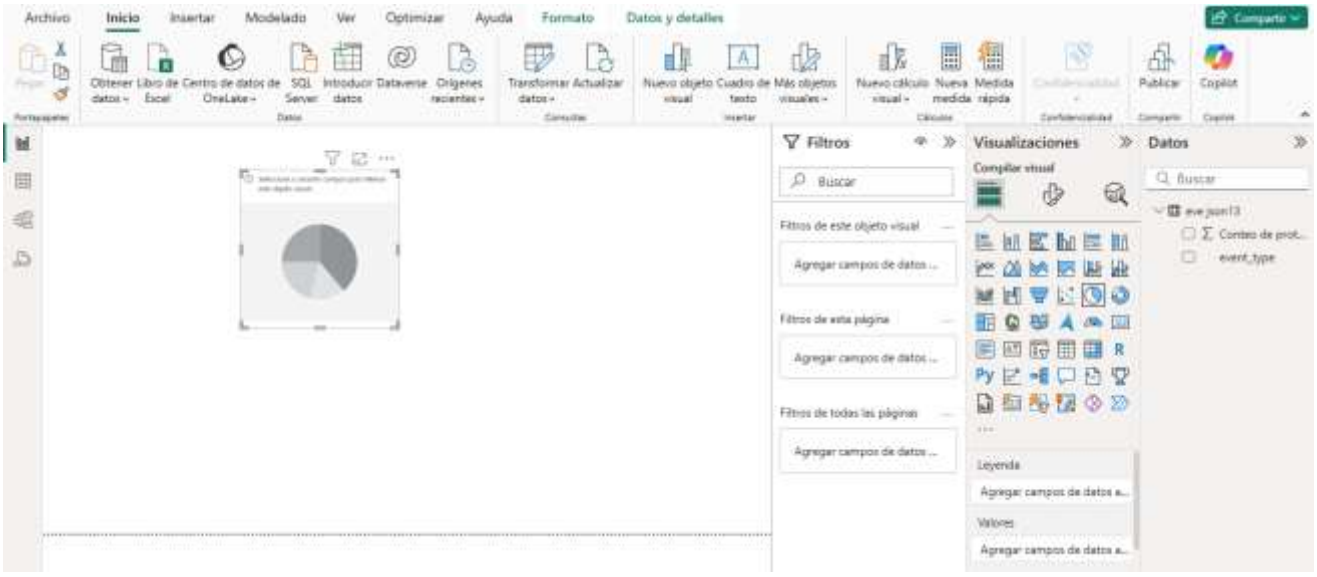


Figura Carga de gráfico tipo pastel en el informe principal. Fuente: Power BI (s.f)

Como se puede ver en la figura 84, se cargaron los nuevos datos agrupados. Vamos a seleccionar el gráfico de pastel que se encuentra en el lado derecho en la sección de "Visualizaciones" y arrastrar hacia la página del informe principal. En el campo de "Leyenda" vamos a agregar la columna "event_type" y en el campo de "Valores" vamos a agregar la columna "Conteo de protocolos".

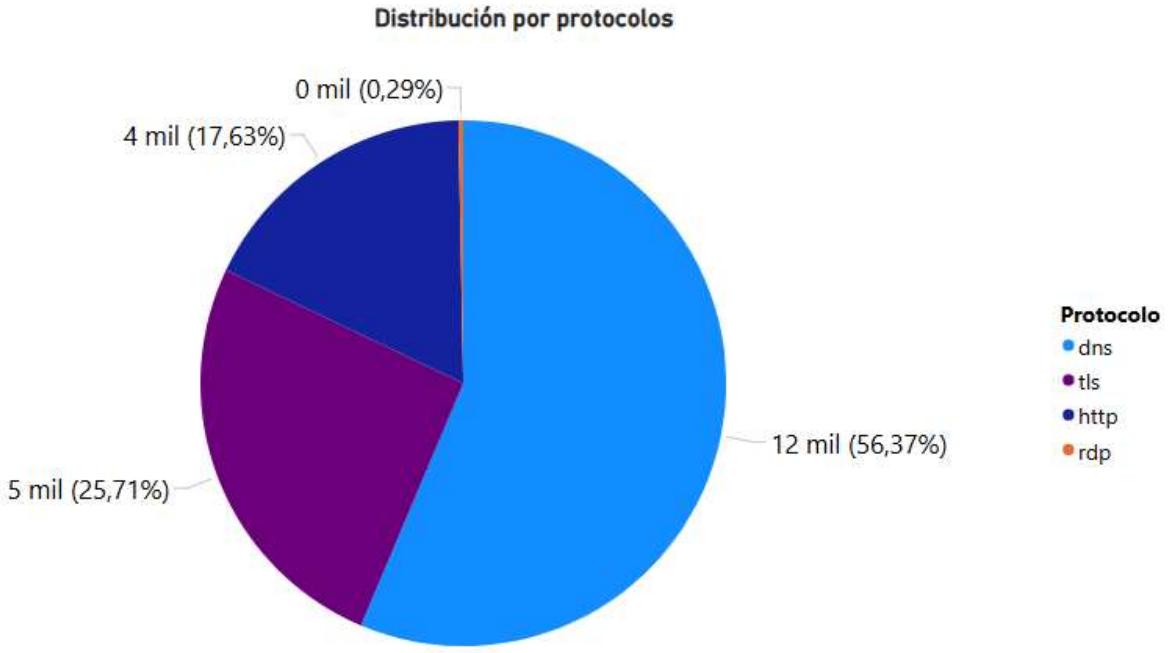


Figura 84 Gráfico tipo pastel por distribución de protocolos. Fuente: Power BI (s.f)

Finalmente, se puede observar en la figura 85 el resultado final. En este caso podemos ver los diferentes protocolos representados por un color diferente además del porcentaje total de conexiones junto a un valor estimado contado por "mil". Se puede observar que más del 50% de conexiones se han realizado por DNS y en el gráfico está interpretado de color celeste. También se puede ver que menos del 1% de conexiones han sido por RDP.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Como conclusión, dentro del presente trabajo de titulación, se realizó el análisis de la infraestructura de red de la empresa en la que se trabajó el presente trabajo de titulación. Una vez que se realizó el análisis, se pudo identificar las actividades críticas que requieren un monitoreo constante.

- Además, como conclusión, se pudo aplicar la herramienta Suricata dentro del entorno controlado de la empresa. Se pudo realizar la instalación, configuración y monitoreo del tráfico de red junto con el análisis gracias a la aplicación de la herramienta durante un periodo de tiempo.

- Igualmente, se realizó la instalación de la herramienta Zui, que permitió realizar la carga y el análisis de los archivos json generados por Suricata a través del lenguaje de consultas Zed. Gracias a esta herramienta se pudo cargar y visualizar los archivos json generados por Suricata y además poder realizar un análisis por los eventos generados durante un periodo de tiempo.

- Asimismo, se utilizó la herramienta Power BI para así poder cargar los archivos json generados por Suricata, filtrar los datos, y poder generar gráficos que ayuden a poder visualizar de mejor manera la información generada en base a filtros dependiendo del análisis que se llegó a realizar.

- También, una vez que se visualizó y se observaron los datos generados, se pudo realizar el análisis de los hallazgos obtenidos del monitoreo del tráfico de red por parte de la herramienta Suricata para así lograr obtener un mejor panorama en base al tráfico de red que transita dentro de la empresa del presente caso de estudio.

- Finalmente, luego de la muestra y análisis de información gracias a estas herramientas, se pudo evaluar la efectividad de Suricata como sistema de detección de intrusos midiendo su capacidad para poder identificar alertas, amenazas, protocolos, direcciones y entre otros campos que ayudaron a realizar un análisis preciso del tráfico de red.

6.2 RECOMENDACIONES

- Una vez que se realizó la implementación y el análisis de los resultados con la herramienta suricata, se recomienda establecer políticas y restricciones a nivel de aplicaciones dentro de la empresa donde se realizó la aplicación.

- Además, se recomienda actualizar constantemente la herramienta suricata con nuevas reglas que puedan alertar sobre nuevas amenazas que pueden ocasionar daños en la empresa. Se pueden actualizar las reglas desde portales como Emergin Threats.

- También, se recomienda establecer políticas de seguridad al momento de acceder a los sistemas donde se manejan los procesos críticos de la empresa. Las políticas pueden ser de respuestas ante posibles incidentes para así poder abordar de manera rápida y proactiva cualquier problema de seguridad o falla en el sistema que se registre en los logs que proporciona Suricata.

- Finalmente, se recomienda proporcionar capacitación al personal de TI de la empresa para así poder administrar y gestionar la herramienta Suricata para analizar eventos o alertas de niveles críticos que puedan generar daños en la empresa. Es importante que el personal capacitado esté actualizado de nuevas amenazas y establecer políticas de seguridad para evitar su explotación.

CAPÍTULO VII: REFERENCIAS BIBLIOGRÁFICAS

REFERENCIAS BIBLIOGRÁFICAS

Almantas Kakareka, C. G. (2014). Detecting System Intrusions. En J. R. Vacca, *Network and System Security* (págs. 1-27). USA: ELSEVIER.

Axess Network. (30 de November de 2022). *¿Qué son las topologías de red y cuál es su clasificación?* Obtenido de https://axessnet.com/topologias-de-red/

Becolve. (7 de November de 2020). *IDS vs IPS: ¿Cuál es la diferencia?* Obtenido de https://becolve.com/blog/ids-vs-ips-cual-es-la-diferencia/

Berman, D. (18 de February de 2019). *). Network Security Monitoring with Suricata, Logz.io and the ELK Stack*. Obtenido de Logz.io: https://logz.io/blog/network-security-monitoring/

CISA. (2024). *Mitigating cyber threats with limited resources: Guidance for civil society*. Obtenido de Cybersecurity and Infrastructure Security Agency. : https://www.cisa.gov/sites/default/files/2024-08/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3_ES.pdf

Comisión Federal de Comercio. (16 de April de 2019). *Marco de ciberseguridad del NIST*. Obtenido de https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Cuadrado, G. C. (7 de April de 2021). *Topología de redes informáticas: Tipos, características y aplicaciones.* Obtenido de OpenWebinars: https://openwebinars.net/blog/topologia-de-redes-informaticas/#:~:text=La%20topolog%C3%ADa%20l%C3%B3gica%20se%20refiere,significativamente%20de%20la%20topolog%C3%ADa%20f%C3%ADsica.

Departamento de Consultoría. (3 de September de 2021). *Estándares y normas ISO para mejorar la ciberseguridad*. Obtenido de GlobalSuite Solutions: https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/#La_ciberseguridad_y_las_normas_ISO

Durán, J. J. (16 de July de 2024). *Manual Operativo de Instalación y Configuración de Suricata*. Obtenido de Binario 0: https://binariocero.com/linux/manual-operativo-de-instalacion-y-configuracion-de-suricata

EITCA Academy. (2 de April de 2024). *Diferenciar entre redes de área local (LAN) y redes de área amplia (WAN), incluidas sus respectivas funciones y casos de uso típicos*. Obtenido de https://es.eitca.org/la-seguridad-cibern%C3%A9tica/eitc-es-cnf-fundamentos-de-redes-inform%C3%A1ticas/introducci%C3%B3n-eitc-es-los-fundamentos-de-las-redes-inform%C3%A1ticas-cnf/introducci%C3%B3n-a-la-creaci%C3%B3n-de-redes/examen-revisi%C3%B3n-introducc

España, G. d. (16 de Julio de 1992). *Ley 21/1992, de 16 de julio, de Industria. Boletín Oficial del Estado*. Obtenido de https://www.boe.es/buscar/doc.php?id=BOE-A-1992-17363

Geekflare. (31 de August de 2021). *IDS vs IPS: Guía completa de soluciones de seguridad para redes*. Obtenido de https://geekflare.com/es/ids-vs-ips-network-security-solutions/

GeeksforGeeks. (2017). *Types of area networks LAN, MAN and WAN*. Obtenido de https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/

Gunashree, R. d. (8 de August de 2024). *Guide to Suricata: Network Security, IDS, IPS, and NSM*. Obtenido de Devzery Latest: https://www.devzery.com/post/guide-to-suricata-network-security-ids-ips-and-nsm

Hwang, D. (2021). *Red de área local o LAN*. Obtenido de ComputerWeekly: https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

IBM. (28 de July de 2021). *¿Qué es la seguridad de red?* Obtenido de https://www.ibm.com/es-es/topics/network-security

IBM. (20 de September de 2021). *Networking*. Obtenido de https://www.ibm.com/es-es/topics/networking

IBM. (2 de November de 2023). *¿Qué es el marco de ciberseguridad del NIST?* Obtenido de https://www.ibm.com/es-es/topics/nist

IBM. (19 de April de 2023). *Sistema de detección de intrusiones*. Obtenido de https://www.ibm.com/es-es/topics/intrusion-detection-system

INCIBE. (3 de September de 2020). *¿Qué son y para qué sirven los SIEM, IDS e IPS?* . Obtenido de https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

Kaspersky. (25 de May de 2020). *¿Qué es la ciberseguridad?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOoqWUI4gfYdNjOUOIMG2hweBkg1ebgYRtf5472Ex0VfrK5MuC9ni

Moes, T. (June de 2023). *What is network topology? Everything you need to know*. Obtenido de SoftwareLab: https://softwarelab.org/blog/what-is-network-topology/

National Cybersecurity Alliance. (6 de May de 2022). *Seguridad Digital Básica. Alianza Nacional de Ciberseguridad*. Obtenido de https://staysafeonline.org/es/resources/online-safety-basics/

NormasISO.org. (13 de January de 2023). *Norma ISO 27033: Seguridad de las redes.* . Obtenido de https://normasiso.org/norma-iso-27033/

Orovengua, J. (2 de December de 2022). *Suricata: Herramienta para la detección y prevención de intrusiones y seguridad*. Obtenido de Linux Party: https://www.linuxparty.es/57-seguridad/11235-suricata-herramienta-para-la-deteccion-y-prevencion-de-intrusiones-y-seguridad.html

OWASP Foundation. (s.f.). *Intrusion Detection*. Obtenido de https://owasp.org/www-community/controls/Intrusion_Detection

Robinette, D. (8 de January de 2024). *What is the Difference Between Snort and Zeek?* . Obtenido de Stamus-Networks.com: https://www.stamus-networks.com/blog/what-is-the-difference-between-snort-and-zeek

Saavedra, J. (1 de June de 2023). *¿Qué es Power BI?* Obtenido de EBAC: https://ebac.mx/blog/que-es-power-bi

Santos, J. J. (28 de October de 2022). *Seguridad de la red: ¿Qué es, cómo funciona y qué tipos existen?* . Obtenido de https://www.deltaprotect.com/blog/seguridad-de-la-red

Santos, J. J. (20 de April de 2023). *7 Principales Amenazas de Ciberseguridad: Cómo Prevenirlas*. Obtenido de Deltaprotect: https://www.deltaprotect.com/blog/amenazas-de-ciberseguridad

SensorTech. (25 de September de 2023). *Estándares de seguridad: Todo lo que necesitas saber*. Obtenido de SensorTech: https://sensorstechforum.es/cuales-son-los-estandares-de-seguridad/

Seguridad de la información Asia. (21 de September de 2024). *¿Qué es un sistema de detección de intrusos (IDS)?* . Obtenido de https://informationsecurityasia.com/es/what-is-an-intrusion-detection-system/

Software y Hardware. (10 de November de 2023). *¿Cómo funciona un sistema de detección de intrusos (IDS)*. Obtenido de https://softwareyhardware.com/ciberseguridad/como-funciona-un-sistema-de-deteccion-de-intrusos-ids/

Team Ambit. (9 de July de 2024). *Herramientas y Tecnologías para Mejorar la Seguridad Informática*. Obtenido de . https://www.ambit-bst.com/blog/herramientas-y-tecnologias-seguridad-it

Troan, E. (2019). *Ubuntu manuals*. Obtenido de Canonical: https://manpages.ubuntu.com/manpages/focal/es/man8/logrotate.8.html

Universidad Nacional De La Plata. (2017). *Algunas amenazas y sus consecuentes precauciones*. Obtenido de https://www.econo.unlp.edu.ar/detise/amenazasinformaticas-3918

West, M. (2014). Chapter 2 - Preventing System Intrusions. En J. R. Vacca, *Network and System Security* (págs. 29-56). USA: ELSEVIER.