UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTOR: Ing. Marcos Andrés Alcocer Bahamonde

Ing. Jean Pierre del Castillo Soto

Ing. Boris Emerson Gomez Cumbajin

Ing. Carlos Luis Hidalgo Llumiquinga

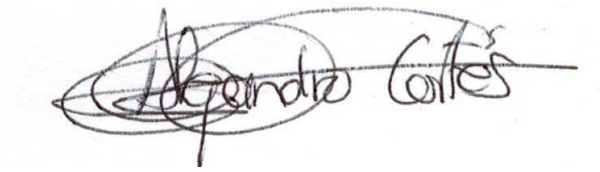
TUTOR: Ing. Alejandro Cortés López

Implementación y análisis de un sistema de monitorización y correlación de eventos para infraestructuras empresariales

QUITO – ECUADOR | 2022

APROBACIÓN DEL TUTOR

Yo, Alejandro Cortés, certifico que conozco a los autores del presente trabajo siendo los responsables exclusivos tanto de su originalidad y autenticidad, como de su contenido.



ALEJANDRO CORTÉS

DIRECTOR DE TESIS

CERTIFICACIÓN DE AUTORÍA

Nosotros, Marcos Andrés Alcocer Bahamonde, Jean Pierre del Castillo Soto, Boris Emerson Gomez Cumbajín, Carlos Luis Hidalgo Llumiquinga, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

…… ……

Marcos Andrés Alcocer Bahamonde Jean Pierre del Castillo Soto

…… ……

Boris Emerson Gomez Cumbajin Carlos Luis Hidalgo Llumiquinga

IMPLEMENTACIÓN Y ANÁLISIS DE SIEM

Dedicatorias

A mis padres Fabian y Angélica que ha base de su esfuerzo, paciencia, cariño y apoyo han sabido guiarme y mantenerme en un buen camino y así mismo a mi hermano Carlos por ser el motor fundamental que me ha impulsado a tomar las mejores decisiones a lo largo de mi vida personal como laboral y además por brindarme todo el cariño y su ayuda de forma desinteresada.

Marcos Andrés Alcocer Bahamonde

A mi familia y amigos cercanos que me han acompañado y educado durante toda mi vida, especialmente en esta etapa, brindándome su incondicional apoyo, amor y paciencia, sin ellos no cumpliría está meta planteada.

Jean Pierre del Castillo Soto

Dedico este proyecto a mi esposa Daniela e hijos José Ignacio y Alessia por todo el cariño, la paciencia y el apoyo constante durante el tiempo dedicado para obtener el título de Magister en Ciberseguridad. Así como a todos mis seres queridos ya que sin ellos la culminación de este no hubiera sido posible.

Boris Emerson Gómez Cumbajín

A mi familia por el apoyo y confianza brindado, por ser los pilares de cada una de mis metas planteadas, pero sobre todo a mí Rosita mi querida madre que con su esfuerzo, dedicación y comprensión me ha permitido concluir una nueva meta.

Carlos Luis Hidalgo Llumiquinga

Agradecimientos

Agradezco a Dios, a mi familia y compañeros de maestría por brindarme el apoyo necesario a lo largo de este arduo camino para alcanzar esta meta.

Marcos Andrés Alcocer Bahamonde

A Dios.

A mi familia por su amor, compañía y apoyo en mis estudios, gracias por su confianza en mí, gracias por siempre desear lo mejor para mí, gracias por los consejos y su motivación para lograr cada pequeño paso que he dado.

Jean Pierre del Castillo Soto

Agradezco a mi familia, amigos compañeros de maestría, por todo el apoyo y confianza que me ha permitido llegar a este punto de cierre y alcanzar esta nueva meta.

Boris Emerson Gómez Cumbajín

Agradezco a Dios, a mis padres Luis, Rosa y mis hermanos Diego, Roxana por su apoyo y aliento a lo largo del camino para conseguir esta nueva meta, que se ven reflejados en este proyecto.

Carlos Luis Hidalgo Llumiquinga

Resumen

En este documento, se consultaron diferentes herramientas de correlación de eventos, las 6 principales que se reflejan como líderes en el Cuadrante Mágico de Gartner (Schneider, 2022) con software propietario, donde nos decidimos levantar un laboratorio con LogRhythm por las buenas reseñas que se presenta en el estudio concerniente a la facilidad de implementación y otro laboratorio con herramientas Open Source muy utilizadas por su integración y dashboard intuitivo como es Wazuh, que fue considerada por los conocimientos adquiridos en el módulo de tecnologías SIEM. En este módulo se eligió Wazuh como SIEM por ser una herramienta Open Source que además nos permite integrar varios activos con varias alternativas de registros para tener un control detallado y automatizado de alertas. Aprovechando Slack y Telegram como herramientas de comunicación hicimos que las alarmas sean visualizadas a través de la plataforma y de su aplicativo móvil para un control y acción ágil ante anomalías detectadas. Por otro lado, se eligió Pfsense como Firewall Open Source al ser una herramienta que nos brinda una interfaz web permitiéndonos realizar sus configuraciones de forma sencilla, además cuenta con un gestor de paquetes como Squid, Snort, etc. Ampliando las funcionalidades solamente seleccionando el paquete y Pfsense lo descarga e instala automáticamente.

Como resultado de la implementación de los laboratorios se proponen recomendaciones para que una empresa pueda elegir de mejor manera el SIEM que se ajuste a sus necesidades, presupuesto y tiempo de implementación, tomando en cuenta las ventajas del Software propietario vs Open Source.

Palabras clave: SIEM, Open Source, Wazuh, LogRhythm

Abstract

In this document, different event correlation tools were consulted, the 6 main ones that are reflected as leaders in the Gartner Magic Quadrant (Schneider, 2022) with proprietary software, where we decided to set up a laboratory with LogRhythm due to the good reviews presented in the study concerned to the ease of implementation and another laboratory with Open Source tools widely used for their integration and intuitive dashboard, such as Wazuh, which was considered for the knowledge acquired in the SIEM technologies module. In this module, Wazuh was chosen as SIEM because it is an Open Source tool that also allows us to integrate various assets with various record alternatives to have a detailed and automated control of alerts. Taking advantage of Slack and Telegram as communication tools, we made the alarms visible through the platform and its mobile application for quick control and action in the event of detected anomalies. On the other hand, Pfsense was chosen as the Open Source Firewall as it is a tool that provides us with a web interface allowing us to configure it easily, it also has a package manager such as Squid, Snort, etc. Extending the functionalities just by selecting the package and Pfsense automatically downloads and installs it.

As a result of the implementation of the laboratories, recommendations are proposed so that a company can better choose the SIEM that fits its needs, budget and implementation time, taking into account the advantages of proprietary software vs. Open Source.

Keywords: SIEM, Open Source, Wazuh, LogRhythm

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

CAPITULO 1 - INTRODUCCIÓN

Hoy en día empresas de todos los sectores se enfrentan a un panorama en evolución de amenazas cibernéticas que son resultados de la crisis post Covid - 19, esto sumado a que en el 2021 quedó claro que el trabajo remoto llegó para quedarse, cada vez se evidencia que están poniendo en apuros a los equipos de seguridad de las empresas y estos equipos necesitan comprender y abordar rápidamente una ola de posibles riesgos de seguridad.

En lo que va de este año, el porcentaje de compañías amenazadas en el plano digital aumentó, haciéndose públicos muchos de estos ataques en todo tipo de empresas, pero como factor común es la falta de visibilidad de lo que pasa en una infraestructura y al preguntar si tuvieron ataques nos da como respuesta: No tuve incidentes de seguridad, como lo menciona Eset en su estudio Security Report Latam 2022 (Latinoamérica, 2022) (Pag. 6 incidentes de Seguridad reportados por empresas de América Latina en 2021 el 52% de las respuestas fue No tuve incidentes de seguridad); por esto hoy en día muchas empresas consultoras están decidiendo apostar por entregar a sus clientes sistemas de seguridad con visibilidad y flexibilidad para respuestas ante incidentes. Dentro de estas opciones resalta el SIEM, como una de las grandes apuestas entre los consultores.

Antecedentes

Hablar de Ciberseguridad no es algo nuevo, puesto que desde los años ochenta que comenzó a difundirse la red de redes, el mundo se ha visto envuelto en una serie de cambios en todas las áreas y lo más reciente y evidente fue la pandemia por Covid-19. Este hecho sin precedentes a nivel mundial causó el desarrollo inconmensurable y sin precedentes de las Tecnologías de Información (TI) y todo lo que conlleva. Hoy las TIC´s están generando efectos que nos han permitido adoptar nuevas maneras de trabajo, y determinando la forma en la que percibimos la realidad actual.

Debido a la creación, uso y popularidad de una enorme y nueva variedad de palabras, conceptos e ideas que ahora se debe manejar como por ejemplo en el caso de reuniones en ambientes virtuales, el teletrabajo y las comunicaciones por mensajería, han llegado a modificar nuestro lenguaje y percepción del entorno tecnológico en el que nos desenvolvemos. Es por esto por lo que con este documento esperamos profundizar sobre estos aspectos y conocer un poco más sobre la realidad que vivimos al hablar de la Seguridad de la Información e integrarlo con la Ciber Seguridad como un dogma que todos los expertos de TI lo lleven en la sangre y mostrar alternativas para usar sistemas de mensajería que además nos podría ayudar como complemento para responder ,as rápidamente ante incidentes de seguridad y a desenvolvernos de mejor manera con los nuevos retos que nos trae la sociedad humana actual, es decir, la «Sociedad de la Información» del Siglo XXI. (Install, 2020)

Por otro lado, es importante definir que es la Seguridad de la Información. Actualmente lo vemos como el área del conocimiento que consiste en mantener la información con 3 pilares primordiales, como son: confidencialidad, integridad y disponibilidad, así como de los sistemas, servicios y aplicaciones implicados en su tratamiento, dentro de una organización (Redacción, 2019). Es por esto la importancia de conocer a mayor detalle, cuales son estos 3 pilares que son lo primordial al momento de hablar de una arquitectura de seguridad.

Confidencialidad: Se la ve como privacidad, donde las políticas de la empresa se van a encargar de restringir el acceso a información sensible al personal no autorizado y garantizar que solo las personas autorizadas sean los únicos que podrán ver, acceder y modificar estos datos, esto garantiza la privacidad de los datos mediante la restricción del acceso, por ejemplo, con el cifrado de la información. (Ramirez, 2020)

Integridad: Es precisión, consistencia y confiabilidad de los datos durante su ciclo de vida, por lo que debe garantizar que la información sea precisa y confiable, por ejemplo, al

recuperar los respaldos de una base de datos, esta no debería sufrir cambios ya sea en fechas de creación o en el contenido de las tablas. (Ramirez, 2020)

Disponibilidad: Generalmente deben existir planes para recuperarse rápidamente ante desastres naturales o provocados por el hombre, y así garantizar que la información esté disponible a las personas autorizadas, por ejemplo, una base de datos ha sido comprometida, pero por mi política de respaldo tengo un backup con RTO y RPO=0 que me va a permitir continuar con la operación de la empresa sin retraso o perdida de información (Ramirez, 2020)

En 2005 Gartner acuñó el término “SIEM" en un reporte titulado “Mejore la Seguridad de IT con la Gestión de Vulnerabilidades” (helpsystems, 2018). Este término se encarga de unificar 2 conceptos, como son: Gestión de Eventos de Seguridad (SEM) y la Gestión de Información de Seguridad (SIM) (Rouse, 2017), para obtener lo mejor de ambos mundos. En este caso, SEM se encargará de monitorear y correlacionar logs o registros en tiempo real, mientras que en paralelo se encargará de alertar configuraciones y vistas de la administración relacionadas con esas actividades. Por otro lado, SIM se encargará de llevar los registros encontrados a otra fase incluyendo almacenamiento, análisis y generación de reportes de los incidentes encontrados. (Edwards, 2021)

Luego de varios años desde el primer reporte. Gartner redefine el concepto y lanza al mundo la gestión de eventos de seguridad e información (SIEM) esto apalancado por la necesidad del cliente de analizar datos de eventos en tiempo real y así pueda detectar oportunamente ataques dirigidos y violaciones de datos, sin dejar a un lado la recolección, almacenamiento, investigación y los informes sobre datos de los logs para dar una respuesta a incidentes, análisis forense. y cumplimiento normativo. En resumen, una herramienta que ayude a analizar y responder en tiempo real (Álvarez, 2020). Generalmente los datos de eventos se combinan con información contextual sobre usuarios, activos, amenazas y vulnerabilidades, pero hoy en día estas tecnologías proporcionan análisis en tiempo real de

eventos para monitoreo de seguridad, consultas y análisis de largo alcance para análisis históricos e incluyen machine learning para poder procesar el comportamiento de usuarios y dispositivos que se da a conocer como User and Event Behavioral Analytics UEBA. (Ramiro, 2017)

Estado del arte

Actualmente las infraestructuras tecnológicas presentan varios retos, por ejemplo: el crecimiento del volumen de datos, infraestructuras On-Premise y Cloud, sistemas heterogéneos y dentro de estos generalmente se presentan sistemas y aplicaciones legacy. Lo que convierte la implementación de sistemas de seguridad como un factor decisivo en los entornos de las empresas que utilizan recursos informáticos de TI para desarrollar sus labores del día a día ya que son parte de su giro de negocio. El análisis, control y visibilidad del gran volumen de datos hace una tarea compleja para las unidades de seguridad de las empresas, que debe actuar de manera inmediata y oportuna para poder mitigar un ataque y en el caso particular de Ecuador cumplir con regulaciones locales, como es el caso del EGSI 2.0 para empresas públicas (Electronico, 2020), la resolución jb-2012-2148 para entidades financieras (Ecuador, 2012) y la norma para la administración integral de riesgos de la SEPS SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI- 2022-002 para cooperativas de ahorro y crédito. (Solidaria, 2018)

Adecuar un plan de seguridad de la información que se adecue a las necesidades de todas las organizaciones no es una tarea sencilla, va a depender del segmento y del tamaño de la infraestructura de la empresa para la cual se esté desarrollando el plan de seguridad. Esta labor se complica cuando las empresas no cuentan con documentación sobre la implementación de las prácticas internas de seguridad o no poseen un área de seguridad, un oficial de seguridad, un centro de operaciones de la seguridad (Security operations center SOC) o personal con las capacidades para desempeñar funciones de un SOC.

El análisis de logs no es una tarea fácil, requiere bastante trabajo, conocimiento, y una amplia comprensión del entorno que se planea analizar, por lo que es necesario conocer y definir qué tipo de eventos puede considerados como tráfico normal, mientras que en otros sería una señal de alarma para la seguridad de la información. Estas complicaciones deben ser atendidas por personal que conozca la organización, especialmente cuando es necesario comprender el contexto de la operación de la empresa a la que se va a implementar el Security information and event management SIEM.

Las empresas pueden tener una infraestructura heterogénea con una enorme diversidad de dispositivos de diferentes fabricantes, donde cada fabricante crea sus propios formatos de bitácoras (logs). Por esta razón, los eventos que se generan pueden tener una cantidad de formatos y tamaños, una tarea titánica y casi imposible de hacerla. Por lo tanto, resulta evidente que garantizar la seguridad de la organización no es una tarea insignificante.

Con el contexto mencionado anteriormente, para ayudar al equipo de seguridad a manejar los eventos de seguridad registrados, se ha visto necesario la implementación de soluciones de manejo y correlación de eventos SIEM, que permitirá contar con una rápida capacidad de respuesta ante eventos, capacidad de automatización, escalabilidad e integraciones, cumplimiento de regulaciones locales o internacionales para la seguridad de datos y el monitoreo de infraestructuras On Premises y en la nube. Además, proveen de herramientas de análisis y retención de eventos online y offline aliviando la carga que enfrentan los especialistas en seguridad en su tarea de descubrir amenazas y dar tratamiento a los incidentes de manera rápida y oportuna.

Por otro lado, la implementación de un SIEM presenta otros retos que podrían entorpecer el despliegue correcto de la solución. Estos retos pueden ser muy sencillas como también complejas que podrían ser difíciles de escalar o mitigar, a modo resumen, seguir un

checklist como el siguiente que puede ser de gran utilidad si queremos implantar un SIEM con éxito.

- Evaluar las necesidades, recursos disponibles y el nivel de madurez de la empresa, con la finalidad de confirmar si una herramienta SIEM va a ser de utilidad para la visión que tiene la empresa.
- Utilizar herramientas que nos permita identificar la cantidad de eventos por segundo que se requiere correlacionar y los casos de uso que se podría implementar.
- Verificar los proveedores de SIEM, revisando pros y contras de cada uno de ellos para confirmar cuál de ellos se ajusta a las necesidades de la empresa una alternativa comúnmente usada es revisar los análisis de Gartner.
- Confirmar la disponibilidad de realizar una prueba de concepto (PoC) para conocer el producto a profundidad y saber si se ajusta a las necesidades de la empresa.
- Definir el alcance del proyecto con un set inicial de reglas que cubra las necesidades de detección que se han establecido inicialmente.
- Evaluar continuamente el funcionamiento del SIEM para incluir nuevas reglas de detección (casos de uso) lo cual redundará en una mejor postura de defensa de la organización.

Con estos puntos buscamos clarificar las adversidades que se pueden presentar en la implementación de un SIEM, como podrían ser; es demasiado complejo, el despliegue toma cierto tiempo para completarse, puede llegar a ser demasiado caro, posee integración pobre y genera mucho ruido si no está bien configurado.

Estructura del Documento

En este primer capítulo, se presenta la introducción sobre la investigación realizada, presentando los antecedentes que en Ecuador se han podido percibir con respecto a regulaciones locales, internacionales y la justificación que se planteó para entregar una solución tecnológica capaz de detectar rápidamente, responder y resolver amenazas en una infraestructura empresarial en tiempo real, se explora el estado del arte de las soluciones Security information and event management SIEM. Así como, la problemática actual y los objetivos que se va a cubrir con el presente proyecto, buscando resolver algunos de los problemas que se han identificado.

En el capítulo 2 se describe el marco teórico abarcando los puntos de SW libre y Software propietario, necesarios para el desarrollo del presente proyecto y posterior implementación de dos SIEM para poder evaluarlos. Por otro lado, se estudian diferentes ataques que podemos involucrar para entender el comportamiento y tipo de registros para indexarlos a la base de datos.

Durante el capítulo 3 se describen las herramientas SIEM seleccionadas y cómo fueron usadas al montar el laboratorio de pruebas para comparar estas soluciones y como se integran con otras tecnologías que fueron probadas.

En el capítulo 4 se presentan los resultados obtenidos para cada solución estudiada y los resultados de los ataques que se identificaron para luego plantear las fortalezas y debilidades a considerar a la hora de escoger una de las 2.

En el capítulo 5 se finiquita este proyecto con las conclusiones y el trabajo futuro a desarrollar.

Justificación del proyecto

Las necesidades de implementación de un SIEM en una organización en Ecuador regularmente están enfocadas al cumplimiento regulatorio de una entidad local. Sin embargo, lo ideal es que se trate de contar con una herramienta tecnológica que permita al equipo de seguridad de una empresa a ayudarles a la detección de incidentes de seguridad y dar respuesta oportuna a estos, sobre todo en ambientes donde el personal de seguridad tenga que manejar una gran cantidad de activos y de diferentes características.

Hace algunos años era frecuente que, en las auditorías al buscar registros de información, estos simplemente no existían debido a malas prácticas de almacenamiento y porque no se los consideraban relevantes, sin tener en cuenta la importancia que estos podían proveer. En muchos casos, esto era causa del fin de las auditorias puesto que existía suficiente información para investigar lo sucedido.

En Ecuador existen varias entidades que obligan a las empresas a cumplir regulaciones y estándares que tienen como objetivo el manejo seguro y adecuado de la información. Así como, el correcto uso de los recursos de TI.

En el caso particular del Esquema Gubernamental de Seguridad de la Información EGSI (Electronico, 2020), el cual es de implementación imperativa para todas las instituciones de Administración Pública, presenta el numeral 8.4 que menciona directamente al registro y monitoreo, requerimientos que hacen referencia a los registros generados por los dispositivos tecnológicos de las empresas públicas.

Para las entidades financieras la Resolución JB-2012-2148 en el numeral 4.3.8.15 menciona el almacenamiento por 12 meses de los registros históricos de todas las operaciones que se realicen en los canales electrónicos. (Ecuador, 2012)

Con estos 2 ejemplos se pone en evidencia que las empresas han comenzado a ver la importancia de los registros en entornos empresariales, dónde el cumplimiento de las regulaciones es de gran relevancia. En estos entornos las recomendaciones sobre el almacenamiento de los registros son muy valorados, y es impensable que se pierdan cuando los discos de los storage estén llenos.

Un especialista en seguridad de la información entiende la importancia de contar con registros de eventos. Sin embargo, la tarea de recopilar y examinar estos registros podría llegar a ser compleja, confusa y más aún, si el tamaño de la empresa hace que incremente el volumen de datos. Esto hace que sea imprescindible que se implemente una solución SIEM, pero generalmente esto acarrea más problemas, que es resultado de la poca planeación para implementarla, desconocimiento de herramientas SIEM del mercado, definir el alcance y las necesidades a cubrir y la falta de afinamiento de los casos de uso que resulta en más complicaciones que podría aumentar la carga de trabajo. Estos son los puntos que serán revisados en este proyecto.

Objetivos

El objetivo del presente proyecto consiste en dar pautas para escoger una alternativa de despliegue de un SIEM, ya sea con software Open Source o software Propietario que permitirá que estas tecnologías sean accesibles por todas las empresas que lo necesiten.

Esto se logró con la investigación de este tipo de soluciones SIEM, y mediante el despliegue de laboratorios que nos permitió verificar los aspectos positivos y negativos de las 2 opciones planteadas, que son comúnmente utilizadas en el mercado ecuatoriano. Además, permitirá viabilizar proyectos que permitan cubrir las necesidades de una empresa y que la inversión destinada para la adquisición de estas herramientas tecnológicas sea justificable.

Objetivo general:

- Conocer el mercado y alternativas de las soluciones SIEM a nivel mundial.
- Analizar funcionalidades, módulos, reconocer las fortalezas y debilidades entre las 2 opciones planteadas en este proyecto, con el objetivo de seleccionar e implementar una solución SIEM que se permita resolver las necesidades y problematicas reales de una empresa.

Objetivos específicos:

- Conocer las soluciones SIEM que son líderes en el mercado, características básicas, los casos de uso y diferencias entre Open Source y Propietario.
- Conocer los requisitos de hardware, software. Así como, los factores humanos y organizativos necesarios para una implementación efectiva que resolverá necesidades reales de una empresa.
- Desplegar laboratorios de pruebas con diversos sistemas operativos para clientes y servidores que serán monitoreados por las opciones de SIEM planteadas y de esta manera analizar el desempeño de cada solución para examinar las limitantes de cada una de ellas.
- Implementar funcionalidades adicionales en las soluciones SIEM además del análisis de vulnerabilidades, como es la integración con herramientas de comunicaciones empresariales para poder hacer seguimiento 24X7.

CAPITULO 2 - MARCO TEÓRICO

En el presente capitulo se presenta el sustento teórico del proyecto, tomando en consideración los conceptos necesarios para el entendimiento de todas las etapas involucradas en el proyecto, que van desde la implementación, desarrollo, resultados, discusión y conclusiones.

Security Information and Event Management (SIEM)

Un SIEM es una herramienta de seguridad informática, la cual es capaz de monitorear, detectar, analizar y bloquear posibles incidentes informáticos que pueden comprometer a la información y/o activos tecnológicos de una empresa a través de la correlación de diversos eventos de diferentes fuentes dentro de una red.

Dada la necesidad de visualizar el estado de la red y tener a salvo la información estas herramientas se han convertido en una solución indispensable en los centros de operaciones de seguridad (SOC) que tienen las empresas.

En la actualidad la tecnología de los SIEM para la detección y análisis de posibles amenazas involucra el uso de inteligencia artificial, basándose en el análisis del comportamiento a nivel de usuario o estado de la red, además de contar con motores de escaneo de vulnerabilidades para detectar incidentes que posiblemente aun no ocurran, razón por la que estas soluciones son catalogadas como las más robustas en cuanto a visualización de incidentes de seguridad informática se refiere.

La Inteligencia Artificial será un factor determinante en el futuro de SIEM, ya que proveerá de capacidades cognoscitivas que mejoraran las capacidades para la toma de decisiones ante una eventualidad. Por otro lado, permitirá a los sistemas adaptarse y crecer a medida que aumenta el número de usuarios de una empresa. Teniendo en cuenta IoT, la nube, los dispositivos móviles y otras tecnologías están incrementando la cantidad de datos que un

SIEM va a gestionar hace que la inteligencia artificial incremente el potencial de una solución para admitir más tipos de datos y una comprensión recursiva de las diferentes amenazas que evoluciona van evolucionando. (IBM, 2022)

Las fuentes de información con las cuales trabajan los SIEM son los eventos, registros o logs de todos los dispositivos activos de red, los mismos que son generados todo el tiempo incluso desde cuando el dispositivo se enciendo hasta que se apaga; esta información es recopilada, relacionada y analizada con el fin de promover y poner en marcha la detección de ciertos casos de uso que no son más que las reglas para determinar que incidente está siendo detectado en la red.

La posibilidad de contar con los registros de seguridad en una vista centralizada de la infraestructura de red es eficiente cuando estos registros pueden ser estandarizados. Es decir, a pesar de recibir cantidades exorbitantes de registros capturados desde diferentes fuentes o equipos que generen logs, toda esta información es normalizada en un formato más estándar a tal punto que el SIEM entienda y pueda monitorear, clasificar, correlacionar y llevar a cabo el análisis de un caso de uso específico que previamente se haya configurado en la herramienta. (helpsystems, 2018)

La implementación de este tipo de soluciones de seguridad informática se refleja expresamente en el costo que involucra obtener el software, hardware apropiados para garantizar el correcto funcionamiento de la misma, el licenciamiento de este tipo de herramientas se basa en el costo de eventos procesados y el software o aplicaciones complementarias que los diferentes SIEM ofrecen, así mismo, se debe considerar el costo del almacenamiento en discos de todos los eventos que fueron procesados en su momento, más sin embargo sigue siendo una buena inversión para las empresas implementar un SIEM básicamente por el beneficio de mantener una auditoria y seguridad informática en sus redes.

Capas de un SIEM

a) El parseo de logs basada en expresiones regulares: esta capa hace referencia a la separación de los diferentes campos o elementos que forman parte del log tomando en consideración las fuentes de información, las mismas que pueden ser cualquier elemento activo de la red como por ejemplo un IPS, IDS, Switches, Routers, Firewalls, etc.
b) La normalización: hace referencia a que en base al parseo de los campos o elementos del log, estos podrían ser analizados sin que afecte la forma en que los fabricantes generen los logs, ya que en muchos de los casos los campos de un log para un determinado dispositivo varían entre fabricantes.
c) La categorización: en esta capa se ordena y clasifican los logs dependiendo a prioridad que se establece para los diferentes casos de uso; en este punto cabe señalar que aquí es donde se puede identificar qué tipo de log es, como por ejemplo un login con éxito o un login fallido, etc.
d) La agregación: esta capa hace referencia a la agrupación de diferentes logs obtenidos en un periodo de tiempo definido.
e) El filtrado: si bien es cierto todos los logs contienen información vital en cuanto a los eventos que están pasando en la red, así mismo no todos estos eventos son relevantes, por lo que en esta capa se filtran los logs que dependiendo de los casos de uso se los puede o no tomar en consideración para realizar la correlación. (Bertolín, 2019)

Log o Registros de eventos

Los logs o también llamados eventos del sistema son registros de información proveniente de equipos y/o sistemas informáticos que muestran el historial y por ende el comportamiento de estos equipos, este flujo de información es almacenada en directorios específicos dependiendo del tipo sistema operativo del equipo, para su posterior análisis.

La revista Forbes menciona en su nota “Why users should care about application Logs” lo siguiente:

> También conocidos como archivos de registro, registros del servidor, registros del servidor web o simplemente registros de datos simples, estos son los fragmentos de información que un servidor o sistema de software creará automáticamente para detallar la lista de acciones y eventos que se han realizado o registrado. (Bridgwater, 2015)

El procesamiento y análisis de los Logs generan mucho valor para los negocios, tanto a nivel del adecuado funcionamiento de los sistemas, pero también a nivel de objetivos del negocio, de donde se puede listar las siguientes ventajas:

- Implementar el uso de técnicas de machine learning con el fin hallar información relevante para una mejor toma de decisión.
- Desarrollar una mejor administración, gestión y control de esta información, para con ello aprovechar de mejor manera estos datos.
- Detectar amenazas en los sistemas y poder actuar para mitigar el problema.
- Prevenir fugas de información, así como comportamientos inadecuados que causen errores.

El log o registro de los eventos es la información de más bajo nivel que es generada y reportada por los diferentes dispositivos activos de red o aplicaciones como por ejemplo un Firewall, Switch, Sistemas operativos, etc.

La información que es encontrada en un log es parametrizada en fecha y hora acorde a las acciones o eventos que el usuario o el mismo dispositivo realiza, por lo que en un log se puede visualizar desde cuando se encendió o apaga el dispositivo, así también como los problemas o fallos que el mismo sistema registra mientras está operativo, con ello se puede

llegar a tener una auditoria total en el sistema o dispositivo; por lo general se necesita de una investigación adicional para llegar a la causa raíz del problema.

Poniendo en consideración que si es un sistema operativo o dispositivo de red, la información que se muestra en el log es diferente, por lo que está implícito que para cada dispositivo el formato de la información varia incluso entre fabricantes y de igual forma la ubicación en donde se almacenan estos archivos es diferente a pesar de que existe una normalización llamada SYSLOG, la cual habla de estandarizar el formato de los logs, es muy común que los fabricantes tengan sus propios lineamientos para generarlos.

Tipos de logs

a) Informativos: son logs que permiten visualizar al usuario o administrador que ha ocurrido algo en el sistema, como por ejemplo si se reinicia el equipo forzosamente o si se lo apaga por mantenimiento; ese tipo de información que netamente informativa.
b) Depuración: son logs expresamente propietarios de los aplicativos y ayudan a los desarrolladores a identificar problemas con el código del aplicativo.
c) Advertencia: en este tipo de logs se muestra información de advertencia con el fin de mostrar al usuario que el aplicativo no está funcionando correctamente.
d) Error: muestran los errores que se producen en el sistema operativo, por ejemplo, cuando el sistema no encuentra la dirección de memoria para escribir en disco, volcado de memoria, etc.
e) Alerta: en un log de alerta se indica que algo interesante ha sucedido y generalmente están en el dominio de los dispositivos de seguridad informática como por ejemplo los logs de un Firewall, IPS, IDS, etc.

Dentro de los tipos de logs que los sistemas pueden generar se tiene la criticidad o prioridad con la que el usuario, administrador o desarrollador debe tratar este tipo de información, con lo que se tiene 3 prioridades de los logs:

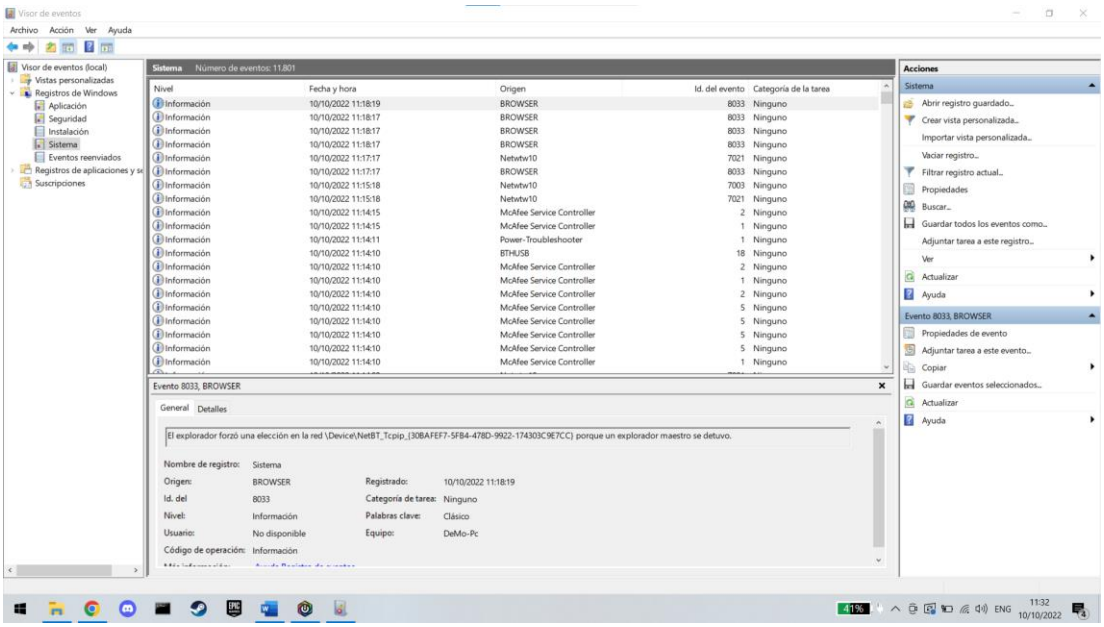
a) Baja: en esta categoría están los eventos que son netamente informativos y no necesitan ser investigados de forma inmediata, por lo que normalmente son solo almacenados.

b) Medio: Estos eventos requieren ser considerados en un análisis de carácter oportuno, pero no inmediato.

c) Alta: este tipo de logs son los de prioridad alta, es necesario que tengan una intervención inmediata para llegar a la causa efecto del hecho. (Díaz Lima, 2018)

Figura 1

Visor de eventos Microsoft Windows

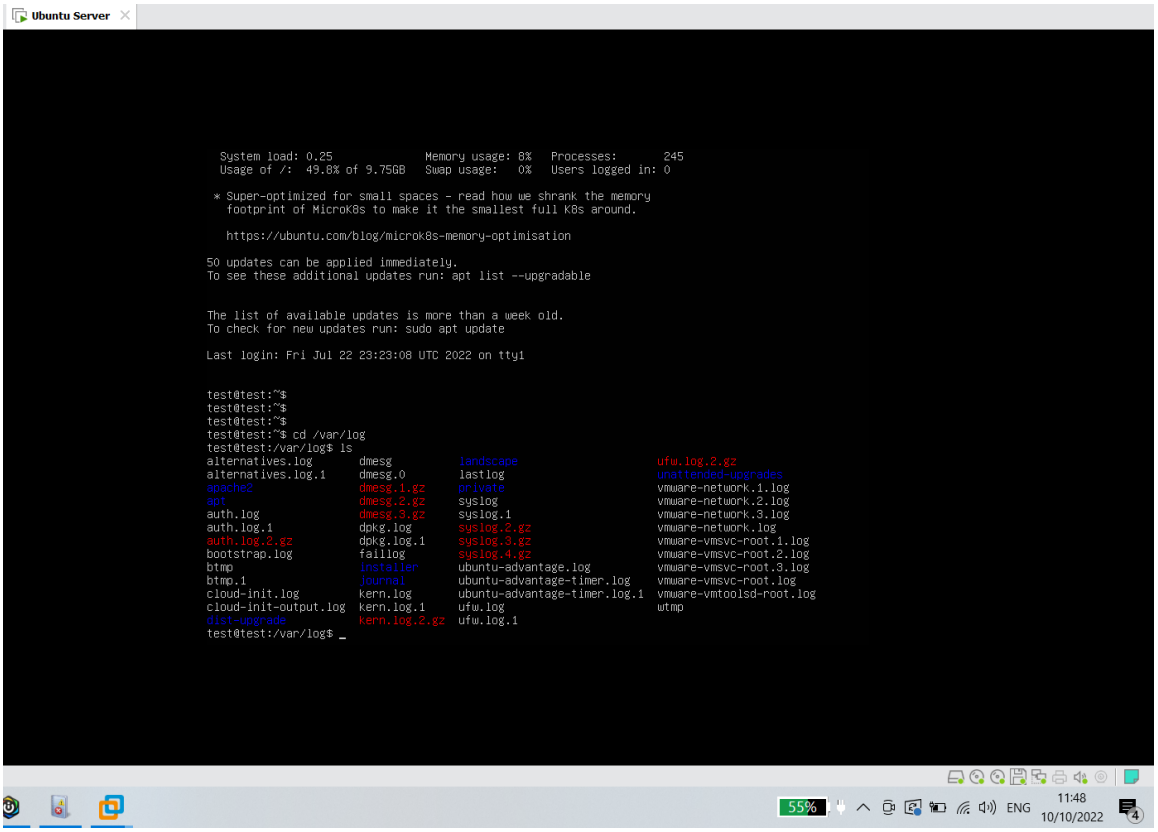


Nota. El gráfico es un ejemplo del Visor de eventos donde se puede ver los registros de actividad de diferentes aplicaciones como el inicio de una sesión proceso o configuración del sistema.

En los sistemas operativos Microsoft Windows se puede encontrar este tipo de información en “eventos del sistema” los cuales se muestran a través del visor de eventos del sistema y cada evento tiene una serie de campos que definen el evento desde la fecha cuando sucedió como su categoría, criticidad y el tipo de información (ver figura 1.)

Figura 2

Ubicación log sistemas Linux



Nota. Los registros o logs se almacenan en una ubicación específica, en el caso de Linux tenemos esta imagen que muestra las rutas del sistema operativo y donde se encuentra /var/log.

Hablando de sistemas Linux, los logs están ubicados en el directorio /var/log y cada aplicación guarda en ese mismo directorio sus registros (ver figura 2); para estos sistemas los logs son archivos en texto plano y accesibles mediante cualquier herramienta para ver o editar texto, lo que no pasa en los sistemas Windows que solo se pueden ver a través de su herramienta visor de eventos.

Recolección de logs

La recolección de logs más común es mediante el protocolo Syslog, este protocolo es usado principalmente en sistemas Unix y Windows mediante una comunicación TCP o UDP, dependiendo de la necesidad o de cómo se configure el envió y recepción de estos mensajes.

En los sistemas Windows se ha implementado su propio sistema de logging para Windows, Windows Event Log, sin embargo, existen aplicaciones que cambian el formato de los logs de Windows Event a Syslog debido a que este protocolo es más común.

Otra forma de recolección de logs es mediante el protocolo SNMP, el cual se basa en "trap" y "polling", este protocolo usa trap cuando el dispositivo necesita informar de un cambio al dispositivo gestor o mejor llamado servidor y en cambio el uso del polling se basa en la solicitud de información desde el dispositivo gestor.

Otro de los mecanismos de recopilación de logs, son la instalación de agentes que se encargan de reenviar y centralizar los datos de los logs, estos agentes se encargan de la monitorización de los archivos de logs o de las ubicaciones que se especifiquen, además también tiene la función de recopilar los eventos de los logs y reenviarlos al servidor de recopilación y análisis.

Software propietario

Es el software en el que sus funcionalidades, características y operatividad se debe a un costo y/o planes de licenciamiento de forma obligatoria, en otras palabras, existe una persona o entidad que posee derechos sobre el software y que limita el libre uso, la posibilidad de analizarlo, de incorporar mejoras, de publicar los resultados del análisis o de distribuirlo libremente. (Llamas, 2022)

Características software propietario

a) Atención al cliente: consiste en que la persona o entidad con los derechos de autor del software provea o incluya en el licenciamiento una atención y soporte especializado para el uso, actualización y mantenimiento si es que el software lo requiere.
b) Especialización y focalización: consiste en brindar al usuario final una capacitación en cuanto al uso y manipulación de ciertas funcionalidades de la herramienta, esta es una característica que puede ser considerada como valor agregado con la adquisición del licenciamiento.
c) Control: consiste en establecer una auditoria en favor al propietario con el fin de hacer un control al uso malintencionado y fraudulento o no ético del software.
d) Compatibilidad: consiste en que este tipo de software es desarrollado para gran parte del hardware existe en el mercado mundial, por lo que se tiene una mejor experiencia para el usuario final.
e) Diseño: consiste en que el equipo de desarrollo tiene como propósito brindar un software amigable y eficiente; en esta característica influye mucho que potencial cliente vea interfaces sólidas y funcionales, ya que en el mercado existen variaciones que pueden ser decisivas para adquirir o no el licenciamiento.

Que es SW Libre

Como lo menciona Julia Uriarte, el Software Libre describe a los programas informáticos que permiten a sus usuarios las facultades de copiar, modificar, personalizar y distribuir libremente el código fuente de su programación, bajo la autorización explícita de sus autores originales, creando múltiples versiones mejoradas y personalizadas. (Uriarte, 2019)

El Software Libre no es un símil de gratuidad, si bien varias de las versiones del software lo son, o su costo únicamente equivalente a su distribución y no al pago de sus derechos de autor. Y que la definición del término en inglés Free Software (“Software Libre”),

conduce a la ambigüedad respecto al sentido de dicha libertad. Sin que esto implique que el software sea gratis, sino la libertad respecto a restricciones de derechos de autor, permitiendo su modificación y mejoramiento por sus propios usuarios. (Uriarte, 2019)

Es así que en el software libre se caracteriza por cuatro libertades fundamentales, según los preceptos originales de Richard Stallman:

- Libertad de uso. Permite a los usuarios el uso del programa con cualquier fin.
- Libertad de estudio. Se da la posibilidad de entender cómo opera el programa y poder modificar el código fuente según sus propios deseos y necesidades.
- Libertad de distribución. Permitir la entrega de copias libremente del programa.
- Libertad de mejoría. Permite modificar el programa, corregir errores y proponer mejorías y soluciones.

El Software Libre puede resumirse en las siguientes ventajas:

Trabajo en comunidad. Permite la colaboración entre varios usuarios para la corrección, desarrollo y perfección del software, atacando directamente los inconvenientes que presente sin necesidad de esperar que los autores originales liberen una versión corregida u actualizada.

Superación de la piratería. Se evita la censura de la distribución y copia del Software, por los derechos autorales del titular, apostando por otro tipo de modelo colocando a disposición de los usuarios el software original o versiones mejoradas por la comunidad.

Profundización del conocimiento informático. La colaboración de los usuarios en el desarrollo, mejoramiento y corrección de problemas, permite que continuamente aprendan del software y su código a medida que lo intervienen, y compartan conocimiento con otros miembros de la comunidad permitiendo que todas las partes involucradas sumen conocimientos.

Ahorro. Los usuarios que utilizan software libre no tienen la necesidad de adquirir licenciamientos periódicos para el uso del software, lo cual permite que se pueda enfocar esos recursos ahorrados en otro tipo de necesidades, sin tener que pagar derechos de uso, sino pagar servicios con la misma empresa que desarrollo el software. (Uriarte, 2019)

El Software Libre posee sus desventajas, entre las que se puede mencionar:

Carece de garantías. El uso de software libre es de responsabilidad completa y única del usuario final, puesto que no existe un pago de derechos autor, por lo que este tipo de software es de uso para usuarios con conocimiento técnico.

Exige esfuerzo individual. Pese a que en la comunidad de software libre se encuentren varias versiones del software que corrijan algún inconveniente o proporcionen algún tipo de actualización o mejora, el ajuste a acontecimientos y requerimientos puntuales dependerán del usuario final de cada caso de uso.

Mayor conocimiento. La manipulación de este tipo de software requiere de un conocimiento no común y más bien técnico. (Uriarte, 2019)

Que es un Firewall / IPS

A medida que las redes informáticas fueron creciendo surgió la necesidad de brindar seguridad a la información que usaba dichas redes en el funcionamiento diario, es así que fueron naciendo dispositivos y elementos de red dedicados a la seguridad de las redes.

El lanzamiento en 1984 del sistema de detección de intrusos (IDS) por SRI International, marcó por primera vez el desarrollo de una herramienta de seguridad de red donde se incluía detección en tiempo real de ataques en curso. Esto permitió a los profesionales de TI responder a dichos ataques, mitigando sus efectos en los dispositivos y usuarios de red. El sistema IPS, que significa sensor de prevención de intrusiones, se implementó como reemplazo

del sistema IDS a fines de la década de 1990, permitiendo detectar actividad maliciosa y bloquearla automáticamente en tiempo real.

Luego de las soluciones IDS e IPS se desarrollaron los elementos de red conocidos como firewalls los cuales tenían la funcionalidad de filtrar el tráfico y prevenir el ingreso de tráfico no deseado a ciertos segmentos de red. Digital Equipment Corporation (DEC) en 1988 desarrollo el primer firewall de red, el cual era un filtro que inspeccionaba los paquetes de datos para verificar que coincidieran con conjuntos de reglas predefinidos, donde la opción de descartar o reenviar los paquetes estaba disponible. Sin embargo los firewalls de filtrado de paquetes examinan cada paquete individualmente; sin importar si el paquete es parte de una conexión existente. AT&T Bell Laboratories en mejora a los firewalls de paquetes implemento el primer firewall de estados (stateful) en 1989, el firewall de estados al igual que los firewalls de filtrado de paquetes, utilizan reglas predefinidas para permitir o denegar el tráfico, con la diferencia que los firewalls de estados rastrean las conexiones establecidas y determinan si un paquete pertenece a un flujo existente de datos, ofreciendo una mayor seguridad y un procesamiento más ágil.

Con el tiempo los firewalls originales que eran aplicaciones de software agregadas a los dispositivos de red como los enrutadores, fueron siendo implementados por varias empresas en elementos de red autónomos y dedicados únicamente para las funciones de firewall. (Ariganello, 2013)

Tipos de ataques

Vulnerabilidad

Se las conoce como puertas abiertas para posibles ataques, “son debilidades o fallas en cualquiera de los ambientes que se maneja la parte informática, ya sea software, hardware o en las personas que trabajan con estas tecnologías” (Mieres, 2009)

Ataque informático

"Consiste en aprovechar las vulnerabilidades que los sistemas poseen para obtener beneficios, en la mayor parte económicos, afectando negativamente en los sistemas, datos, operatividad de las empresas víctimas" (Mieres, 2009). Este tipo de ataques se clasifican en 3 categorías:

Phishing. "Se denomina phishing al tipo de ingeniería social utilizado por los atacantes para robar datos. Por lo general se extrae información como: contraseñas o números de tarjetas de crédito" (Bello, 2021).

Whaling. "En el Whaling así como en el Phishing se realiza un ataque de ingeniería social, enfocado en perfiles de altos directivos como CEOs. El objetivo continúa siendo extraer datos importantes de las víctimas, pero en este caso tener acceso a la información delicada que los directivos manejan" (Bello, 2021).

Malware. "Se utiliza el termino malware para identificar los programas o códigos maliciosos creados para introducirse en sistemas informáticos e invadirlos o dañarlos" (Bello, 2021). Dentro del malware se incluyen software malicioso como:

Ransomware. "Este malware se basa en cifrado de datos importantes o realizando el bloqueo de funciones esenciales como inicio de sesión, mientras que, los atacantes exigirán una recompensa, en muchas de las ocasiones económica, a cambio del 'rescate' de la información que en la mayoría de los casos no es recuperada" (Suastegui Jaramillo, 2022).

Gusano. "Es un malware enfocado en el ataque a redes. Cuando estas se encuentran infectadas con gusanos, el malware se replica a todos los componentes de la red comprometida" (Suastegui Jaramillo, 2022).

Troyano. “Se denomina troyano gracias a la historia del caballo de troya, en este caso el malware es disfrazado como un recurso deseable o útil para que la víctima lo instale y así atacar su sistema” (Suastegui Jaramillo, 2022).

Web Attacks

Inyección de SQL. “Es un método de infiltración de un código intruso que se aprovecha de vulnerabilidades comunes en páginas web. En este tipo de método los atacantes pueden realizar consultas SQL a través de campos de ingreso de texto que no están debidamente controlados, accediendo a la aplicación a través de comandos con los que se puede tener paso a la base de datos” (Bello, 2021).

Herramientas de comunicación empresarial

“Internet se ha convertido en una herramienta esencial para las comunicaciones empresariales, todo tipo de empresas, grandes medianas o pequeñas han implementado en sus estrategias de comunicación diferentes herramientas que internet ofrece, sea a través de redes sociales, páginas web tradicionales o blogs” (Marín Dueñas & Gómez Carmona, 2021).

Telegram

“Aplicación de mensajería instantánea, dedicada principalmente a la comunicación mediante texto, mensajes de audio, llamadas o videollamadas con cifrado end to end. Permite crear grupos y supergrupos, privados y públicos, enviar imágenes, videos, audios y documentos de cualquier tipo” (López, 2020).

Slack

“Se posiciona como una de las mejores opciones para la comunicación continua y en tiempo real de equipos de trabajo. Utilizando esta herramienta las personas pueden trabajar de forma conjunta y efectiva, dentro de un entorno seguro de nivel empresarial. Permite conexiones con Google Workspace o Microsoft Office 365 para compartir directamente

documentos desde la nube y trabajar en línea en conjunto con grupos de trabajo” (Escobar Restrepo, 2021).

CAPITULO 3 - DESARROLLO DEL PROYECTO

Al revisar varias opciones para poder entregar visibilidad y control de la infraestructura se requiere evaluar las soluciones SIEM, para esto se implementó un laboratorio virtual, en el que se instaló máquinas virtuales sobre Vmware ESXi con diversos sistemas operativos que simulan los activos de una arquitectura típica de una red corporativa.

La implementación de este laboratorio tiene como objetivo integrar el SIEM con todos los elementos activos disponibles en una arquitectura de red.

Comparativa entre diferentes SIEM

Para la elección de un SIEM se debe considera las características que se necesiten controlar y los casos de uso necesarios. Generalmente las organizaciones no tienen definido los casos de uso de los SIEM y solicitan uno con todas las características y funcionalidades posibles, pero que no se adecuan a las necesidades de la empresa.

Por otro lado, la razón principal por las que a menudo se opta por el desarrollo de un SIEM propio es debido a los altos costos que tienen los SIEMs comerciales. El objetivo es tratar de equilibrar la balanza de las necesidades de las empresas, ¿Tenemos una gran infraestructura y necesitamos todas las funcionalidades posibles y la mayor fiabilidad? Si se trata del caso de una empresa con gran infraestructura, la mejor opción y lo más aconsejable sería optar por un SIEM comercial.

Es mandatorio, que al adoptar este tipo de tecnologías, esta cumpla con los intereses empresariales, que no afecte a la operación, rendimiento y almacenamiento de la infraestructura actual, la solución deberá brindar un buscador de eventos ágil y flexible, es decir el dashboard donde permita visualizar los eventos y alertas deberá ser intuitivo y deberá permitir la generación de informes.

En la actualidad existe gran diversidad de soluciones SIEM en el mercado de ciberseguridad, teniendo así soluciones de pago y open source; las soluciones de pago prácticamente son las más populares por la profundidad de análisis que brinda al usuario, mientras que las open source tienen características limitadas.

Para abordar de manera más ágil la comparativa de sistemas SIEM nos basaremos en los sistemas más populares. Lo primero que vamos a mostrar es el Cuadrante Mágico de Gatner para los sistemas SIEM, publicado en abril 2021 y nos centraremos en los que se muestran como líderes como lo muestra la figura 3.

Figura 3

Gartner Security Information and Event Management (SIEM) 2021

Nota. Gartner es una empresa multinacional encargada de evaluar diferentes tecnologías, que sirve como una guía mostrando pros y contras de soluciones catalogadas a nivel mundial y que permite a los usuarios tener una visión amplia para elegir una solución tecnológica.

En el anterior cuadrante se puede observar que los sistemas SIEM líderes son Exabeam, QRadar (IBM), Splunk, LogRhythm, Securonix y Rapid7, aunque en el territorio ecuatoriano además de los mencionados se ha trabajado con AlientVault, ArcSight y RSA Netwitness.

En la siguiente comparativa, se añadirá un nuevo producto Open Source como es Wazuh el cual fue caso de uso durante la maestría de Ciberseguridad y que puede llegar a tener similares características.

QRadar (IBM)

QRadar es un SIEM de la empresa IBM, con componentes adicionales como gestión de logs, monitorización de la red, gestión de vulnerabilidades y gestión de riesgos.

Tabla 1

Ventajas y desventajas QRadar.

Ventajas	**Desventajas**
Se adapta a medianas y grandes organizaciones. Arquitectura flexible que soporta varios entornos. Solución disponible como física o virtual, centralizada o distribuida, también puede ser “on cloud” o cogestionada con partners de IBM QRadar.	No integra monitorización de clientes finales (SO) (endpoints), necesita plugins de terceros. Buen motor de búsqueda, aunque competidores como Splunk y LogRhythm lo mejoran.
Posibilidad de conectar al SIEM seguridad de terceros.	La herramienta de respuesta a incidentes (IBM Resilient) no es nativa y debe conectarse a través de la herramienta de conexión de terceros.
Buen sistema de monitorización en tiempo real e histórico.	El licenciamiento es confuso

Splunk

Splunk cuenta con dos opciones, la solución completa con el sistema SIEM y dos soluciones añadidas para nivel premium que es el ESM que se encarga de analizar casos de uso y en conjunto con la solución de UEBA mejorará el análisis de las consultas realizadas integrando inteligencia a nivel de comportamiento de los usuarios.

Tabla 2

Ventajas y desventajas Splunk.

Ventajas	**Desventajas**
El SIEM con el añadido (UBA) presenta un magnífico motor de búsqueda. Podría ser el mejor junto con LogRhythm.	Elevado precio de licenciamiento.
Es un producto apreciado por los clientes.	Splunk no ofrece una versión Appliance, se debe instalar sobre hardware soportado.
Posee una buena cantidad de empresas asociadas, que ayuda a la implementación de estas herramientas en otras organizaciones.	
Posee una gran integración 0con otros sistemas de Ciber Seguridad, puede usar casos de uso predeterminados, lo que facilita la gestión de la respuesta ante incidentes de los equipos de seguridad.	

LogRhythm

LogRhythm consta de varios componentes, la distribución permite trabajar en conjunto sobre un appliance o si es necesario sobre una arquitectura distribuida lo que hace una solución flexible ante cualquier infraestructura o cliente.

Tabla 3

Ventajas y desventajas LogRhythm.

Ventajas	**Desventajas**
Es una plataforma sólida y escalable desde un solo dispositivo hasta arquitecturas de n niveles.	Difícil integración con soluciones de terceros. APIs menos abiertas a terceros que sus competidores.
Poderosa interfaz de usuario que provee una gran experiencia para el monitoreo en tiempo real.	Dificultad de escalado para soportar volúmenes de eventos muy altos.
Complementa actividades de respuesta ante incidentes de seguridad de manera automática y manual.	
Buen modelo de implementación y soporte a través del servicio de implementación central.	
Muy adecuado para entornos ICS/SCADA	

Securonix Next-Gen

Securonix Next-Gen SIEM presenta una propuesta enfocada a reducir los falsos positivos y a monitorear las amenazas de usuarios y entidades en toda la empresa enfocados en 3 pilares; Puntuación de riesgos, Análisis de casos de uso estándares y el uso de modelos de cadena de amenazas aplicándolos a los marcos de MITRE ATT&CK y US-CERT.

Tabla 4

Ventajas y desventajas Splunk.

Ventajas	**Desventajas**
Desde una única plataforma ayuda perfectamente a detectar y responder a amenazas de seguridad avanzadas.	Automatización/Playbooks no funcionan. Es importante que estas características funcionen para que los equipos de respuesta a incidentes puedan automatizar tareas repetitivas.
Posee una inteligencia artificial robusta, que es casi perfecta en términos de detección de ataques, y sus herramientas poderosas y eficientes, que ayudan a los analistas de seguridad a investigar y responder a los problemas.	Algunos campos derivados en los registros de eventos tienen nombres vagos, es difícil determinar qué información se extrae sin comprender cómo se analizan los registros de eventos.
El servicio al cliente es rápido y eficiente para resolver cualquier dificultad que los consumidores puedan tener.	El rendimiento puede ser dolorosamente lento a veces, lo cual es inaceptable en el caso de un incidente de seguridad crítico.

Exabeam Fusion

Exabeam es una solución que permite visualizar y combatir los posibles incidentes de ciberseguridad añadiendo a sus componentes existentes como a sus componentes como SIEM, XDR y data lake el complemento que es capaz de analizar el comportamiento del usuario basado en inteligencia artificial y machine learning, haciéndola una herramienta que va

a la par con la tecnología de punta vigente; capaz de detectar usuarios comprometidos y maliciosos.

Tabla 5

Ventajas y desventajas Exabeam Fusion.

Ventajas	**Desventajas**
Permite una implementación tanto on premise como en la nube.	La configuración para nuevos casos de uso es poco entendible.
Tiene la compatibilidad de proporcionar el servicio en plataformas SaaS.	En cuanto a reportes depende mucho de sus otros complementos.
Posee una arquitectura escalable la cual está basada en Elasticsearch y Hadoop (HDFS).	De difícil manejo.
La plataforma permite orquestación y respuesta ante posibles incidentes.	Funcionamiento pobre en casos de usos complejos.
Tiene el complemento de Advanced Analytics basado en UEBA.	

Rapid7 InsightIDR

InsightIDR es capaz de identificar el acceso no autorizado de las amenazas tanto externas como internas, así como la actividad sospechosa para que no tenga que examinar miles de flujos de datos. Sus características principales son: Detección y respuesta de endpoint (EDR), Análisis del comportamiento de usuarios y entidades (UEBA), Alineación MITRE ATT&CK®, entre otras.

Tabla 6

Ventajas y desventajas Rapid7 InsightIDR.

Ventajas	**Desventajas**
La plataforma hace un buen trabajo proporcionando detalles para ayudar a investigar una alerta	Muchos de los servicios más útiles requieren un complemento adicional, por ende, más dinero.
La plataforma hace un buen trabajo integrándose con otras plataformas como Darktrace para ayudar a proporcionar una mayor visibilidad	Casi ninguno de los complementos que se requiere está disponible con la versión base
A diferencia de otras plataformas, IDR no produce una cantidad abrumadora de falsas alarmas	La consola de búsqueda de registros es mejor que muchos otros productos líderes, pero aún tiene cierto margen de mejora, a veces resulta difícil encontrar registros sobre fuentes de eventos específicas. Necesita tener más opciones para personalizar y suprimir registros no deseados. -Debería tener algún tipo de soporte para Kubernetis y entorno Linux también.

Wazuh - The Open Source Security Platform

Wazuh es una plataforma gratuita y de código abierto de correlación de eventos, usada para prevenir, detectar y responder de manera rápida y oportuna ante incidentes de seguridad. Posee capacidades para integrarse con distintas cargas de trabajo ya sea en entornos on-premise, nubes, virtualizados y en contenedores.

La plataforma Wazuh cuenta con opción de monitoreo sin agentes y de requerirse mayor información se puede desplegar agentes para puntos finales, que se despliega desde los sistemas a supervisarse, y el servidor de administración, el cual recoge y analiza los datos enviados por los agentes, sus funciones destacadas tenemos: Detección de vulnerabilidades, respuesta a incidentes, cumplimiento normativo ISO27001, PCI DSS, GPG13 o GDPR.

Tabla 7

Ventajas y desventajas Wazuh.

Ventajas	**Desventajas**
Facilidad de implementación y comienzo con la interfaz de usuario web común con paneles preconfigurados	La utilización de recursos del lado del servidor es pesada
Función de búsqueda flexible	Complejo manejo/configuración de archivos yaml
Wazuh ayuda a minimizar los esfuerzos de recopilación y el monitoreo diarios de los registros del servidor para más de 10 servidores con las mejores capacidades de generación de informes listas para usar	
Excelente opción si se necesita satisfacer la necesidad de ciberseguridad de una organización sin mucho costo y con muy buen soporte de la comunidad de usuarios	

Fase de reconocimiento

Para el caso de estudio se plantea 2 escenarios de acuerdo con lo revisado en el apartado de comparativas donde se plantea revisar un sistema Open Source y un sistema Propietario.

Arquitectura Propietario

Para el presente caso de estudio, se utilizarán como fuentes de datos (eventos) a los dispositivos y aplicaciones que se consideran las más importantes y esenciales dentro de una red corporativa como se visualiza en la tabla 8.

Tabla 8

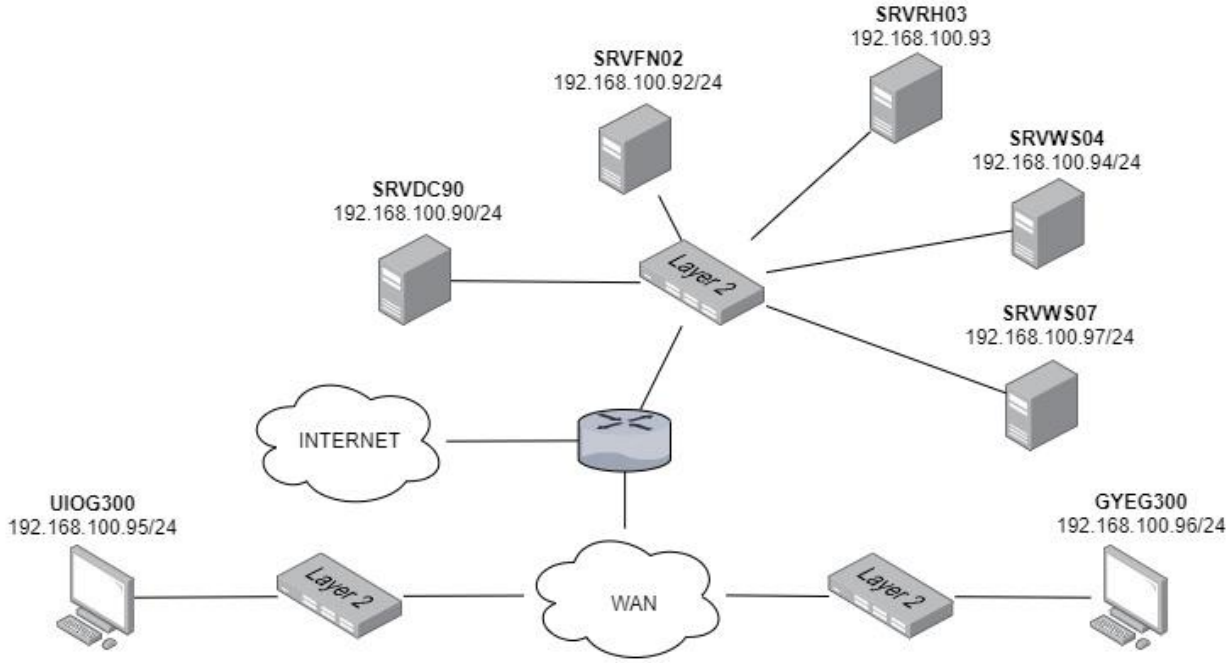
Activos de una infraestructura empresarial.

S.O	HOSTNAME	IPADRESS	GATEWAY	ROL
Windows Server	SRVDC90	192.168.100.90	192.168.100.1	DOMAIN CONTROLLER ACTIVE DIRECTORY DNS DHCP
Windows Server	SRVFN02	192.168.100.92		FILE SERVER
Windows Server	SRVRH03	192.168.100.93		HOME SERVER
Windows PC	UIOG300	192.168.100.95		Workstation PC
Windows PC	GYEG300	192.168.100.96		Workstation PC
Linux Server	SRVWS04	192.168.100.94		WEB SERVER
Linux Server	SRVWS07	192.168.100.97		WEB SERVER

El diagrama de red planteado para el análisis de este proyecto corresponde a la figura 4

Figura 4

Estado inicial de la red empresarial

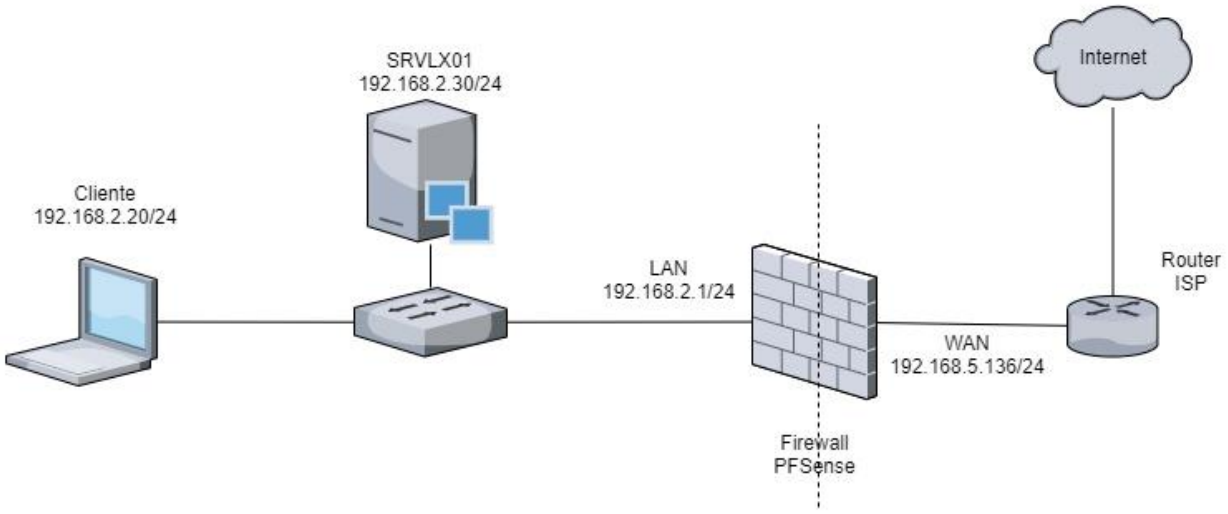


Nota. Diagrama de red de la empresa, se muestra direccionamiento IP de cada uno de los servidores con los que se cuenta al inicio de este análisis.

Arquitectura Open Source

Figura 5

Arquitectura Open Source



Nota. Arquitectura de red propuesta para el analisis de un ambiente con sistemas Open Source.

Tabla 9

Activos Siem y Firewall Open Source.

S.O	HOSTNAME	IP ADDRESS	GATEWAY	ROL
FreeBSD	PFSENSE	192.168.2.1	192.168.5.136	FIREWALL
Ubuntu Server	SRVLX01	192.168.2.30	192.168.2.1	SERVER LINUX
Windows PC	CLIENTE	192.168.2.20	192.168.2.1	CLIENTE

Fase de diseño

Para poder simular la integración de las versiones de tecnologías SIEM en un entorno real, vamos a desplegar agentes como recolectores de datos para los sistemas operativos comúnmente encontrados en los centros de datos.

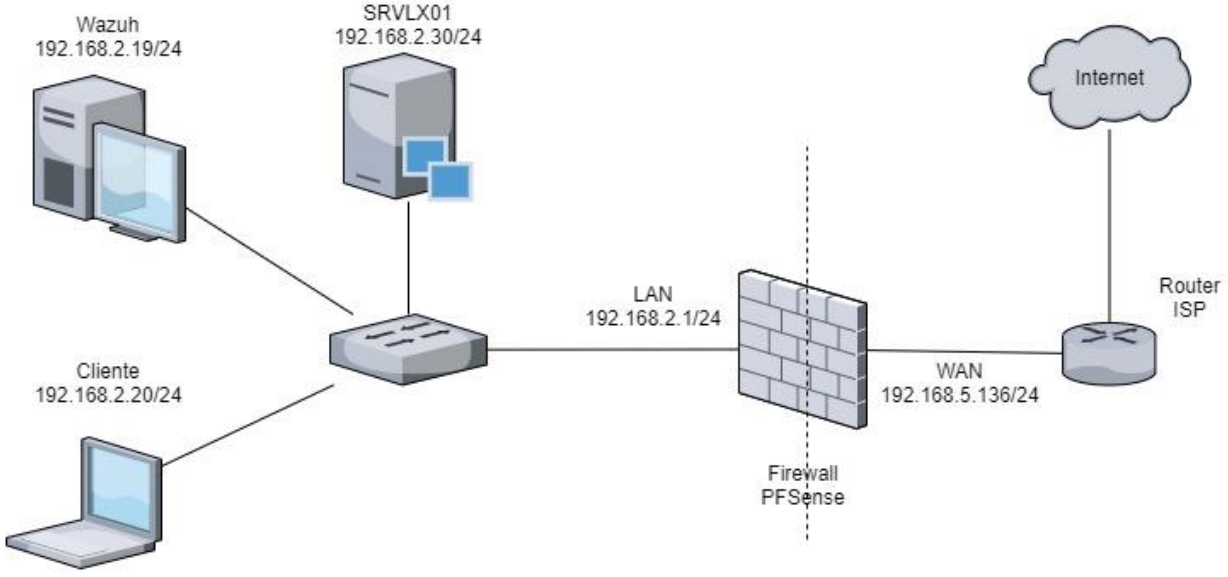
Las máquinas virtuales que vamos a utilizar como activos generadores de eventos durante la instalación fueron seleccionados pensando en ambientes comúnmente usados en una infraestructura empresarial, por lo que se implementaron los sistemas operativos actuales, Windows (.msi) y Linux (.deb).

Diseño SIEM Open Source

La arquitectura de red propuesta tiene un dispositivo de seguridad perimetral open source y se planea un laboratorio diferente (ver figura 6) en el que se tiene como fuentes de información el equipo de seguridad perimetral (Firewall), el servidor Linux y un cliente Windows, los cuales proporcionaran todos los eventos generados por los dispositivos de la red al SIEM, teniendo así la tabla 10.

Figura 6

Arquitectura SIEM y Firewall Open Source



Nota. Diagrama de red donde se incluye un Sistema de Correlación de eventos Open Source Wazuh.

Tabla 10

Activos Siem y Firewall Open Source.

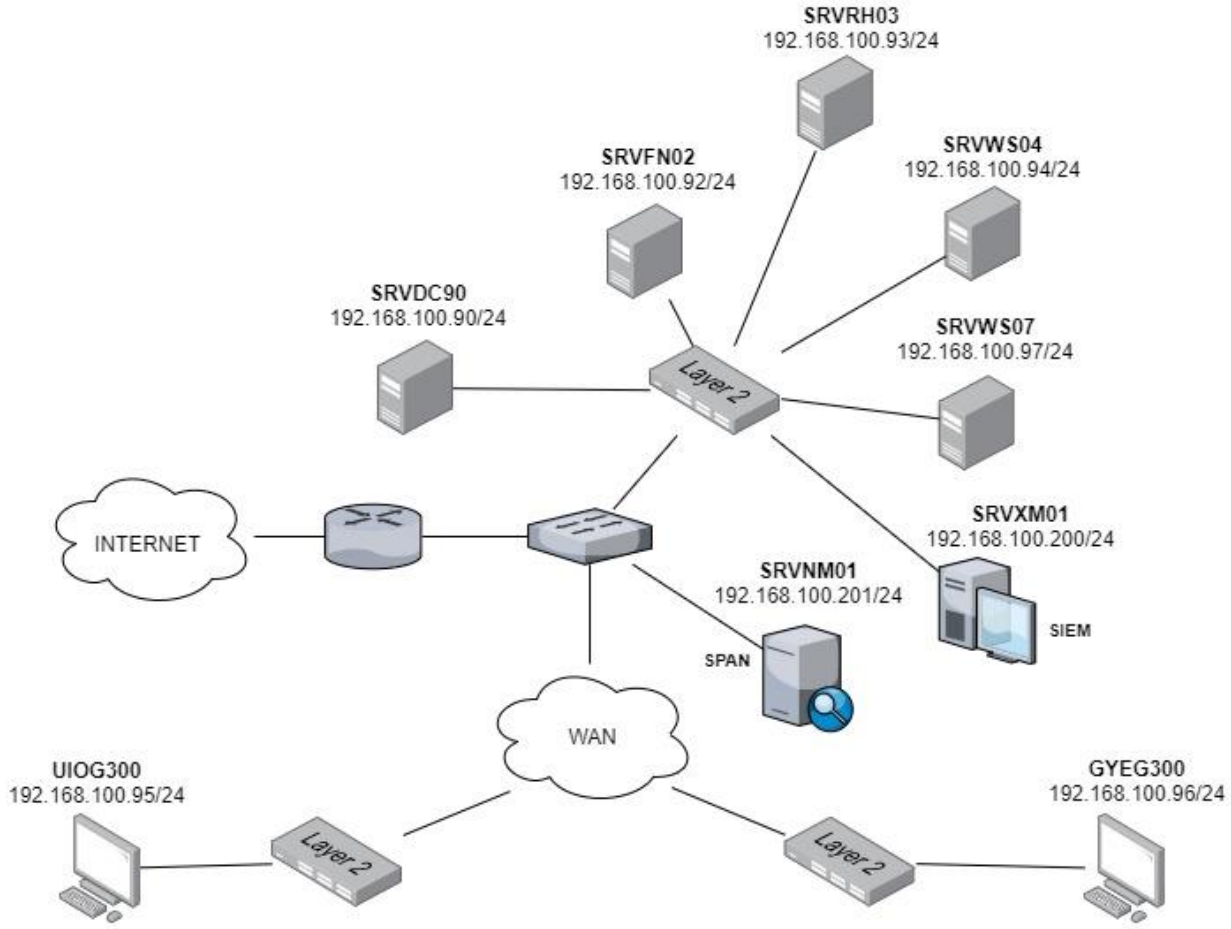
S.O	HOSTNAME	IP ADDRESS	GATEWAY	ROL
FreeBSD	PFSENSE	192.168.2.1	192.168.5.136	FIREWALL
Debian	WAZUH	192.168.2.19	192.168.2.1	SIEM
Ubuntu Server	SRVLX01	192.168.2.30	192.168.2.1	SERVER LINUX
Windows PC	CLIENTE	192.168.2.20	192.168.2.1	CLIENTE

Diseño SIEM Propietario

La arquitectura de red propuesta para este escenario posee varias fuentes de recopilación de datos y se planea un laboratorio diferente (ver figura 7), se cuenta como fuentes de información: DOMAIN CONTROLLER, ACTIVE DIRECTORY, DNS, FILE SERVER, HOME SERVER, Workstation PC y WEB SERVER. Estos proporcionaran todos los eventos generados por los dispositivos de la red al SIEM, teniendo así la tabla 11.

Figura 7

Arquitectura SIEM propietario.



Nota. Diagrama de red con la solución propuesta con un Sistema de Correlación de Eventos con Software Propietario como es LogRhythm.

Tabla 11

Activos Arquitectura SIEM Propietario.

AGENT INSTALLED	FIM/RIM/ SYSMON	S.O	HOSTNAME	ROLE
SI	SYSMON	Windows Server	SRVDC90	DOMAIN CONTROLLER ACTIVE DIRECTORY DNS
SI	FIM SYSMON	Windows Server	SRVFN02	FILE SERVER
NO	NA	Windows Server	SRVRH03	HOME SERVER
SI	ALL	Windows PC	UIOG300	Workstation PC
NO	NA	Windows PC	GYEG300	Workstation PC
SI	ALL	Linux Server	SRVWS04	WEB SERVER
NO	NA	Linux Server	SRVWS07	WEB SERVER
SI	NA	Windows Server	SRVXM01	LogRhythm NextGen SIEM Platform
NO	NA	Linux Server	SRVNM01	LogRhythm Nwtwork Monitoring Platform

Fase de implementación

Para comprobar la generación de eventos en cada una de las propuestas, se realizaron una serie de pruebas a los diferentes casos de uso. Simulando ataques controlados hacia la infraestructura de red, y obteniendo dashboards que permitieron evaluar los resultados.

Implementación del SIEM propietario

Para la implementación de la arquitectura SIEM propietario (ver figura 7) se utilizó un servidor ESXI (ver tabla 12) con el fin de instalar los diferentes servidores y estaciones de trabajo con el fin de integrar y obtener una solución SIEM del tipo propietario, la cual tiene las siguientes formas de recolección de información:

Tabla 12

Características servidor ESXI

Característica	**Detalle**
CPU	3.9 GHz
Memoria	14.48 GB
Almacenamiento	967.86 GB
Adaptador de red	Vswitch

Mediante un agente SIEM

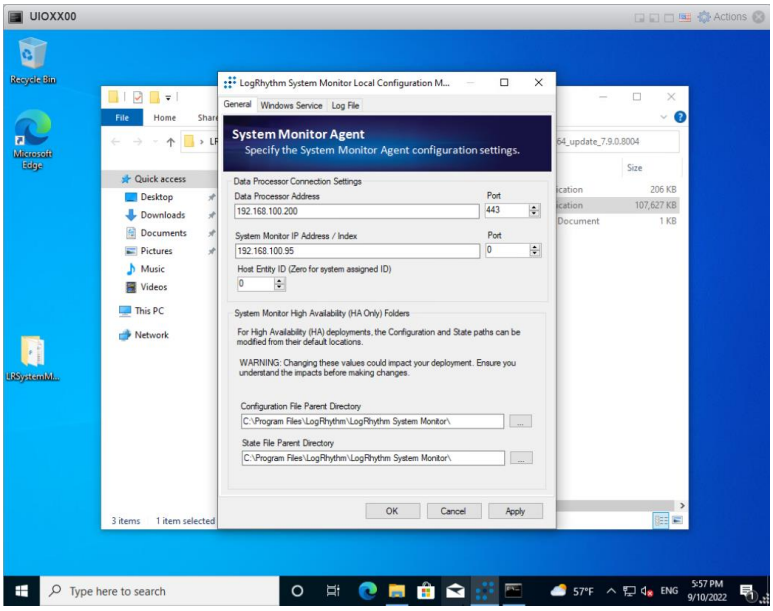
Para recolectar la información a través de un agente es necesario identificar el sistema operativo que se tenga disponible en las Workstation o en el servidor, para este tipo de SIEM se debe destacar que la instalación y configuración es de menor complicación puesto que la instalación no tiene complicaciones y la configuración es mínima independiente del sistema operativo, sea Linux o Windows; por lo que con el paquete de instalación apropiado se tiene una integración exitosa.

Como ejemplo se presenta la instalación y configuración del agente SIEM en la maquina UIOG300 en la que destaca que al tener en un ambiente grafico es sencilla y sin complicaciones. En este escenario la configuración necesaria se basa en la configuración en base al equipo centralizado, es decir el agente debe enviar sus logs a la consola SIEM que está

en la dirección IP 192.168.100.200 y el puerto, así mismo es necesario identificar desde que dirección IP él está enviando todos sus registros, así mismo es necesario configurar un parámetro que se basa en levantar el servicio cada vez que el sistema operativo se encienda. (ver figura 8)

Figura 8

Instalación y configuración agente SIEM propietario.

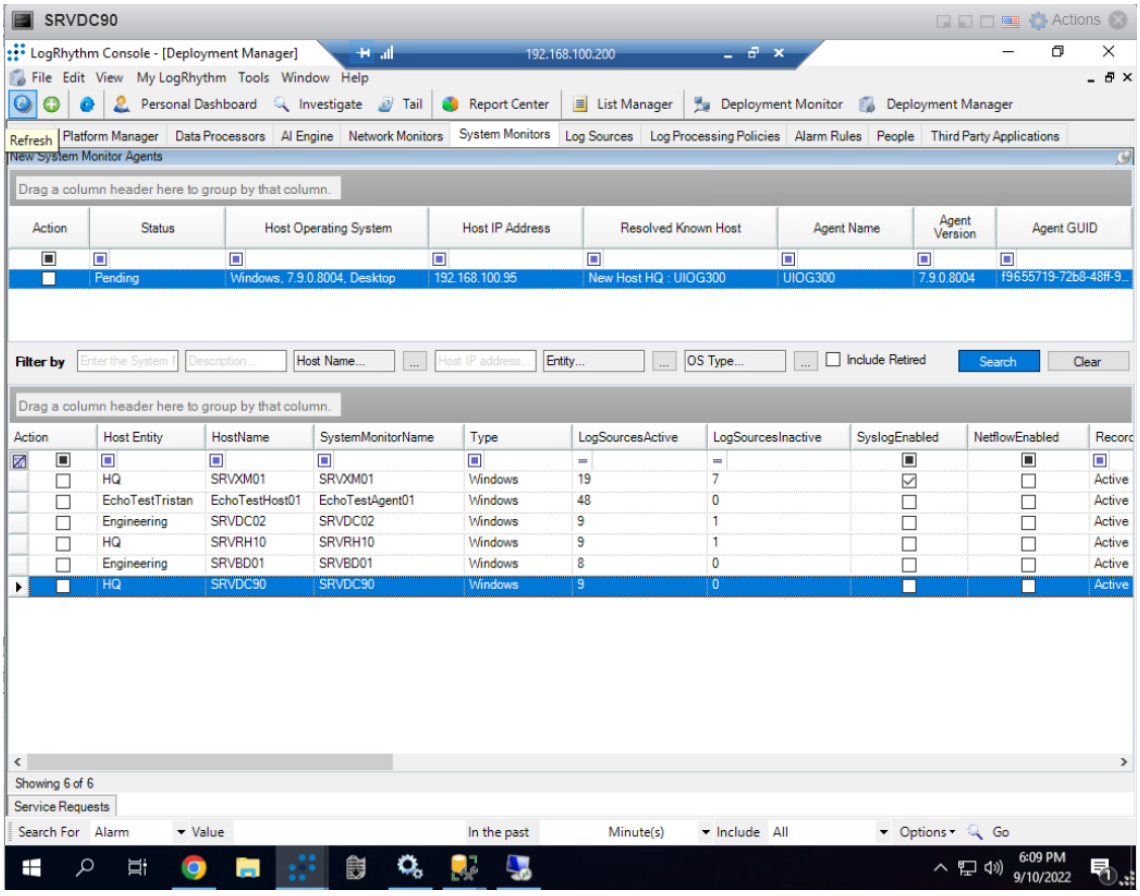


Nota. Ventana de configuración del agente para la recolección de los registros o eventos de un Workstation con Sistema Operativo Windows.

Una vez realizada esta configuración en consola es necesario añadir o permitir el intento de integración que el agente solicita al sistema consola, en donde posteriormente se van a crear reglas o políticas para el monitoreo de los diferentes casos de uso. (ver figura 9)

Figura 9

Agregación del agente en consola SIEM.

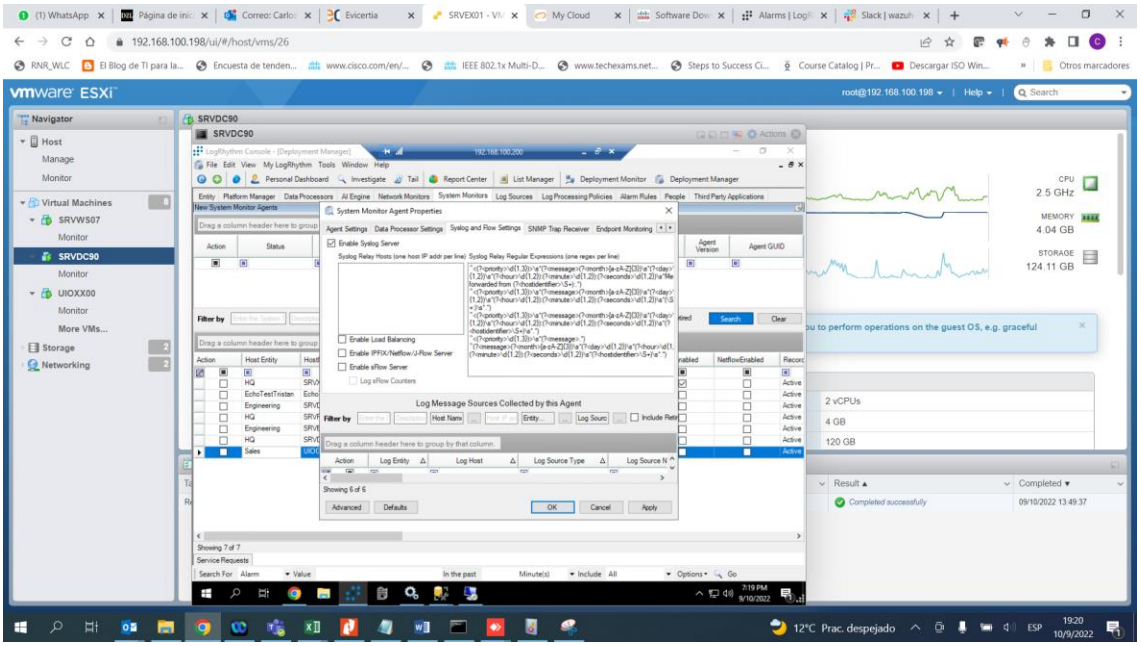


Nota. Ventana de administración para el despliegue de los agentes del sistema SIEM donde se agregan las políticas de recolección de información.

Finalmente se puede corroborar la agregación del agente a la consola revisando la información que está siendo recolectada por el SIEM. (ver figura 10)

Figura 10

Iinformación recolectada en el SIEM.



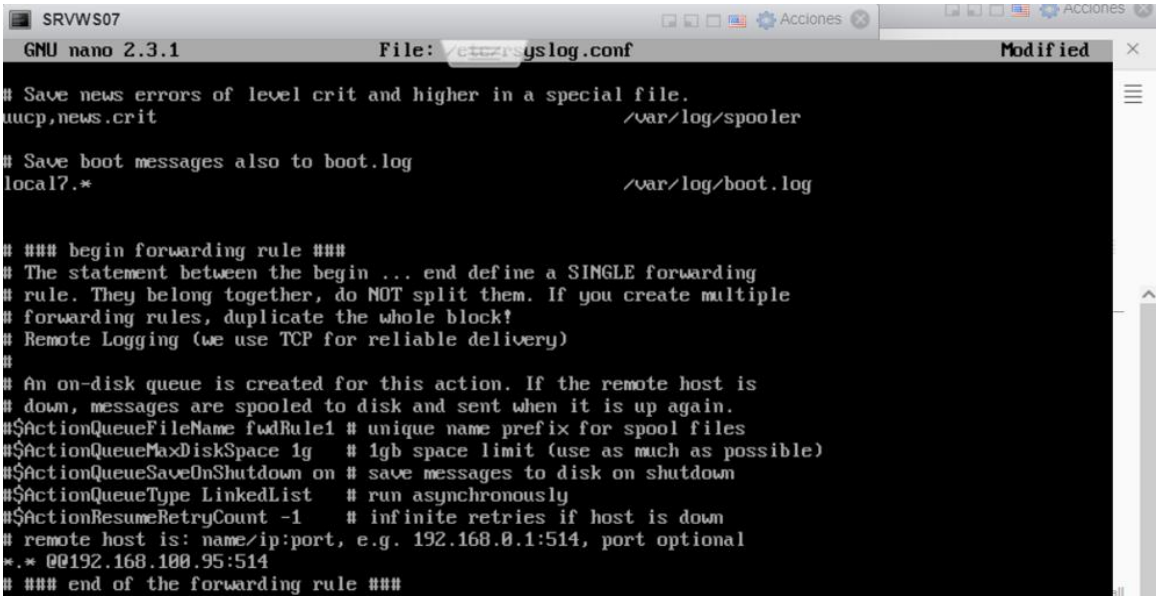
Nota. Ventana de visualización de logs recolectados por el agente.

Mediante SYSLOG.

Para esta forma de recolección de logs el sistema operativo será un CentOs instalado la maquina SRVWS07, en la cual es necesario modificar el archivo /etc/rsyslog.conf en el que se debe añadir la dirección IP y el puerto (ver figura 11) por el que tendrá esa comunicación con el agente instalado en la maquina UIOG300 y posteriormente él envió de sus registros del sistema, en esta configuración es necesario señalar que la dirección IP que se configura puede ser también la de la propia consola SIEM, puesto la herramienta puede recibir estos eventos también de forma directa.

Figura 11

Información recolectada en el SIEM.



Nota. Visualización del archivo de configuración del Workstation con Linux CentOs para el envío de logs desde la ruta /etc/rsyslog.conf hacia el agente con dirección IP 192.168.100.95:514.

Para finalizar con la recolección de información mediante SYSLOG es necesario configurar al agente del SIEM para que también haga el rol de recolección y a su vez envíe sus propios registros más la de la maquina SRVWS07 a la consola SIEM.

Implementación del siem open source

Para este laboratorio se creó una máquina virtual en Vmware con las características presentadas en la tabla 13.

Tabla 13

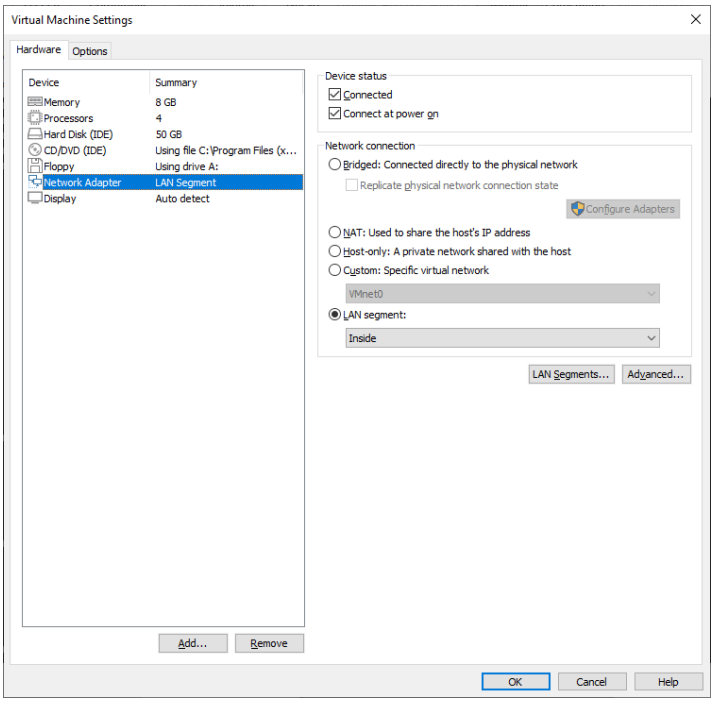
Requerimientos para Wazuh.

Característica	Detalle
Memoria	8 GB
Procesadores	4
Almacenamiento	50 GB
Adaptador de red	Bridged

Luego de aprovisionar los recursos, se procedió a verificar la configuración de red para colocar en el mismo segmento de LAN en el que se encuentra los activos de la red empresarial como se muestra en la figura 12.

Figura 12

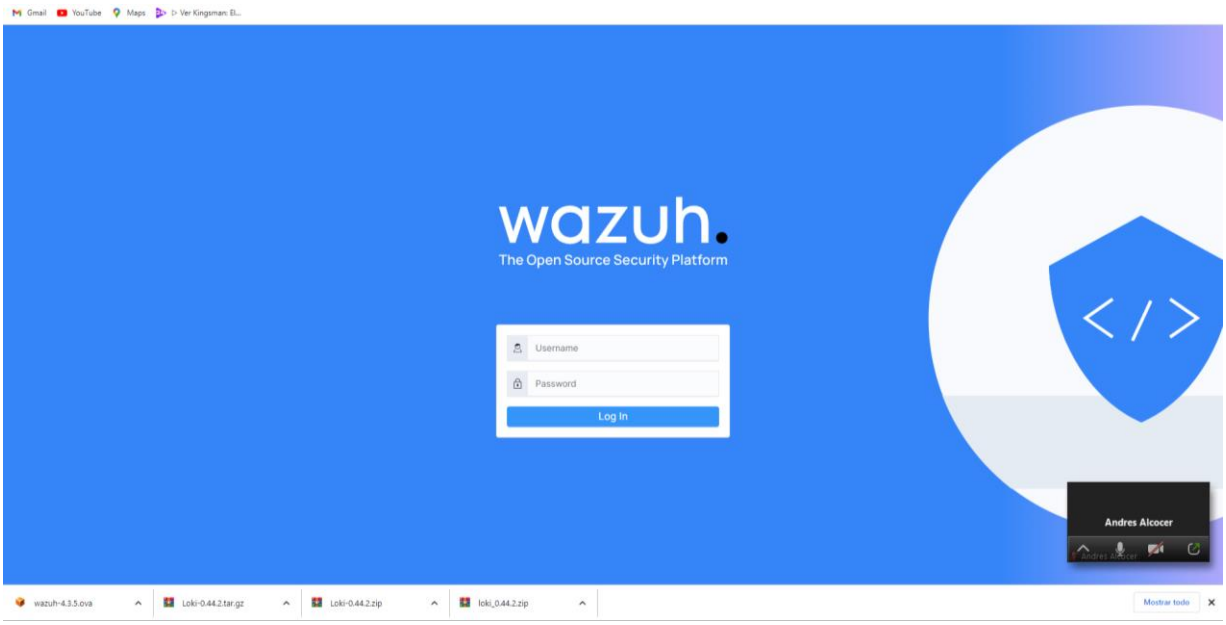
Configuración tarjeta de red virtual.



Se configuró las políticas de red en el Firewall Pfsense que permitió el acceso a la red y la operatividad del SIEM. Una vez instalada y configurada la máquina virtual de Wazuh se procedió a acceder mediante navegador web apuntando a https://192.168.2.19 como se indica en la figura 13.

Figura 13

Interfaz acceso SIEM Wazuh.

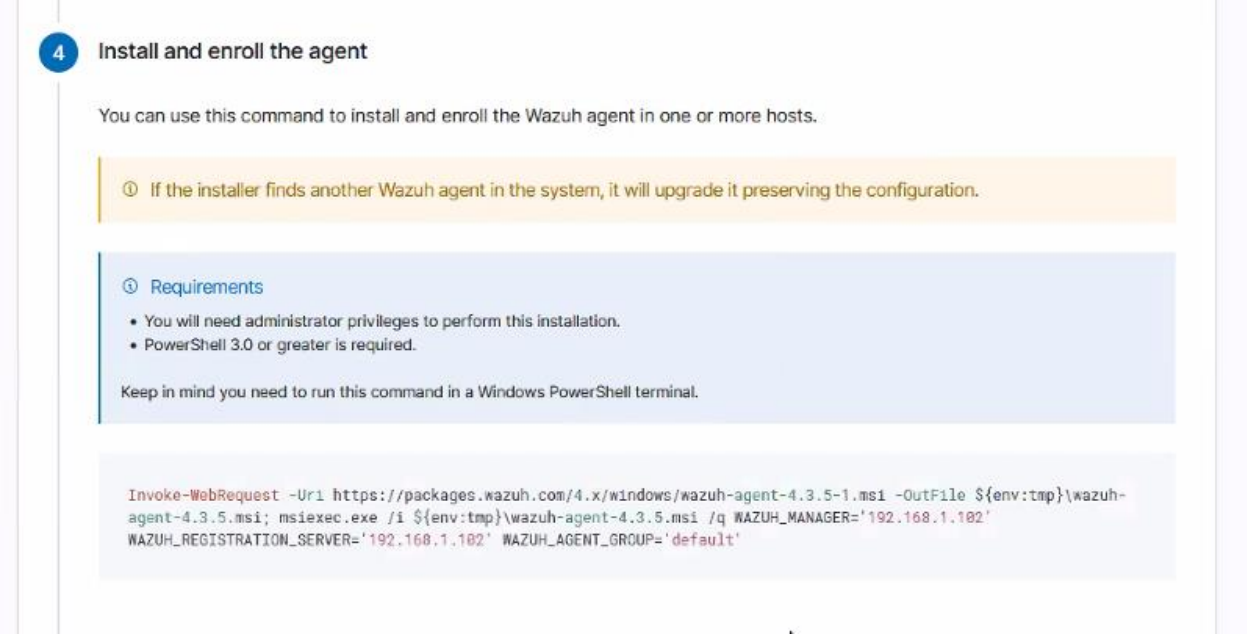


Despliegue de agentes Wazuh. El SIEM wazuh permite recolectar información de los registros de varios activos de la red empresarial ya sean Windows, Linux (RedHat/CentOS / Debian / Ubuntu) y MacOs, aquí se realizó el despliegue en un sistema windows y un freeBSD.

Despliegue de agentes en Workstation Windows. Para desplegar el agente es necesario ingresar a Wazuh – Agents en donde es necesario seleccionar le sistema operativo el direccionamiento IP y el grupo con el fin de obtener el comando para desplegar por medio de PowerShell el agente a la Workstation (ver figura 14).

Figura 14

Instalación y enrolamiento de agente Windows en Wazuh.

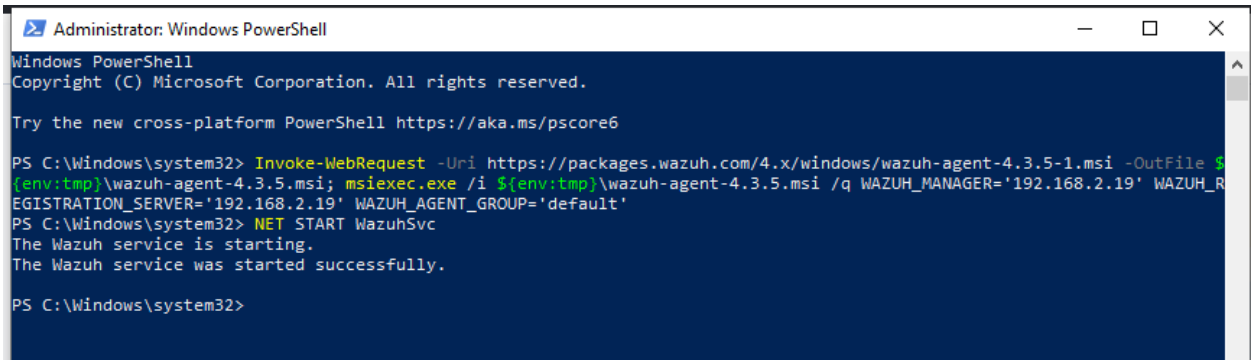


Nota. Proceso para obtener el comando con la configuración (versión del agente, dirección IP del SIEM y el grupo al que pertenece el agente) para instalar y enrolar el agente con la consola de administración.

Se procedió a la activación del agente y se inició el agente a través de líneas de comando en PowerShell como se observa en la figura 15

Figura 15

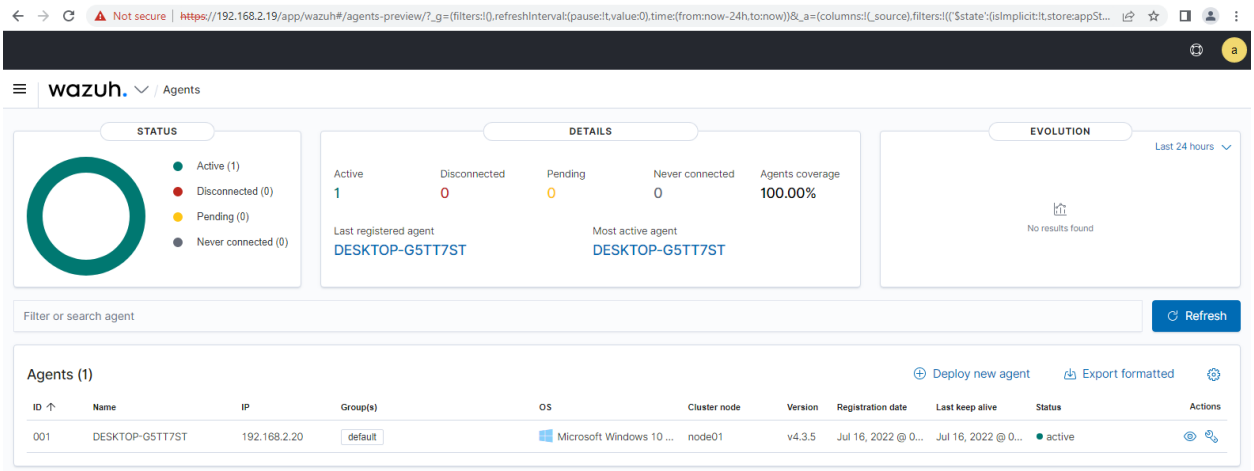
Inicio y activación de agente wazuh en windows.



Se verificó desde la plataforma de Wazuh el agente desplegado y los detalles como sistema operativo, IP y su registro de actividad como se muestra en la figura 16.

Figura 16

Dashboard Wazuh con agente Windows añadido.



Nota. Visualización del dashboard principal de agentes del SIEM Wazuh; se puede apreciar las características del host en donde está instalado el agente, tales como Sistema Operativo, Versión , Dirección IP, nombre del Host, el grupo y además el estado con el cual se puede determinar si está recolectando los registros.

Despliegue de agentes en Firewall / FreeBSD. Para realizar la integración del firewall PFsense es necesario la instalación de un agente de Wazu en su plataforma, para lo cual primero es necesario habilitar el uso de los repositorios FreeBSD, mediante la ejecución del comando **“pkg update”.**

Una vez realizada esta tarea se procedió con la instalación del agente de wazuh por medio de los siguientes comandos:

Búsqueda en la memoria caché el paquete del agente oficial

pkg search wazuh-agent

Instalar agente con la última versión

pkg install wazuh-agent-4.1.5

Una vez terminada la instalación es necesario configurar ciertos parámetros como la dirección IP del SIEM, la misma que ayudó al reconocimiento e integración del firewall con el SIEM, para lo cual se editó el campo address en el archivo de configuración "/var/ossec/etc/ossec.conf":

<server>

<address>WAZUH-MANAGER-IP-ADDRESS</address>

</server>

Con la IP 192.168.2.19

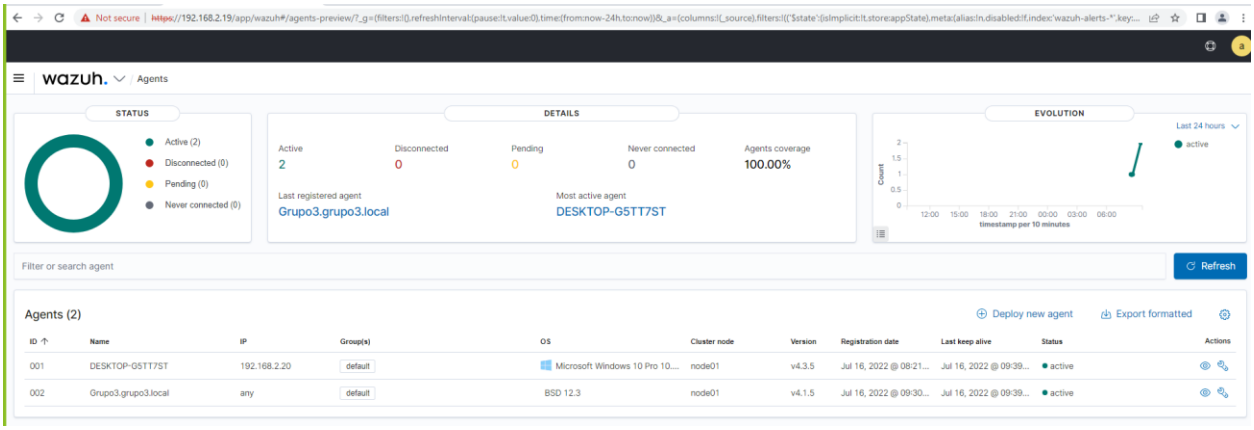
Se inicializa el servicio del agente en el firewall.

service wazuh-agent start

Como se puede observar en la figura 17, el agente ya está siendo reconocido en el SIEM.

Figura 17

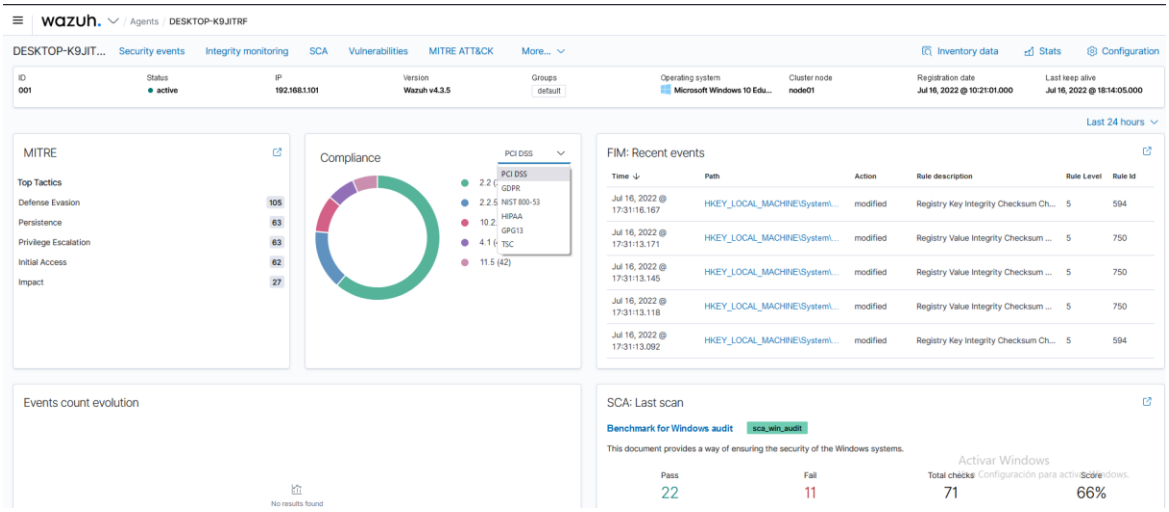
Dashboard de agentes registrados en SIEM.



Recolección de log mediante agente Wazuh. Desde la plataforma de Wazuh se puede visualizar los logs generados por el agente instalado en la máquina de Windows como se muestra en la figura 18.

Figura 18

Dashboard eventos agentes windows.

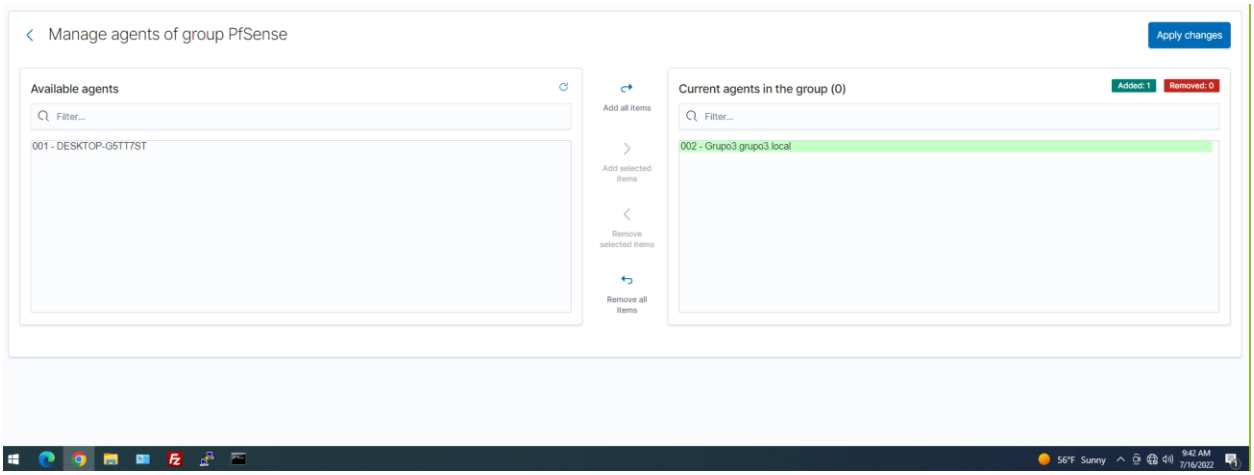


Nota. Dashboard de la recolección de información del agente Windows, donde se muestra los tipos de ataque, nivel de compliance de diferentes estándares internacionales y los eventos recientes como por ejemplo el EventId 594, el cual denota que la integridad del archivo dentro del path HKEY_LOCAL_MACHINE/System/ fue comprometida; la criticidad de la regla que en este caso es 5 varia acorde del tipo de archivo.

Para que se pueda obtener y visualizar de mejor forma los registros generados desde SURICATA se creó un grupo para personalizar la configuración como se observa en la figura 19.

Figura 19

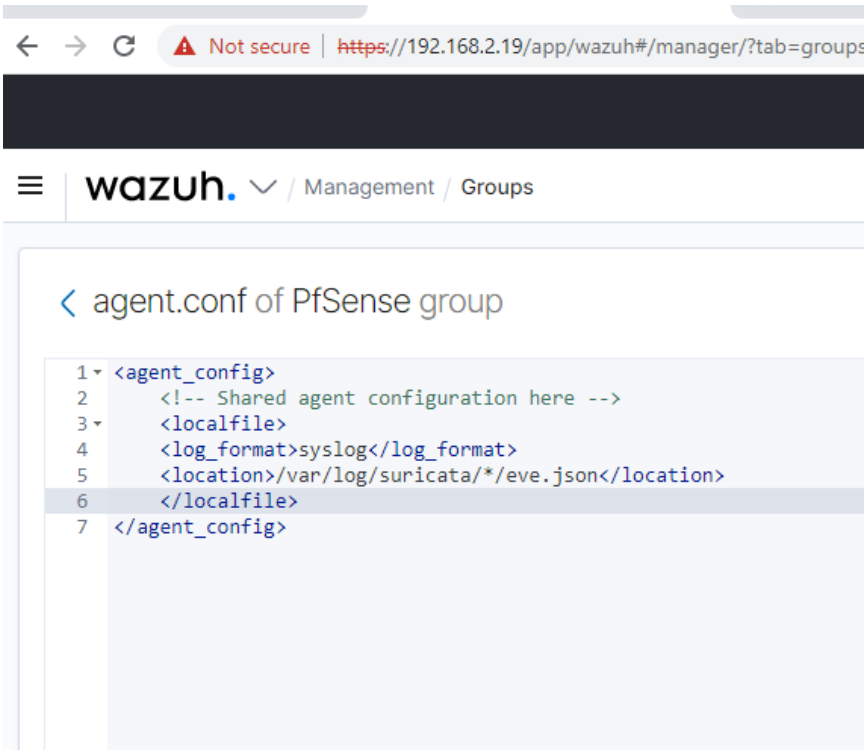
Administración de grupo de agentes de PfSense en Wazuh.



Para poder visualizar los logs del Firewall PfSense se debe configurar la ruta de estos logs en Wazuh como indica la figura 20.

Figura 20

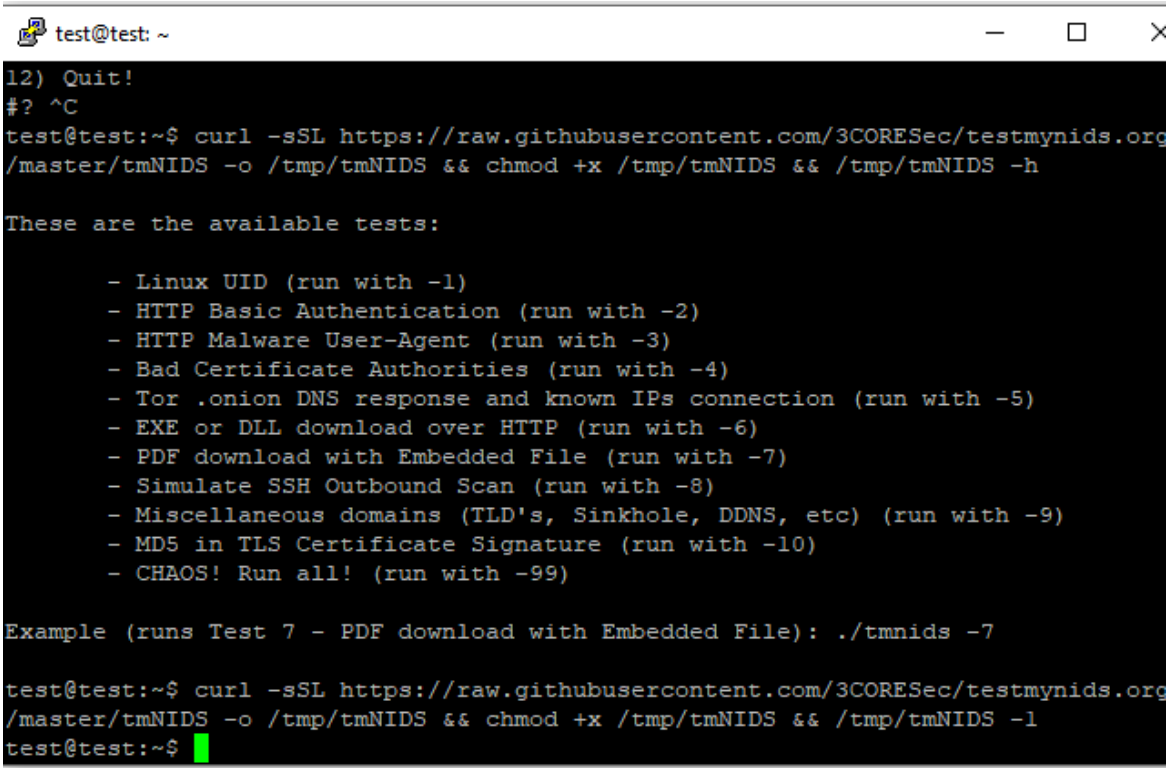
Configuración agente en PfSense y Wazuh.



Reconocimiento de ataques. Se realizaron pruebas de detección de eventos maliciosos a través de las opciones del tester de NIDS como HTTP Basic Authentication, Bad Certificate Authorities, PDF download with Embedded File, Linux UID (ver figura 21).

Figura 21

Opciones para realizar pruebas NIDS.

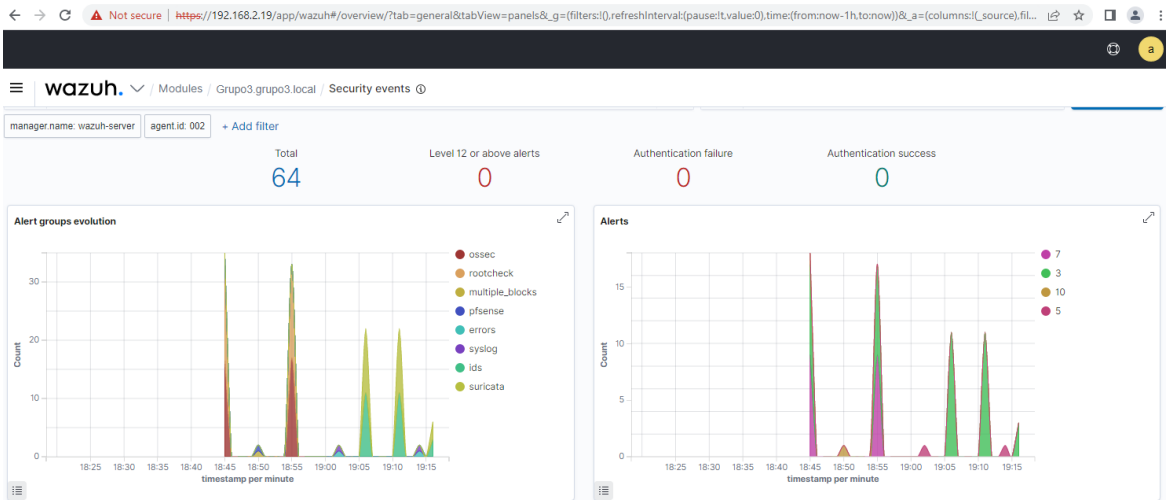


Nota. Visualización de ataques preconfigurados en NIDs para poder ejecutarlos como prueba y obtener los resultados en un ambiente controlado.

Se logró visualizar desde Wazuh en tiempo real los eventos de seguridad que se generaron con NIDS como alertas y grupos de ataques como se observa en la figura 22.

Figura 22

Dashboard incidentes detectados.



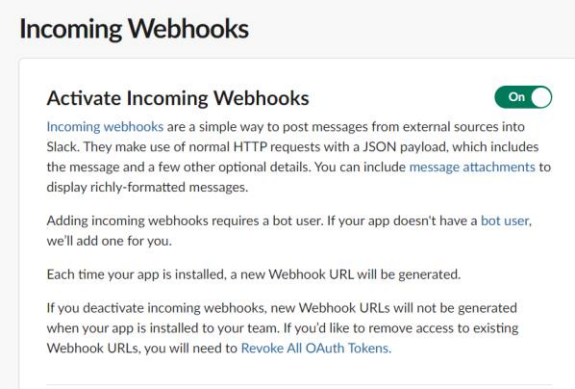
Nota. Dashboard Wazuh con los diferentes tipos de eventos de seguridad detectados en los diferentes componentes de la red durante un determinado lapso de tiempo y la cantidad de estos eventos.

Herramientas de mensajería empresarial. Las herramientas de mensajería empresariales facilitan la conexión de las personas de una organización brindando una alternativa para integrar el SIEM para poder responder de manera oportuna ante un incidente, mejorando la respuesta, disponibilidad y acción ante un evento de seguridad, sin importar su ubicación o zona horaria. Para este proyecto usamos Slack como herramienta de mensajería.

Se configuró la herramienta Slack, la que se utilizó para la comunicación de las alertas detectadas por Wazuh por ser conocida y fácil de integrar con un gran número de sistemas. (ver figura 23)

Figura 23

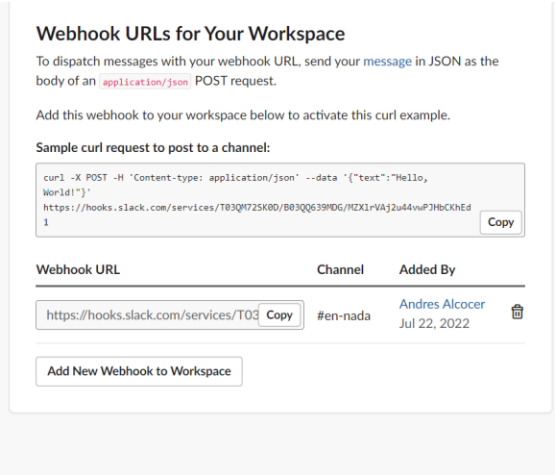
Activación de comunicación de grupo Slack con Wazuh.



Luego de haber activado la comunicación se debe direccionar el envío de las alertas hacia una URL generada por slack. (ver figura 24)

Figura 24

URL de comunicación Wazuh con Slack.

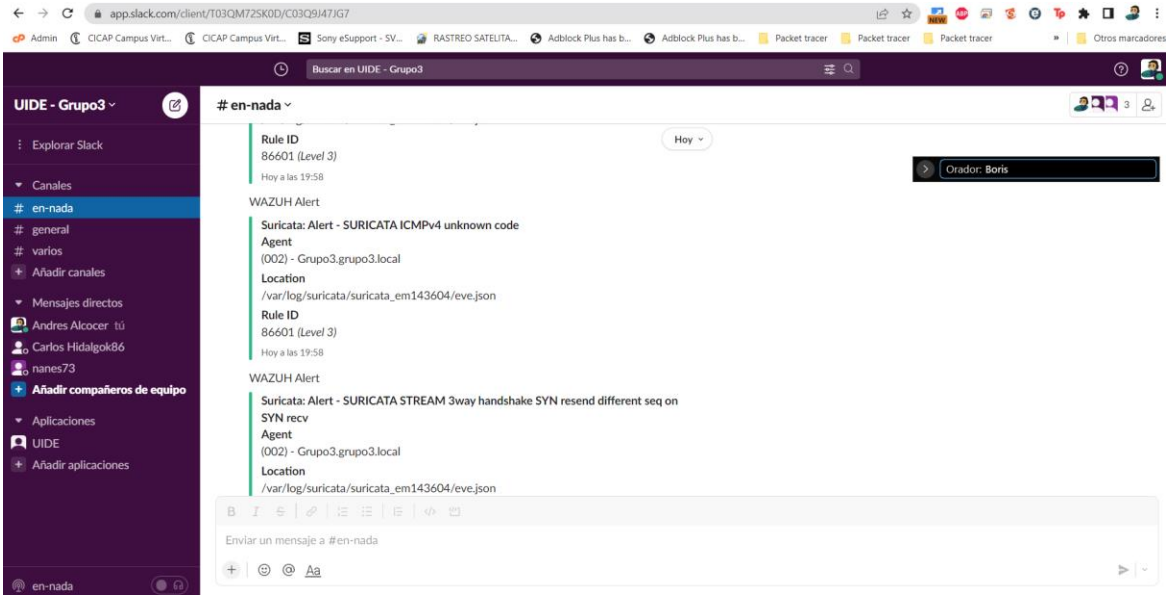


Nota. Ventana que muestra la URL creado, que va a comunicar los mensajes que llegan desde el archivo JSON del SIEM Wazuh

Luego de Activar y direccionar él envió de alertas se puede observar las alertas generadas y presentadas mediante Slack en la aplicación web como se muestra en la figura 25.

Figura 25

Dashboard Slack Web.

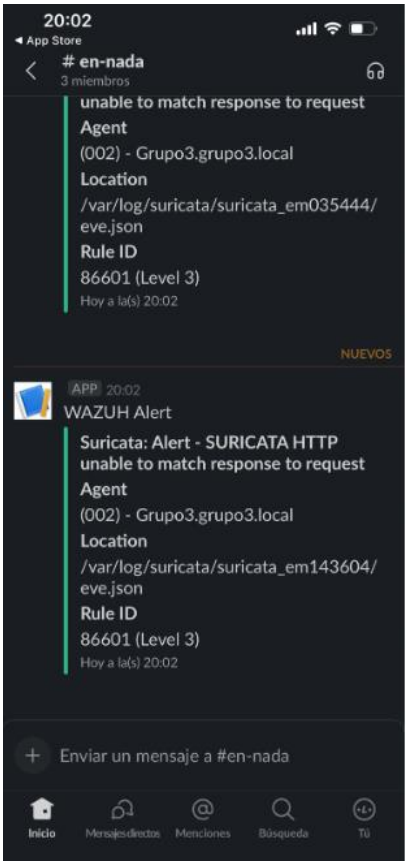


Nota. Dashboard Slack web que muestra las alertas identificando: el dispositivo, agente, ID del evento, así como su nivel de criticidad. Así como, la localización de todos los eventos generados.

Para entregar mayor funcionalidad, se incluyó él envió de alertas de los eventos a través de la aplicación de Slack para iOS, como se puede observar en la figura 26.

Figura 26

Mensajes de alertas en aplicación IOs.



CAPITULO 4 - RESULTADOS Y DISCUSIÓN

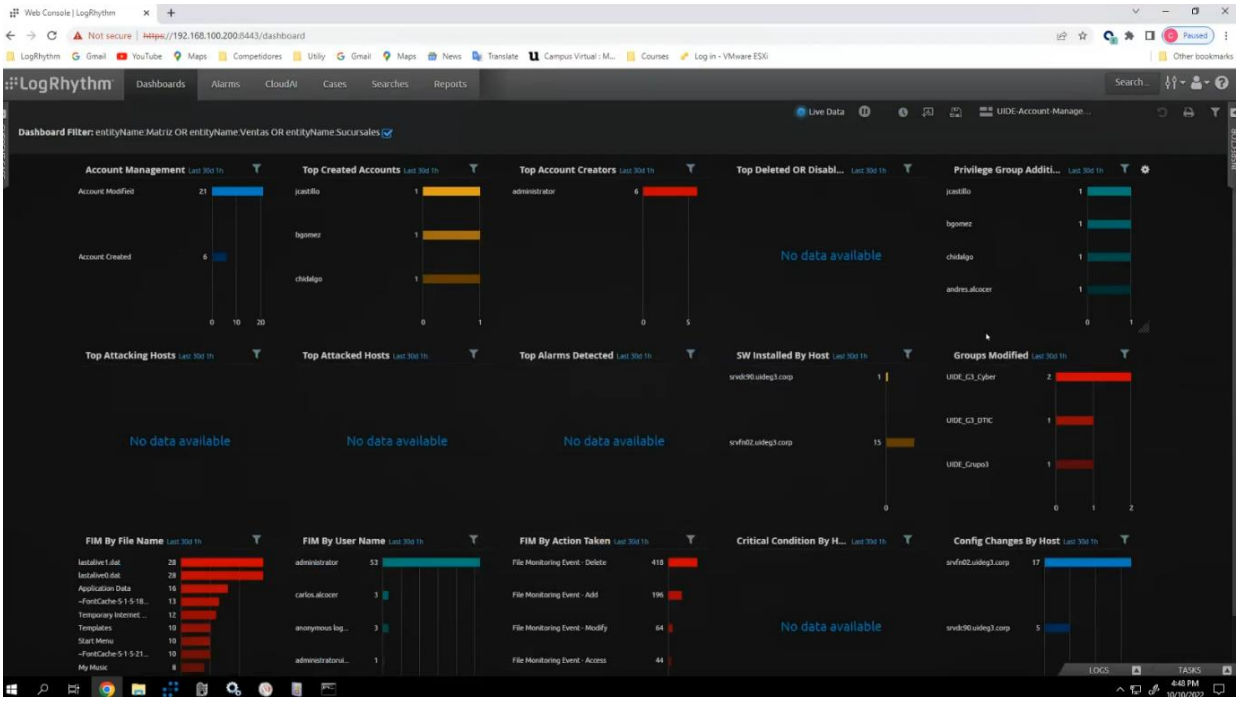
Prueba 1 Windows

Descripción de la prueba

Para realizar esta prueba se implementó la colección de información mediante SYSLOG en la máquina virtual SRVDC90, esta información de este servidor fue receptada a través del puerto TCP/IP 514 en el SIEM y mostrada en el dashboard correspondiente con el fin de visualizar en el SIEM los eventos realizados en el servidor de Active Directory “SRVDC90” cuando un usuario, añada a más usuarios en el servidor o realice cambios en el directorio; para lo cual se implementó una regla para que detecte y muestre este tipo de acciones con el fin de simular un ataque de escalamiento de privilegios sobre el directorio activo de la red. (ver figura 27)

Figura 27

Dashboard de monitoreo AD.



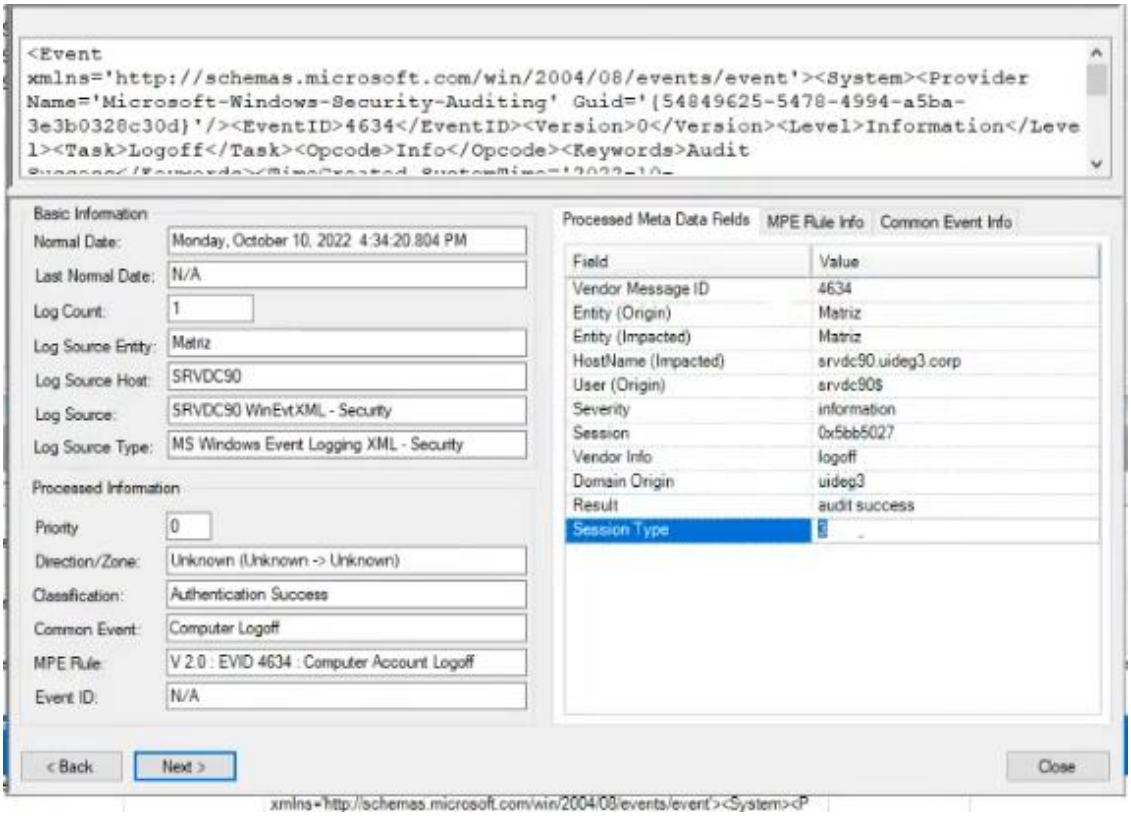
Nota. Dashboard del monitoreo del servicio Active Directory mediante el cual se puede visualizar las diferentes acciones realizadas por el usuario "administrator" el cual crea otros más como "jcastillo", "chidalgo"; asi mismo se puede visualizar que los grupos como "UIDE_G3_DTIC" fue modificado.

Configuración de la regla

Para la configuración de las alertas en el SIEM ante posibles cambios el directorio activo, se debe identificar el EventID del proceso o de los procesos que ejecutan este tipo de acciones en el servidor, esto se lo consigue gracias al parseo, normalización y categorización de los logs que lleva a cabo el SIEM (ver figura 28). Una vez identificada la información involucrada con el servicio del directorio activo, esta información es añadida en el filtro el caso el caso de uso que se creó en el SIEM.

Figura 28

Logs Información de log de autenticación exitosa en Windows.



Nota. Ventana correspondiente al log de evento ID 4634 con la información normalizada.

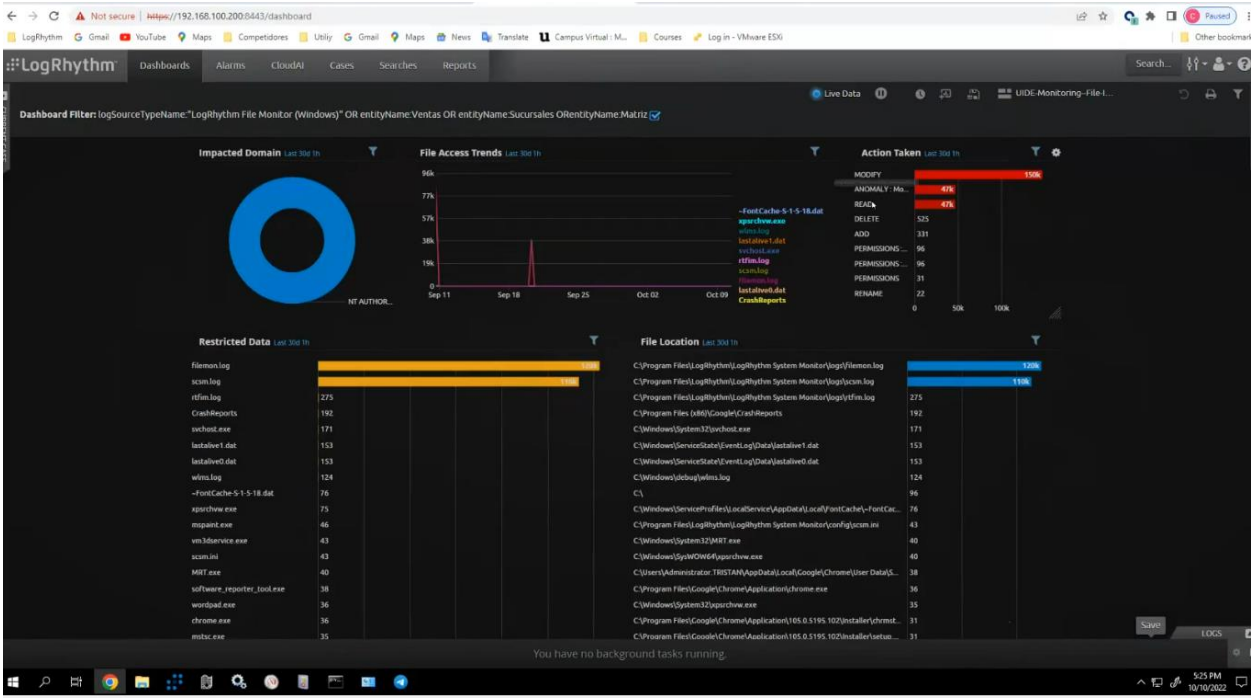
Prueba 2 Windows

Descripción de la prueba

Esta prueba se llevó a cabo mediante un agente instalado y configurado en la máquina virtual SRVFN02, con el fin de monitorear a través del SIEM la integridad de los diferentes directorios o archivos de un path en específico. (ver figura 29)

Figura 29

Dashboard de monitoreo integridad archivos.



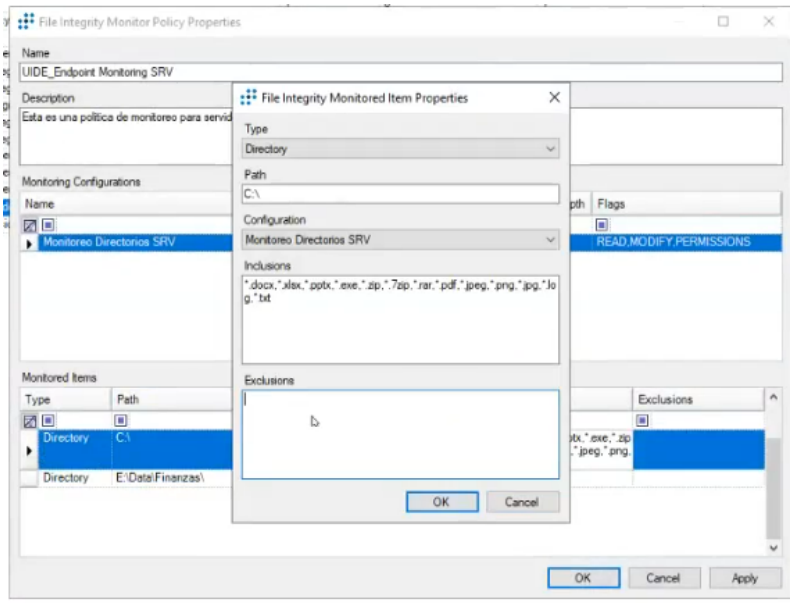
Nota. Dashboard que permite visualizar el cambio en la integridad de los archivos monitoreados por el SIEM, este monitoreo se lo consigue con la configuración previa del path al cual el SIEM verificara el checksum de todos los archivos contenidos en el path.

Configuración de la regla

La regla que muestra este tipo de alertas involucra la configuración en el SIEM de un path en específico, las extensiones de los archivos que van a formar o no parte de esta regla (ver figura 30); posteriormente con esta configuración el SIEM a través del agente es capaz de verificar la integridad de los archivos o directorios dentro del path.

Figura 30

Configuración del path a monitorear.

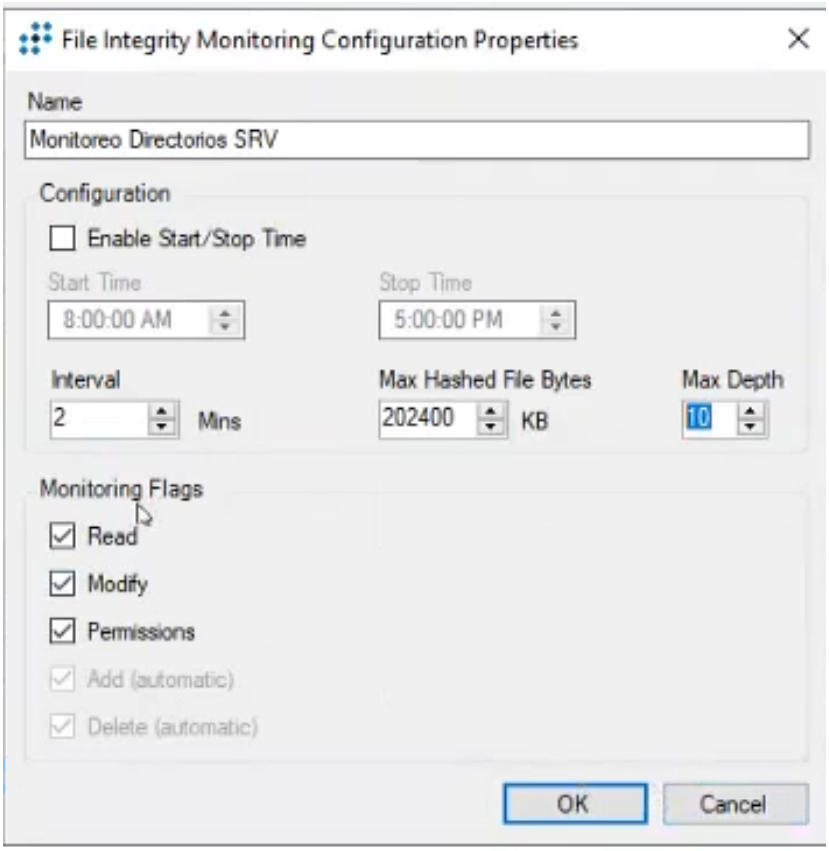


Nota. Ventana de configuración de las propiedades de los directorios que se van analizar por extensiones de archivos.

En este tipo de pruebas es necesario también considerar ciertos campos como cada cuanto tiempo va a tomar estos logs y analizarlos, la profundidad de monitoreo para este directorio, en otras palabras, hasta cuantas carpetas dentro del directorio va a acceder y monitorear y el tipo del evento sea este de lectura, escritura o eliminación. (ver figura 31)

Figura 31

Configuración de regla.



Prueba 3 Windows

Descripción de la prueba

En esta prueba se realizará el monitoreo de procesos en el sistema operativo Windows, estableciendo una política de monitoreo, alarma y respuesta para un proceso en específico (win32calc.exe) en el servidor SRVFN02.

Donde si el proceso en monitoreo es ejecutado el mismo dispara una alarma en el sistema de monitoreo SIEM, y permite reaccionar a dicho evento con las siguientes acciones:

- Eliminar el proceso win32calc.exe usando el administrador de tareas.
- Cierre de sesión del usuario que ejecuta el proceso.

- Deshabilitar la cuenta de dominio que ejecuto el proceso.
- Enviar una notificación por Telegram.

Configuración de la prueba

Al analizar la información del log que se recibe a nivel de la plataforma de SIEM, cuando se ejecuta un proceso en un equipo Windows (ver figura 32) se puede observan parámetros de interés que han sido parseados como:

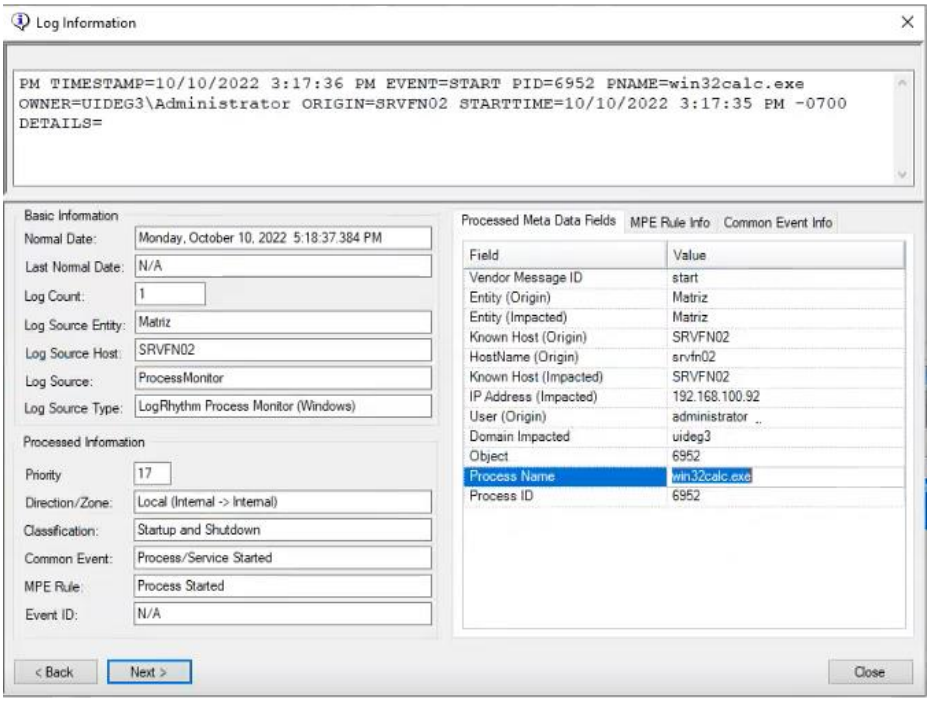
Tabla 14

Información del Log.

Campo	**Valor**
Vendor Message ID	start
Entity (Origin)	Matriz
Entity (Impacted)	Matriz
Known Host (Origin)	SRVFN02
HostName (Ongin)	srvfn02
Known Host (Impacted)	SRVFN02
IP Address (Impacted)	192.168.100.92
User (Ongin)	administrator
Domam Impacted	uideg3
Object	6952
Process Name	win32calc.exe
Process ID	6952

Figura 32

Información de log de inicio de un proceso en Windows.



Con esta información se estableció caracterizar el log que disparara una alarma basada en filtros primarios que relacionaran los parámetros del log de acuerdo a:

Tabla 15

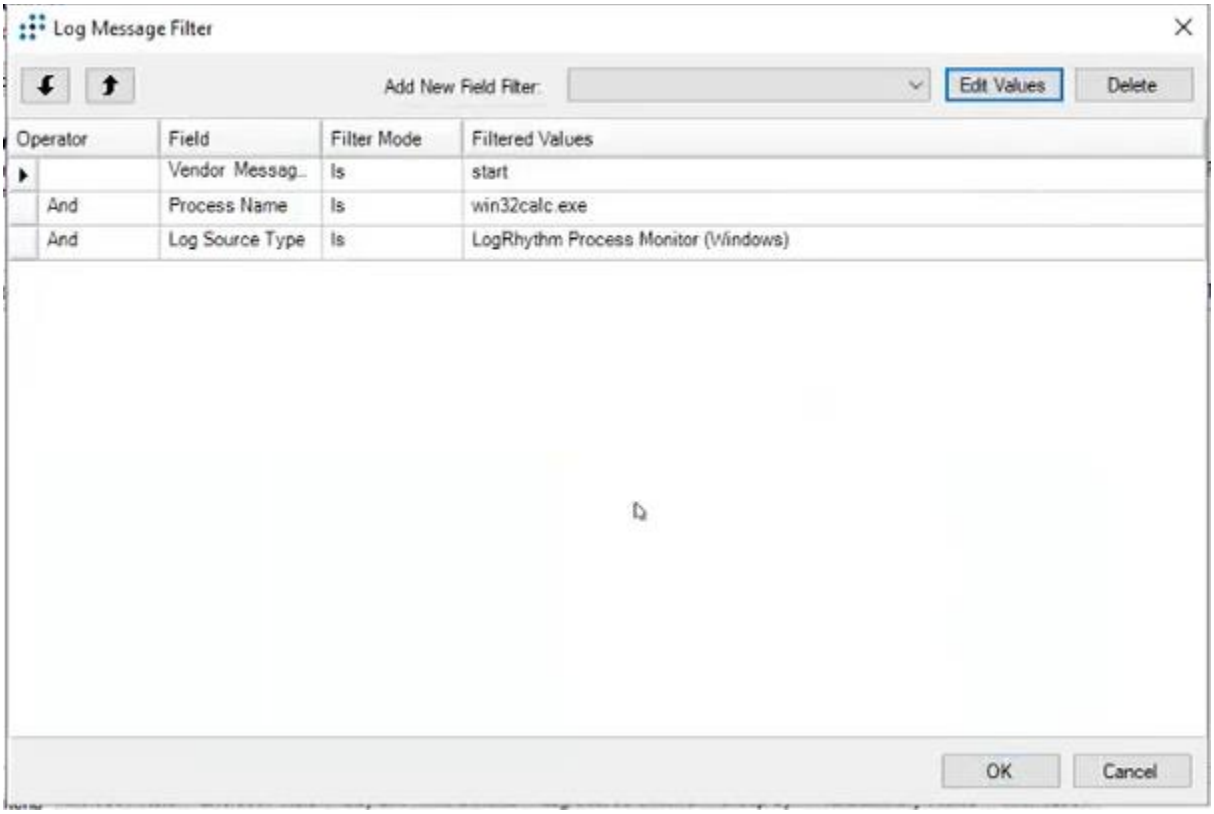
Filtros del log aplicados en la política.

Operador	Campo	Modo de Filtro	Valor Filtrado
	Vendor Message ID	Is	start
And	Process Name	Is	win32calc.exe
And	Log Source Type	Is	LogRhythm Process Monitor (Windows)

De tal forma que se active la alarma cuando un log cumpla con estas características en conjunto, es decir cuando un proceso de tipo Windows inicie y este sea de nombre “win32calc.exe”. (ver figura 33)

Figura 33

Filtros de caracterización del log.



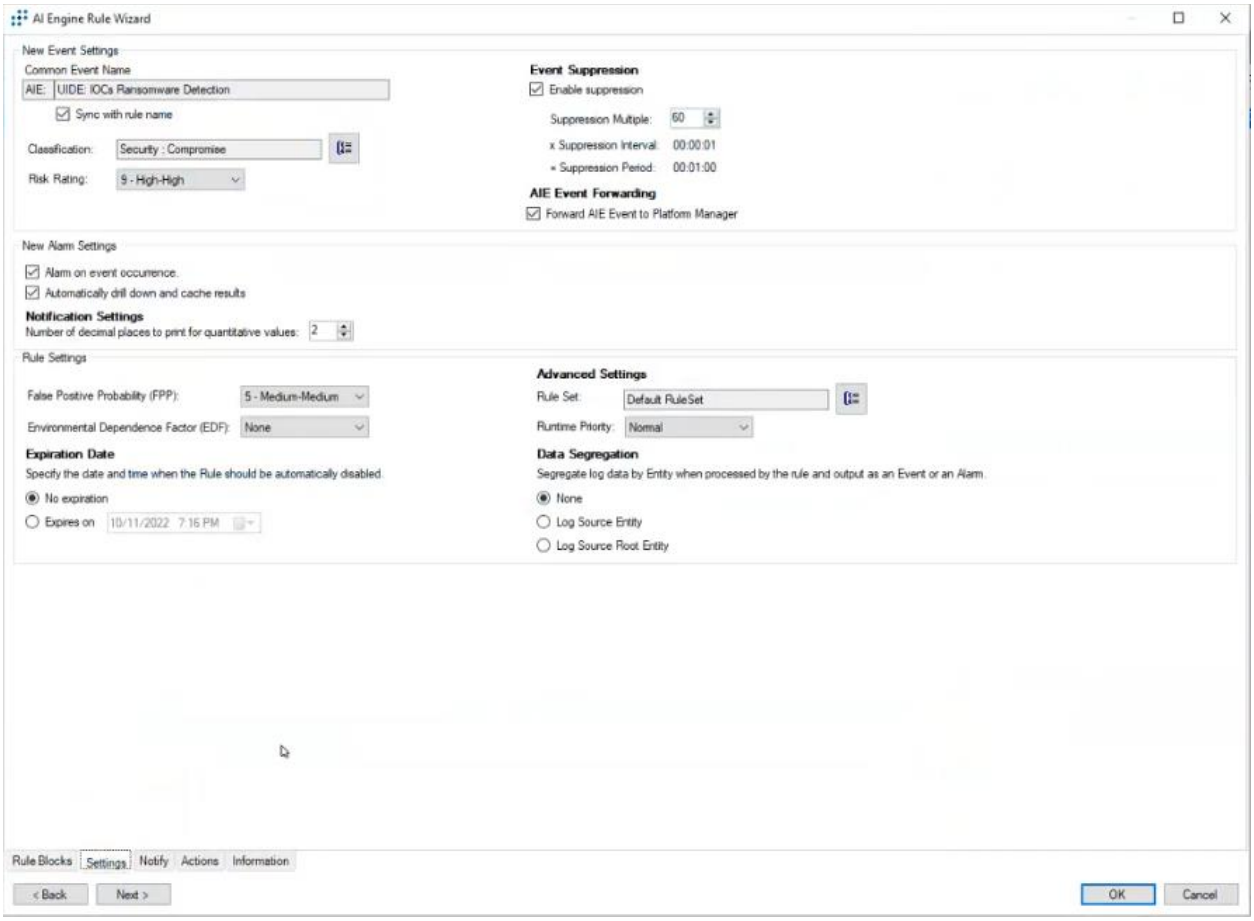
Nota. Ventana de configuración de políticas que se van a ejecutar de acuerdo a los filtros que se establecieron como son: inicio de un proceso, definición del proceso con su extensión y de donde proviene la información.

Una vez se estableció los filtros de caracterización del log, la política se configuro de la siguiente manera: (ver figura 34)

- Nombre del Evento: UIDE: IOCs Ransomware Detection
- Clasificación: Security – Compromise
- Clasificación de Riesgo: 9 – High-High
- Generar Alarma por el evento: SI

Figura 34

Configuración del nuevo evento.



Nota. Ventana de configuración cuando el SIEM detecte un nuevo evento; es necesario categorizar el evento con la regla creada anteriormente UIDE:IOCs Ramsomware Detection, además se configura la criticidad del evento (9 – High High), y su clasificación (Security Compromise)

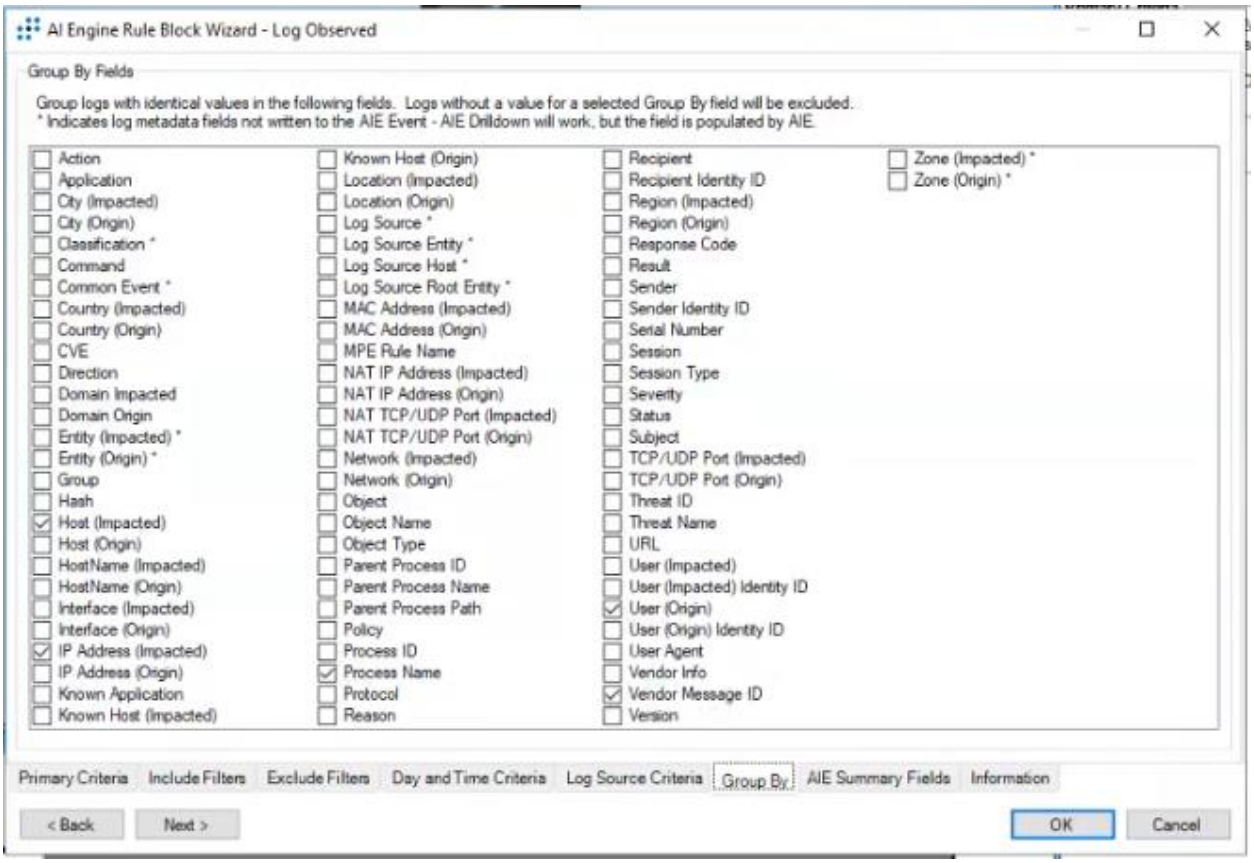
Para evitar varios eventos similares, se realizó la agrupación de los logs en base a campos únicos del log que permitirán señalizarlos y agruparlos para disparar una única alarma, los campos del log por el cual se agrupan son: (figura 35)

- Host (Impacted)
- IP Address (Impacted)

- Process Name
- User (Origin)
- Vendor Message ID

Figura 35

Campos de agrupación del evento.



Para finalizar la configuración de la alarma se estableció las acciones a realizar cuando se genere un evento que cumpla las características establecidas.

Las acciones establecidas se muestran en la tabla 16:

Tabla 16

Acciones a tomar en el evento.

Secuencia de Ejecución	**Nombre de la Acción**	**Requiere Aprobación**	**Establecer Acción**
1	Kill Process Using Job Manager Service Credertials	SI	Kil Windows Process: Kil Process Using Job Manager Service Credentials
2	End RDP Session	SI	Account - Log Off User. End RDP Session
3	Disable AD Account	SI	AD Account ManagementV2.1: Disable AD Account
4	Sent Notification Bot	SI	Telegram Alerts v1.3: Send Notification Bot

Nota. La tabla 16 muestra la secuencia de acciones a tomar en el caso de presentarse el evento y la alarma caracterizada.

A continuación, se muestran las configuraciones de cada una de las acciones a tomar en el evento y alarma que son efecto de la prueba: (ver figura 36)

Tabla 17

Eliminar el proceso win32calc.exe usando el administrador de tareas.

Kil Windows Process: Kil Process Using Job Manager Service Credentials			
Name	Switch	Type	Value
Script	-file KillProcess.ps1	Fixed	
Target Host		Alarm Field	<IP Address (Impacted)>
Target Process		Alarm Field	<Process Name>

Nota. La tabla 17 muestra los parámetros de configuración para la acción de eliminar un proceso en Windows

Tabla 18

Cierre de sesión del usuario que ejecuta el proceso.

Account - Log Off User. End RDP Session			
Name	Switch	Type	Value
Script	-file user_log_off.ps1	Fixed	
Mode	-mode rdp	Fixed	
System	-system	Alarm Field	<IP Address (Impacted)>
Target Process	-user	Alarm Field	<User (Origin)>

Nota. La tabla 18 muestra los parámetros de configuración para la acción de cierre de sesión del usuario que ejecuta el proceso.

Tabla 19

Deshabilitar la cuenta de dominio que ejecuto el proceso.

AD Account ManagementV2.1: Disable AD Account			
Name	Switch	Type	Value
Script	-file Disable-ADAccount.ps1	Fixed	
Target Account Name	-TargetAccount	Alarm Field	<User (Origin)>
Target Domain	-TargetDomain	Constant Value	uideg3.corp
Admin Login User Name	-AdminLoginUserName	Constant Value	Administrator
Admin Password	-AdminPassword	Encrypted Value	*********

Nota. La tabla 19 muestra los parámetros de configuración para la acción de Deshabilitar la cuenta de dominio que ejecuto el proceso.

Tabla 20

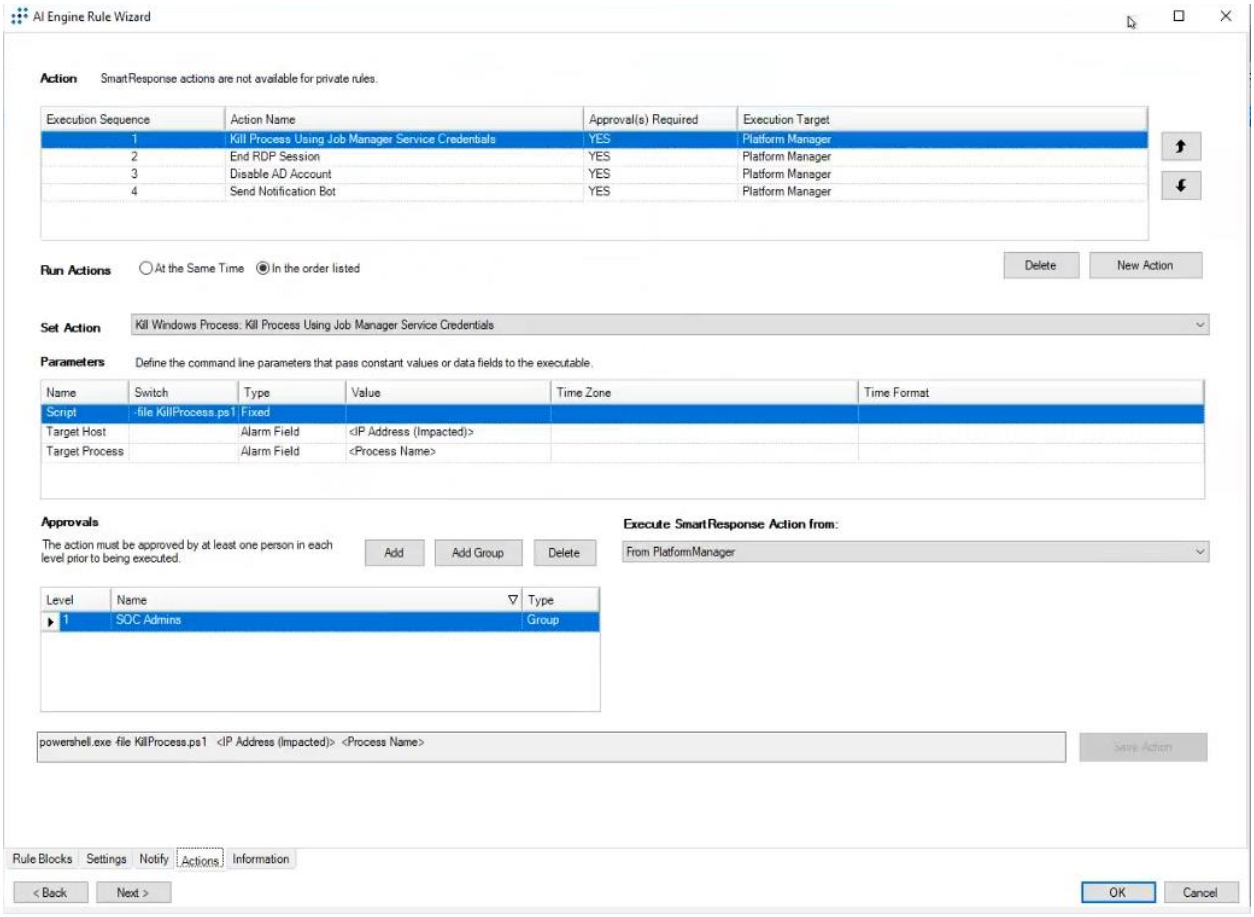
Enviar una notificación por Telegram.

Telegram Alerts v1.3: Send Notification Bot			
Name	Switch	Type	Value
Script	-file C:\MessageTelegram_v13.ps1	Fixed	
BotToken		Constant Value	1545263661:AAFoMI0EBqAdK3k0s7V Jr3sDkXupMo4B5l4
ChatID		Constant Value	803643997
User		Alarm Field	<User (Origin)>
Host		Alarm Field	<Host (Impacted)>
Classification		Alarm Field	<Classification>
AlarmID		Alarm Field	<Alarm ID>
Date		Alarm Field	<Alarm Date>
AlarmName		Alarm Field	<Alarm Rule Name>

Nota. La tabla 20 muestra los parámetros de configuración para la acción de Enviar una notificación por Telegram.

Figura 36

Configuración de acciones (Smart Response).



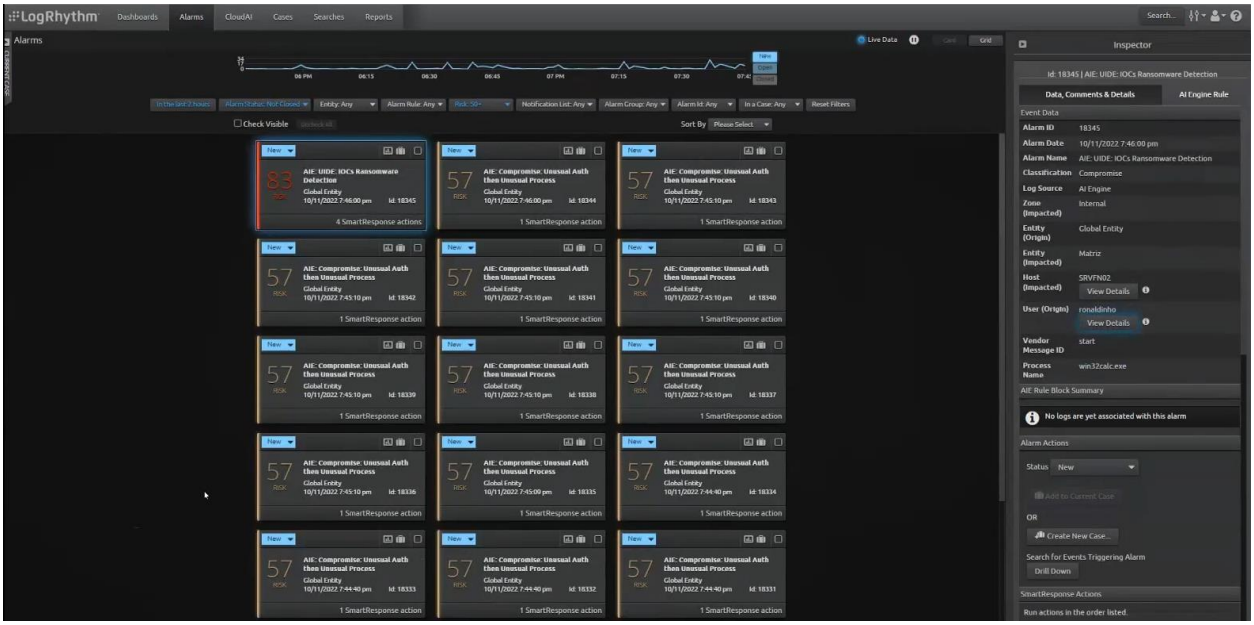
Nota. Configuración de acciones cuando un evento es capturado por el siem y cumple con la políticas establecidas anteriormente para realizar una tarea de remediación o ejecutar una acción determinada como por ejemplo terminar un proceso o cerrar una sesión.

Dashboard

Para validar la ejecución del evento se procedió a acceder vía Escritorio remoto (RDP) al servidor SRVFN02, con el usuario “ronaldinho” y ejecutar la aplicación calculadora, misma que inicia el proceso “win32calc.exe”, y que genera el log de Windows que ejecuta el evento y alarma que se muestra en figura 37.

Figura 37

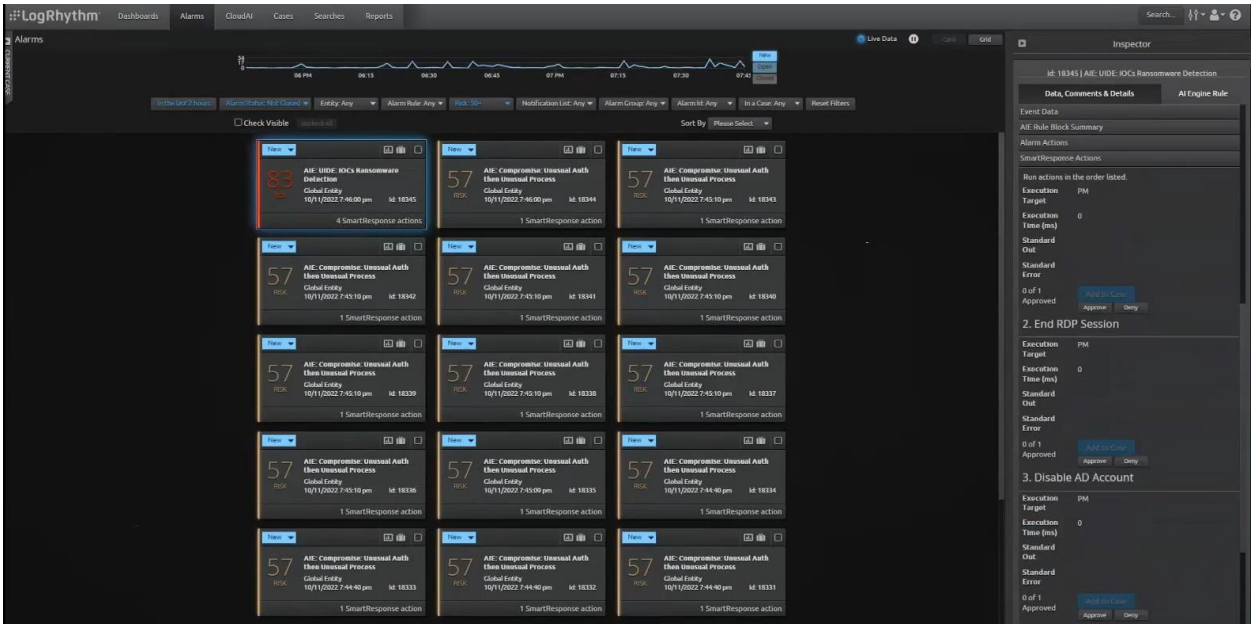
Alarma generada en la prueba.



De igual forma desde este panel se tiene acceso a las acciones de respuesta establecidas en la configuración de la política del evento, y las mismas se muestran en la figura 38.

Figura 38

Acciones de respuesta al evento (SmartResponse).



Nota. Dashboard de las acciones de respuesta ante un incidente, luego que existe un incidente podemos crear un caso, aprobar o denegar una serie de acciones mediante el SIEM, como por ejemplo: terminar un proceso, terminar una sesión RDP o deshabilitar una cuenta de Directorio activo.

Prueba 1 Linux

Descripción de la prueba

En esta prueba se realizó el monitoreo de procesos en sistemas operativos basados en Linux. Se estableció una política de monitoreo, alarma y respuesta para la creación de archivos en el servidor SRVWS04.

Una vez que el proceso de monitoreo es ejecutado el mismo dispara una alarma en el sistema de monitoreo SIEM, y permite reaccionar a dicho evento con las siguientes acciones:

- Bloquear la acción de crear un nuevo archivo.

Configuración de la prueba

Al analizar la información del log que se recibe a nivel de la plataforma de SIEM, cuando se ejecuta un servicio en un equipo Ubuntu, se puede observar parámetros de interés que han sido parseados como: (ver figura 39)

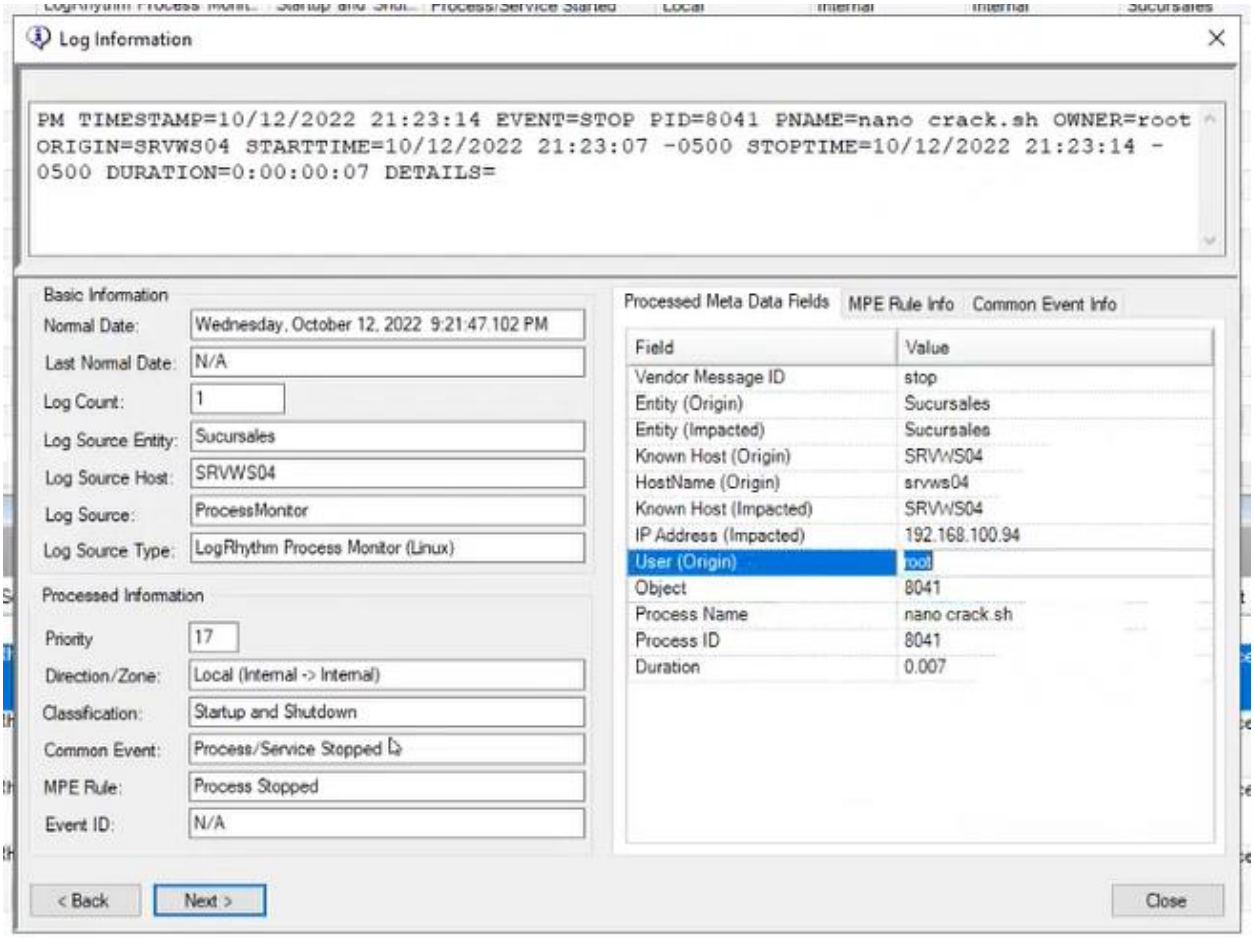
Tabla 21

Información del log.

Campo	**Valor**
Vendor Message ID	stop
Entity (Origin)	Sucursales
Entity (Impacted)	Sucursales
Known Host (Origin)	SRVWS04
HostName (Origin)	srvws04
Known Host (Impacted)	SRVWS04
IP Address (Impacted)	192.168.100.94
User (Origin)	root
Object	8041
Process Name	nano crack.sh
Process ID	8041

Figura 39

Información de log de inicio de un servicio en Linux.



Con esta información se estableció caracterizar el log que disparara una alarma basada en filtros primarios que relacionaran los parámetros del log de acuerdo con: (ver figura 40)

Tabla 22

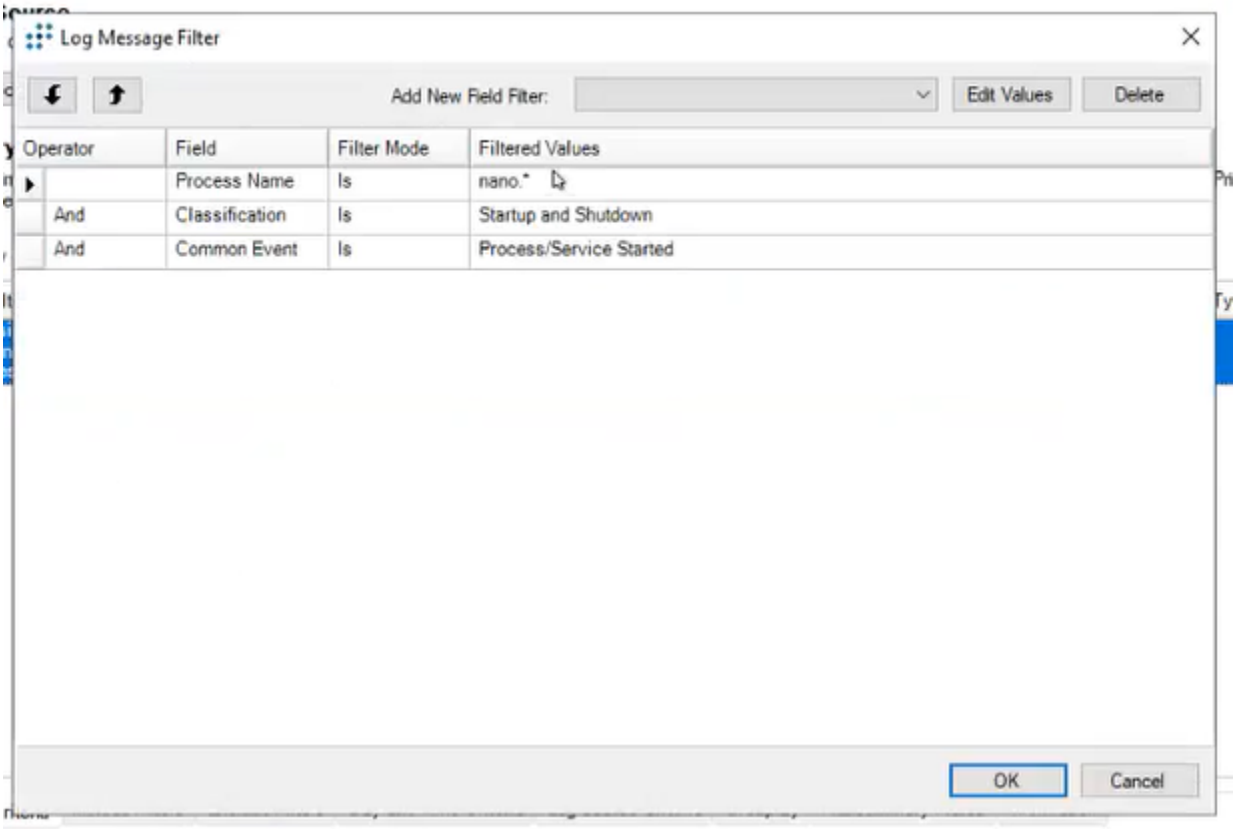
Filtros del log aplicados en la política.

Operador	Campo	Modo de Filtro	Valor Filtrado
	Process Name	Is	nano.*
And	Classification	Is	Startup and Shutdown
And	Common Event	Is	Process/Service Started

De tal forma que se active la alarma cuando un log cumpla con estas características en conjunto, es decir cuando se cree un archivo y este coincida con el nombre “nano.*”.

Figura 40

Filtros de caracterización del log.



Una vez se estableció los filtros de caracterización del log, la política se configuro de la siguiente manera:

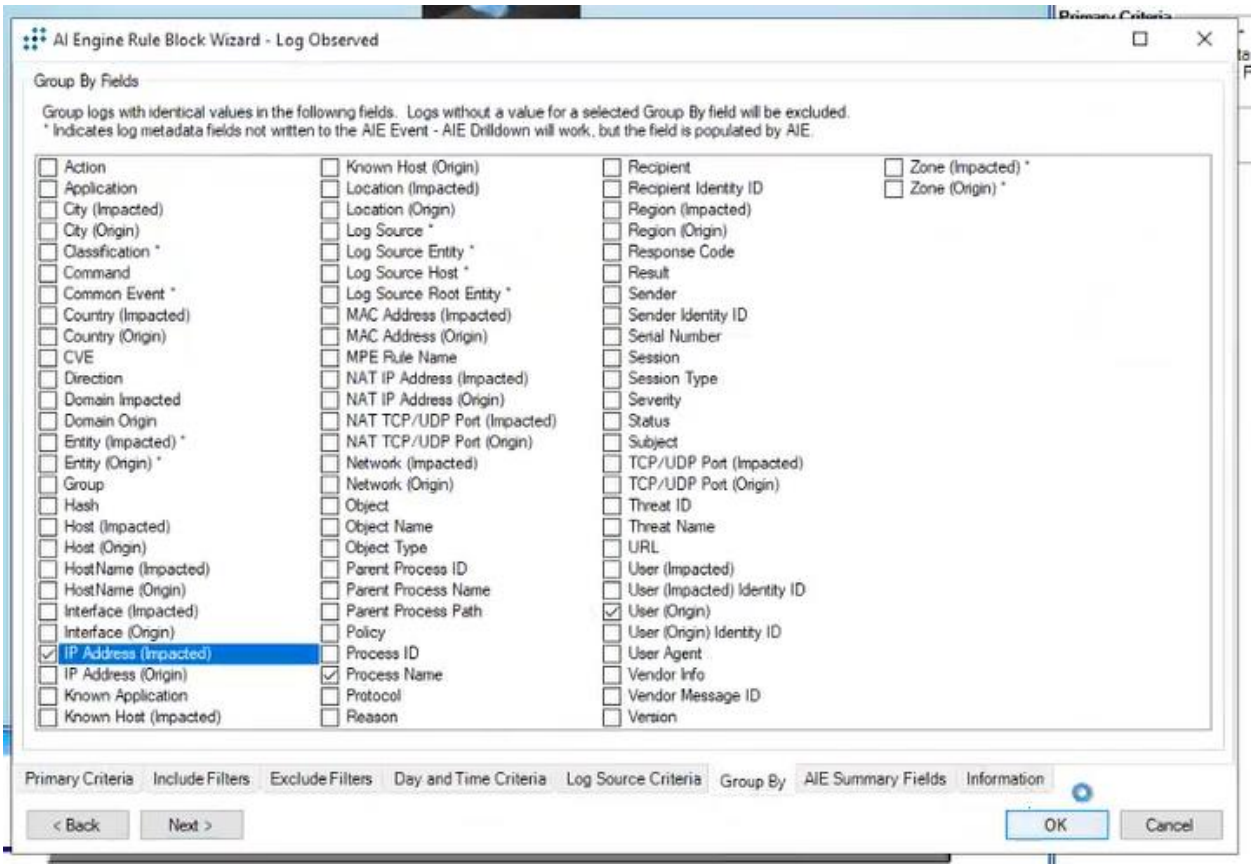
- Nombre del Evento: UIDE: Creation Script Linux
- Clasificación: Security – Attack
- Clasificación de Riesgo: 9 – High-High
- Generar Alarma por el evento: SI

Para evitar varios eventos similares, se realizó la agrupación de los logs en base a campos únicos del log que permitirán señalizarlos y agruparlos para disparar una única alarma, los campos del log por el cual se agrupan son: (ver figura 41)

- IP Address (Impacted)
- Process Name
- User (Origin)

Figura 41

Campos de agrupación del evento.



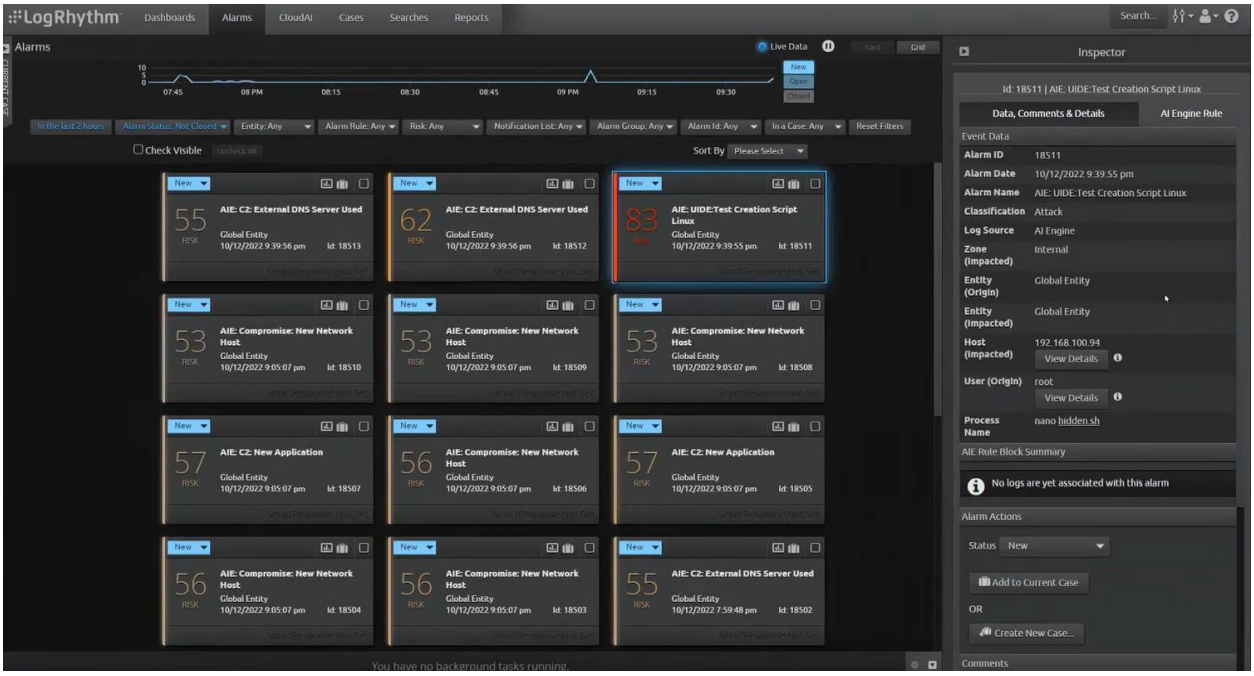
Dashboard

Para validar la ejecución del evento se procedió a acceder vía telnet al servidor SRVWS04, con el usuario “root” y ejecutar el comando nano hidden.sh, mismo que inicia el

proceso “nano hidden.sh”, y que genera el log que ejecuta el evento y alarma que se muestra en la figura 42.

Figura 42

Alarma generada en la prueba.



Prueba 2 Linux

Descripción de la prueba

En esta prueba se realizó el monitoreo de procesos en sistemas operativos basados en Linux. Se estableció una política de monitoreo, alarma y respuesta para el servicio apache2 en el servidor SRVWS04.

Una vez que el proceso de monitoreo es ejecutado el mismo dispara una alarma en el sistema de monitoreo SIEM, y permite reaccionar a dicho evento con las siguientes acciones:

- Bloquear la detención del servicio apache2.

Configuración de la prueba

Al analizar la información del log que se recibe a nivel de la plataforma de SIEM, cuando se ejecuta un servicio en un equipo Ubuntu (ver figura 43), se puede observar parámetros de interés que han sido parseados como:

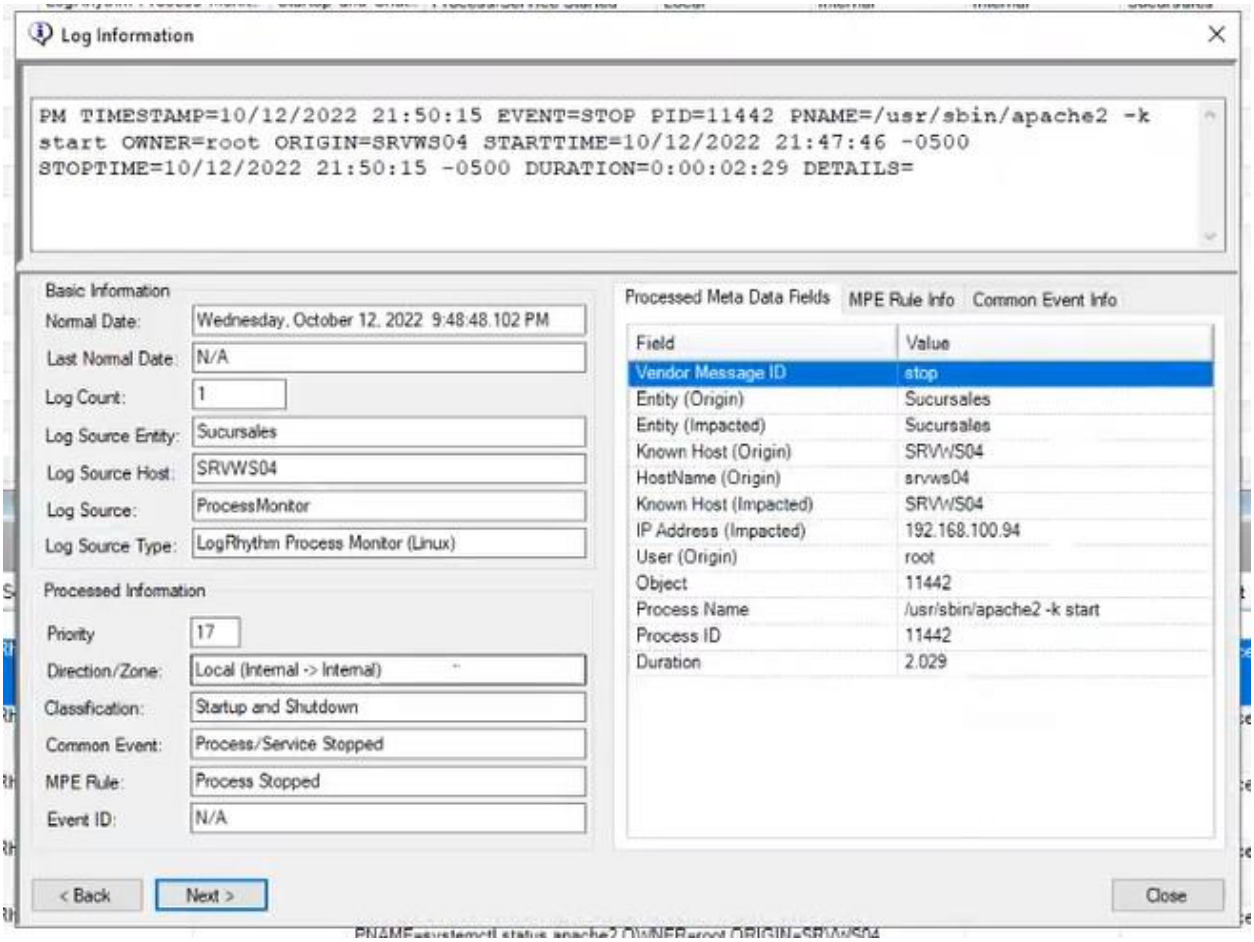
Tabla 23

Información del log.

Campo	**Valor**
Vendor Message ID	stop
Entity (Origin)	Sucursales
Entity (Impacted)	Sucursales
Known Host (Origin)	SRVWS04
HostName (Origin)	srvws04
Known Host (Impacted)	SRVWS04
IP Address (Impacted)	192.168.100.94
User (Origin)	root
Object	11442
Process Name	/usr/sbin/apache2 -k start
Process ID	11442

Figura 43

Información de log de inicio de un servicio en Linux.



Con esta información se estableció caracterizar el log que disparará una alarma basada en filtros primarios (ver figura 44) que relacionarán los parámetros del log de acuerdo a:

Tabla 24

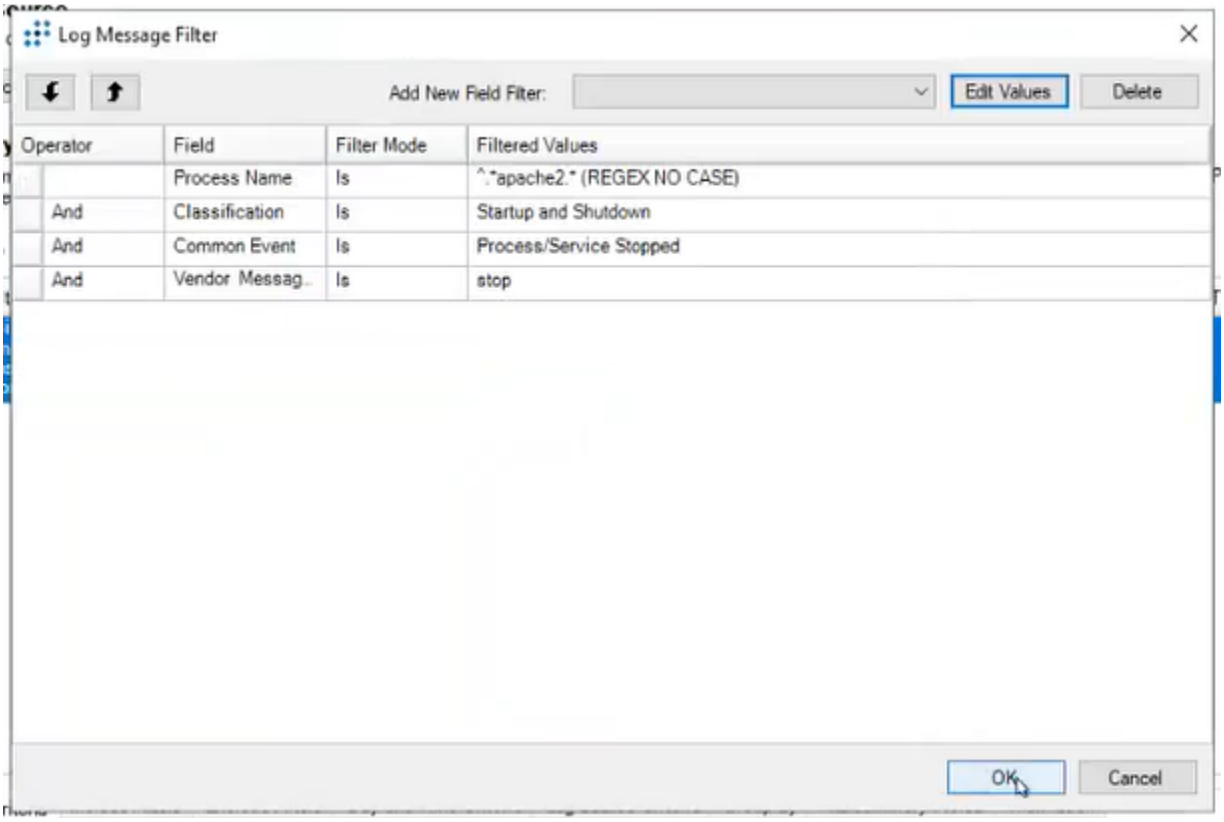
Filtros del log aplicados en la política.

Operador	Campo	Modo de Filtro	Valor Filtrado
	Process Name	Is	^.*apache2.*(REGEX NO CASE)
And	Classification	Is	Startup and Shutdown
And	Common Event	Is	Process/Service Stopped
And	Vendor Message ID	Is	stop

De tal forma que se active la alarma cuando un log cumpla con estas características en conjunto (ver figura 44), es decir cuando un servicio se detenga y este sea de nombre “/usr/sbin/apache2 -k start”.

Figura 44

Filtros de caracterización del log.

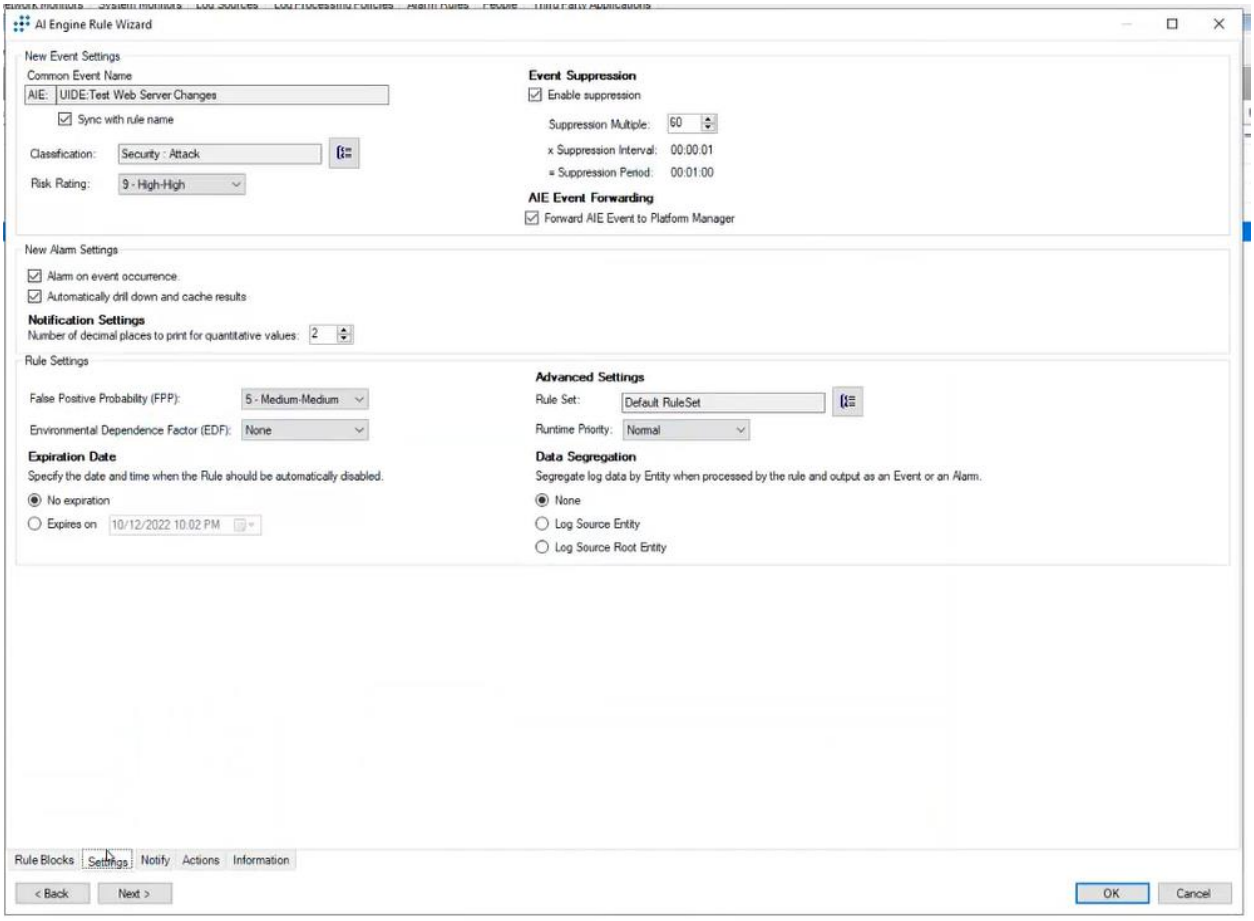


Una vez se estableció los filtros de caracterización del log (ver figura 45), la política se configuró de la siguiente manera:

- Nombre del Evento: UIDE: Web Server Changes
- Clasificación: Security – Attack
- Clasificación de Riesgo: 9 – High-High
- Generar Alarma por el evento: SI

Figura 45

Configuración del nuevo evento.

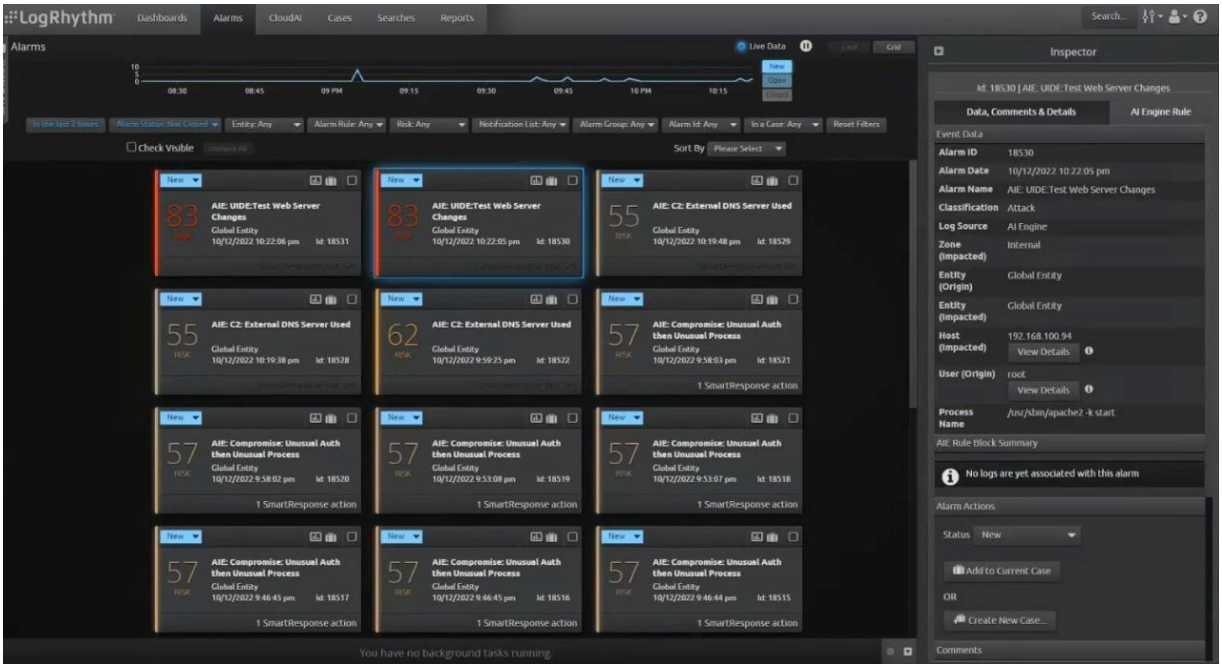


Dashboard

Para validar la ejecución del evento se procedió a acceder vía telnet al servidor SRVWS04, con el usuario “root” y ejecutar el comando “systemct1 stop apache2”, mismo que inicia el proceso “/usr/sbin/apache2 -k start”, y que genera el log que ejecuta el evento y alarma que se muestra en la figura 46.

Figura 46

Alarma generada en la prueba.



Integración con herramientas de comunicación empresarial (slack, telegram)

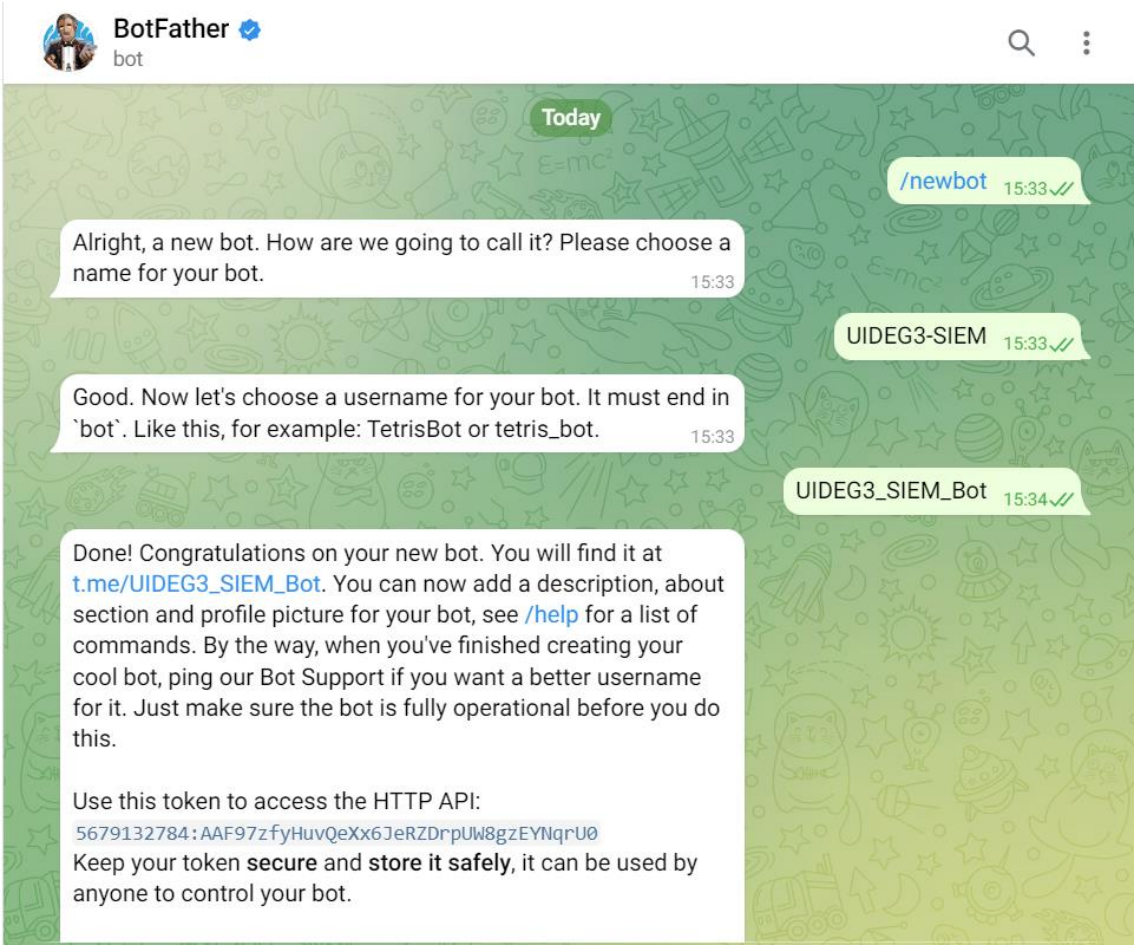
Para poder integrar a la solución de SIEM Logrhythm con la plataforma de mensajería Telegram, es necesario la creación de un bot en Telegram, el cual se encargará del envió de publicaciones en un grupo de Telegram mediante el llamado de una API que se ejecuta a través de un script powershell en Logrhythm. (ver figura 47)

Crear un bot de Telegram

1. Buscamos el “@Botfather” en Telegram
2. Se inicia una conversación y se escribe "/ newbot"
3. Ingrese el nombre del nuevo bot (este será un nombre para mostrar)
4. Ingrese el nombre de usuario del bot (debe terminar con "_bot")
5. Obtenga el token API del bot

Figura 47

Configuración bot Telegram.



Obtener detalles del grupo Telegram

1. Crea un nuevo grupo de Telegram para la recepción de alarmas
2. Invite a su bot al grupo (busque por el nombre de usuario del bot) y agréguelo como administrador
3. Encuentre la ID del canal al que desea enviar mensajes a través del bot.

   NOTA: Los ID de los canales siempre comienzan con un símbolo menos (-).
4. Publique algo en el canal con el bot (para que el bot "vea" que se agregó al canal)

Una vez se generó el bot y creo el grupo de Telegram tenemos los datos:

Tabla 25

Información creación bot Telegram.

Parámetro	**Valor**
Nombre bot	UIDEG3-SIEM
Token HTTP API	5679132784:AAF97zfyHuvQeXx6JeRZDrpUW8gzEYNqrU0
Chat ID	752893113

Con esta información se procede a ejecutar una prueba y se ejecuta la API mediante la siguiente url, donde el mensaje a enviar es “TestReply”:

https://api.telegram.org/bot**<your-bot-token>**/sendMessage?**chat_id**=<chat-id>&text=**TestReply**

Por lo que para nuestro ejemplo la URL de la API es:

https://api.telegram.org/bot**5679132784:AAF97zfyHuvQeXx6JeRZDrpUW8gzEYNqrU0**/sendMessage?chat_id=-**752893113**&text=**TestReply**

Figura 48

Prueba API envio de mensajes Telegram.

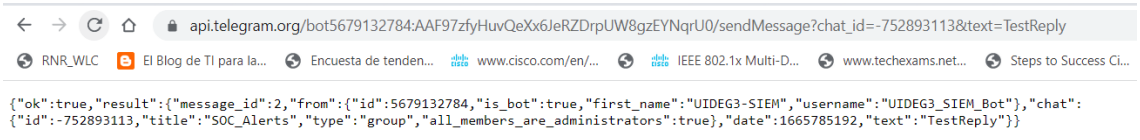
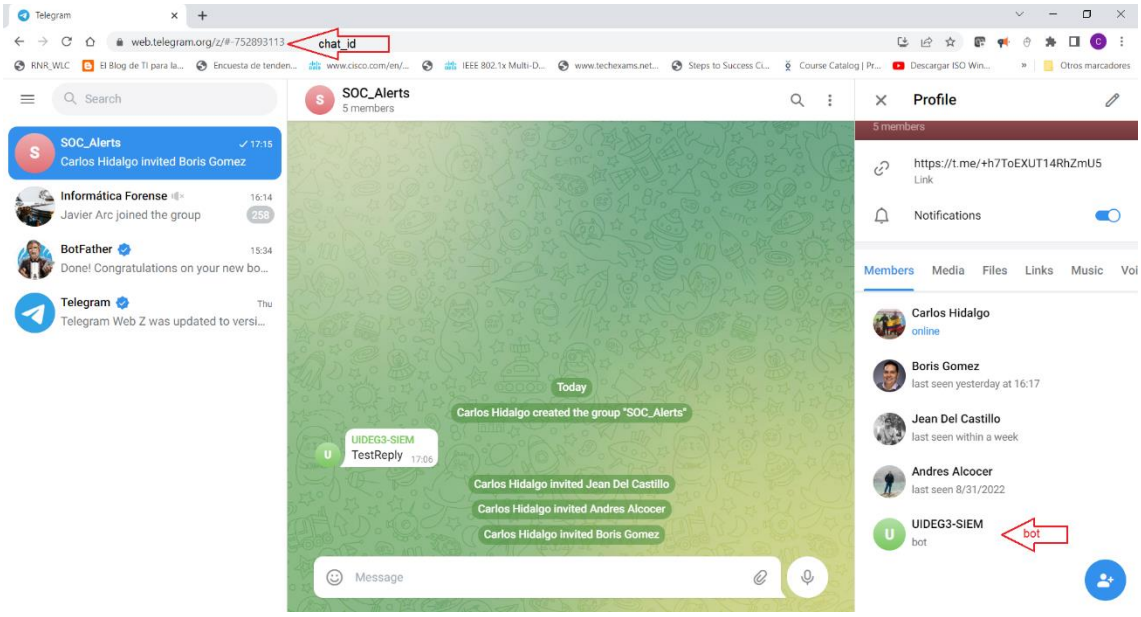


Figura 49

Resultado prueba API Telegram.



Con la validación del funcionamiento de la API (ver figura 49) para envió de mensajes mediante bot, se procede a integrar el API a Logrhythm, mediante el uso del script "MessageTelegram_v13.ps1":

Figura 50

Telegram Push Notification Bot.

```
#--------------Telegram Push Notification Bot----------------------------------#
Param (
    [Parameter(Mandatory=$true)][string]$BotToken,
    [Parameter(Mandatory=$true)][string]$ChatID,
    [Parameter(Mandatory=$true)][string]$User,
    [String]$Host_Impacted,
    [String]$Classification,
    [String]$AlarmID,
    [String]$Date,
    [String]$AlarmName
)
```

Nota. Declaración de parámetros obligatorios y variables

Figura 51

TLS 1.2 Forced.

```
#--------------TLS 1.2 Forced-----------------------------------#
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
add-type @"
    using System.Net;
    using System.Security.Cryptography.X509Certificates;
    public class TrustAllCertsPolicy : ICertificatePolicy {
        public bool CheckValidationResult(
            ServicePoint srvPoint, X509Certificate certificate,
            WebRequest request, int certificateProblem) {
            return true;
        }
    }
"@
[System.Net.ServicePointManager]::CertificatePolicy = New-Object TrustAllCertsPolicy
```

Nota. Forzado de seguridad aplicando TLS 1.2

Figura 52

Concat Strings Messages.

```
#---- Concat Strings Messages------------------------------#
$string0 = "------LogRhythm Push Notification ------"
$string1 = "1. Alarm ID: "
$string2 = "2. Date: "
$string3 = "3. User: "
$string4 = "4. Host: "
$string6 = "6. Classification: "
$string7 = "7. Alarm Name: "
$string00 = "----------------------------------------"
$command = $string0 , $string1,$AlarmID , $string2,$Date ,$string3,$User , $string4,$Host_Impacted , $string6,$Classification , $string7,$AlarmName , $string00 -join "`n"
```

Nota. Concatenado de mensajes de cadenas almacenadas en las variables.

Figura 53

Request API Telegram.

```
#--------------Request API Telegram----------------------—-----#
function Telegram{
$Result = Invoke-RestMethod -Uri "https://api.telegram.org/bot$($BotToken)/sendMessage?chat_id=-$($ChatID)&text=$($command)"
Write-host "Smart Response Executed - Done! -- "$Result
} Telegram
```

Nota. Conexión a la API de Telegram.

Y para poder ejecutar las notificaciones es necesario que bajo las acciones de una alarma se cree la tarea de envió de notificaciones por Telegram con los parámetros:

Enviar una notificación por Telegram.

Tabla 26

Parámetros configuración Telegram en Logrhythm.

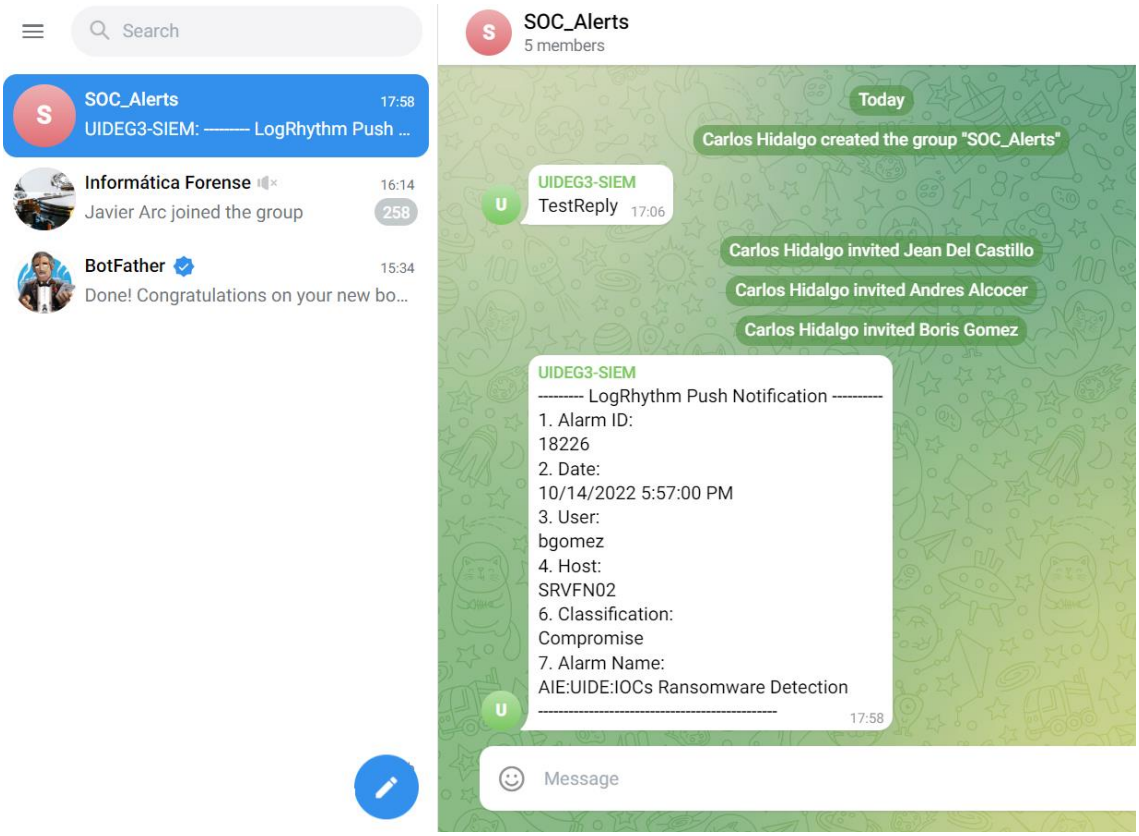
Telegram Alerts v1.3: Send Notification Bot			
Name	Switch	Type	Value
Script	-file C:\MessageTelegram_v13.ps1	Fixed	
BotToken		Constant Value	5679132784:AAF97zfyHuvQeXx6JeRZDrpUW8gzEYNqrU0
ChatID		Constant Value	752893113
User		Alarm Field	<User (Origin)>
Host		Alarm Field	<Host (Impacted)>
Classification		Alarm Field	<Classification>
AlarmID		Alarm Field	<Alarm ID>
Date		Alarm Field	<Alarm Date>
AlarmName		Alarm Field	<Alarm Rule Name>

Nota. La tabla muestra los parámetros de configuración para la acción de Enviar una notificación por Telegram.

Y el resultado se visualiza que el bot envía las alertas vía mensaje al grupo de Telegram configurado:

Figura 54

Resultado integración API Telegrma - Logrhythm.



CAPITULO 5 – CONCLUSIONES Y RECOMENDACIONES

Conclusiones

En este capítulo se expresa el resultado de varios meses de aprendizaje, investigación, trabajo, esfuerzo y dedicación. Durante este ciclo, se pudo aprender y ejecutar acciones de Ciber inteligencia, Hacking Ético Seguridad de teléfonos inteligentes, desarrollo seguro y tecnologías tan interesantes como es el SIEM y otras que serán de gran ayuda en un futuro.

Al terminar el proyecto, se puede rectificar que se ha logrado conocer, configurar e integrar en plataformas SIEM, herramientas necesarias para recolectar logs de diferentes fuentes para tener visibilidad y ejecutar una respuesta adecuada en tiempo real.

Con la implementación de la solución SIEM Open Source Wazuh, se pudo evidenciar que existen herramientas que no son propietarias. Con altas prestaciones que permitirán a las empresas establecer un plan de recuperación anti-desastres con un análisis de riesgos basado en las evidencias que puede encontrar el SIEM en su infraestructura tecnológica. Así como, tener una mayor visibilidad de los logs o registros en tiempo real de los diferentes activos más críticos para las empresas lo que permitirá a los especialistas de seguridad tomar decisiones oportunas para generar acciones preventivas en caso de presentarse comportamientos anómalos.

El SIEM Open Source Wazuh y su contraparte con software propietario LogRhythm presentan soluciones donde se puede apreciar que, por sus propias características, facilitan el control, registro, supervisión y evaluación de todos los registros o logs generados por cada uno de los activos de las empresas. Cada uno posee su propio Dashboard de visualización donde se presentan gráficamente los diferentes eventos de seguridad, suministrando estadísticas que permiten identificar comportamientos anormales en tiempo real y realizar una acción de remediación de manera inmediata. Sin embargo, se pudo constatar la rapidez en el despliegue y generación de filtros. En el caso de LogRhythm cuenta con muchos casos de uso de

correlación pre armados, de igual manera los conectores e interfaz que nos ayuda a crear parsers por medio de expresiones regulares.

Para las 2 herramientas se pudo visualizar un excelente dashboard para que un especialista de seguridad pueda interactuar con las alertas registradas ante comportamientos anómalos, pero con Wazuh no se tiene la certeza que los casos de uso estén correctamente creados ya que algunos de estos se los puede encontrar por ejemplo en GitHub, lo que nos trae la pregunta que es lo mejor en Software de seguridad, Open Source o Propietario, donde el decisor es el cliente con sus necesidades, tiempo de implementación y presupuesto.

Todos los dispositivos se pueden integrar a un SIEM ya sea de una forma nativa (conectores ya establecidos) o con parsers desarrollados por un especialista que conozca los mecanismos de gestión de logs como pueden ser son Syslog, SNMP, Windows log Events o Rsyslog. Sin embargo, dependerá del caso de uso para poder generar un caso de uso para que no sea evaluado como un falso positivo y el SIEM en lugar de ser un apoyo genere más carga de trabajo por el ruido que genera las alertas.

Recomendaciones

Para la elección de un SIEM y su posterior implementación es recomendable evaluar las necesidades del negocio, ya que si se trata de evaluar y registrar un log talvez un SIEM Open Source sea suficiente para una empresa pequeña, pero no así para empresas grandes o medianas con rápido crecimiento y donde se requieran características de nueva generación con su SIEM, como análisis de comportamiento de usuarios y entidades (UEBA), aprovechando la IA y el machine learning, para observar patrones de comportamiento de los usuarios y los sistemas de TI que permitan detectar anomalías de alto riesgo u orquestación. Y la automatización y respuesta de seguridad (SOAR) que permiten automatizar los procesos de respuesta a incidentes, como mitigar un ataque de exfiltración de datos o malware.

Para un buen diseño e implementación de un SIEM se recomienda dimensionar las fuentes de monitoreo, así como los eventos a evaluar, ya que en la práctica no es óptimo analizar todos los eventos y que esto puede acarrear un mal dimensionamiento de los recursos del SIEM, como un gasto innecesario de recursos.

Se recomienda que en las configuraciones de las fuentes de información se filtren los logs y programar que eventos van al correlacionador y cuáles no. realizando una correcta administración de los logs de eventos que quieres que lleguen al correlacionador, esto evitará que los recursos se agoten y poder tener una herramienta optimizada.

Es recomendable mantener un buen programa de retención de los logs generados en el correlacionador, que permitan un desarrollo investigativo y que permita ver tipos de eventos similares que han tenido en determinado tiempo.

Es recomendable que sobre la consola de administración se creen paneles de monitoreo específico que permitan enfocar la revisión en características como tipo de servicio, sistema operativo, gestión de cuentas de AD, integridad de archivos, etc.

Es recomendable que en la configuración de un SIEM se establezca integraciones con herramientas de comunicación empresarial como Slack, Telegram, o en su defecto vía correo, para que la información más importante y crítica sea informada en tiempo real, sin importar donde se encuentre un administrador y pueda saber en tiempo real lo que sucede en sus plataformas de tecnología, simplificando los tiempos de respuesta a los incidentes de seguridad.

REFERENCIAS

Álvarez, A. C. (20 de Abril de 2020). *Grupo ICA*. Obtenido de I.C.A. Informática y Comunicaciones Avanzadas, SL: https://www.grupoica.com/blog/-/blogs/tecnologia-siem-mar-de-dudas-o-confusion-provocada-

Ariganello, E. (2013). Redes CISCO. Guía de estudio para la certificación CCNA Security. En E. Ariganello, *Redes CISCO. Guía de estudio para la certificación CCNA Security* (pág. 402).

Bello, E. (29 de noviembre de 2021). *IEBS Digital School Ciberseguridad: Tipos de ataques y en qué consisten.* Obtenido de https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Bertolín, D. J. (25 de 01 de 2019). *Interempresas*. Obtenido de https://www.interempresas.net/Electronica/Articulos/232650-Integracion-SIEM-SOC-Ciberseguridad-privacidad-motores-clave-esencia-accesibilidad.html

Bridgwater, A. (29 de Enero de 2015). *Forbes*. Obtenido de https://www.forbes.com/sites/adrianbridgwater/2015/01/29/why-users-should-care-about-application-logs/?sh=20d36fb71647

Díaz Lima, F. d. (01 de 08 de 2018). *BUAP*. Obtenido de https://hdl.handle.net/20.500.12371/7634

Ecuador, J. B. (27 de Abril de 2012). RESOLUCIÓN JB-2012-2148. Quito, Pichincha, Ecuador. Obtenido de Super de Bancos: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjN7rzT7d76AhViVzABHZulB3cQFnoECA8QAQ&url=http%3A%2F%2Foidprd.sbs.gob.ec%2Fmedios%2FPORTALDOCS%2Fdownloads%2Fnormativa%2F2012%2Fresol_JB-2012-2148.pdf&usg=AOvVaw3HE2dUeCElURlwficmhRT

Edwards, M. P. (02 de Septiembre de 2021). *ACKTIB*. Obtenido de ACKTIB: https://acktib.com/que-es-siem-y-para-que-sirve/

Electronico, G. (10 de Enero de 2020). Esquema Gubernamental de Seguridad de lnformación EGSI. Quito, Pichincha, Ecuador. Obtenido de Esquema Gubernamental de Seguridad de lnformación EGSI: https://www.gobiernoelectronico.gob.ec/egsi-v2/

Escobar Restrepo, S. N. (31 de ENERO de 2021). *IMPORTANCIA DE LAS DIFERENTES HERRAMIENTAS TECNOLÓGICAS QUE PUEDEN UTILIZAR LOS LÍDERES PARA UN EFECTIVA COMUNICACIÓN EN ENTORNOS VIRTUALES.* Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/39391/EscobarRestrepoSergioNicolas2021.pdf?sequence=3&isAllowed=y

helpsystems. (28 de 05 de 2018). *helpsystems*. Obtenido de https://www.helpsystems.com/es/blog/que-es-un-siem

helpsystems. (28 de 05 de 2018). *helpsystems*. Obtenido de helpsystems: https://www.helpsystems.com/es/blog/que-es-un-siem

IBM. (13 de 10 de 2022). *IBM Qradar*. Obtenido de https://www.ibm.com/es-es/topics/siem

Install, L. P. (12 de Diciembre de 2020). *Desde Linux*. Obtenido de https://blog.desdelinux.net/seguridad-informacion-historia-terminologia-campo/

Latinoamérica, E. (2022). *ESET Security Report.* ESET.

Llamas, J. (13 de 10 de 2022). *Economipedia*. Obtenido de https://economipedia.com/definiciones/software-propietario.html

López, P. (09 de agosto de 2020). *¿Qué es Telegram y para qué sirve?* Obtenido de https://www.geeknetic.es/Telegram/que-es-y-para-que-sirve

Marín Dueñas, P. P., & Gómez Carmona, D. (18 de febrero de 2021). *La gestión de la comunicación digital en las cooperativas españolas.* Obtenido de https://rodin.uca.es/bitstream/handle/10498/24893/2021_301.pdf?sequence=1&isAllowed=y

Mieres, J. (enero de 2009). *Evil fingers*. Obtenido de https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Ramirez, C. A. (18 de Junio de 2020). *LinkedIn*. Obtenido de LinkedIn: https://es.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez

Ramiro, R. (30 de Agosto de 2017). *ciberseguridad.blog*. Obtenido de ciberseguridad.blog: https://ciberseguridad.blog/ueba-user-and-entity-behavior-analytics-deteccion-por-comportamiento/

Redacción, L. (28 de Julio de 2019). *Lab Linux*. Obtenido de Lab Linux: https://laboratoriolinux.es/index.php/-noticias-mundo-linux-/software/24476-seguridad-de-la-informacion-historia-terminologia-y-campo-de-accion.html

Rouse, M. (01 de Agosto de 2017). *ComputerWeekly.es*. Obtenido de ComputerWeekly.es: https://www.computerweekly.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

Schneider, P. S. (10 de Octubre de 2022). *Gartner*. Obtenido de Gartner: https://www.gartner.com/doc/4019750

Solidaria, S. d. (04 de Septiembre de 2018). Resolucion SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-. 2022-002. Resolucion SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-. 2022-002, Pichincha, Ecuador. Obtenido de

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjK3aCf7976AhXQmYQIHVJHC1sQFnoECBEQAQ&url=https%3A%2F%2Fwww.seps.gob.ec%2Fwp-content%2Fuploads%2FSEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf&usg=AO

Suastegui Jaramillo, L. E. (07 de marzo de 2022). *Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19.* Obtenido de http://201.159.223.180/bitstream/3317/18016/1/T-UCSG-PRE-TEC-ITEL-421.pdf

Uriarte, J. M. (18 de Octubre de 2019). *Enciclopedia de Humanidades*. Obtenido de https://humanidades.com/software-libre/