UNIVERSIDAD POLITECNICA DE VALENCIA

DEPARTAMENTO DE COMUNICACIONES

Máster Universitario en Tecnologías, Sistemas y Redes de Comunicaciones

Generación de CiberInteligencia mediante la herramienta SEC para correlación de eventos

Autor: Jhony Patricio Inca López

Director: Dr. D. Manuel Esteve Domingo

Fecha de comienzo: 13/04/2020

Lugar de trabajo: Trabajo en casa

Objetivos —

1. Como objetivo principal de este trabajo se plantea el estudio de la correlación de eventos a través de SEC (Simple Event Correlator) junto a su motor de correlación y lenguaje Perl para la integración con herramientas de gestión de la información, centrada en la seguridad mediante la recopilación de eventos. Para esto se utilizarán herramientas de versión libre enfocadas en la detección y generación de archivos de log para su posterior análisis, filtración y extracción de datos.
    a. Estudiar y comprender las definiciones técnicas, metodológicas de los eventos en los archivos de logs para su posterior manejo y manipulación.
    b. Investigar, conocer y estudiar la estructura de la correlación de eventos, como también sus técnicas y herramientas necesarias para la realización del presente trabajo.
    c. Estudiar Perl como el motor de correlación de SEC y herramienta de generación de expresiones regulares para la correlación de eventos.
    d. Generar una estructura hibrida máquina-hombre a través de la integración de herramientas de software libre con el fin de establecer una herramienta capaz de gestionar logs de información para la visualización de datos procesados para mejor entendimiento por parte del usuario.
    e. Establecer una base de datos para uso y correlación de la información.

Metodología —

- Análisis y estudio de problemática actual, tomando como punto de partida la anterior en analizando los fallos de antiguos intentos por establecer una arquitectura hibrida de SEC en Windows, estableciendo así los objetivos por indagar y desarrollar en este trabajo.
- Establecimiento de límites de parámetros técnicos, como también de herramientas software necesarias para el trabajo de fin de máster.
- Búsqueda y selección adecuada de fuentes bibliográficas para el correcto inicio en los conceptos básicos necesarios para mejor compresión de los temas inmersos que se encontrarán a futuro en el ámbito de la CiberInteligencia y sobretodo en la ciber concienciación mediante el uso de herramientas informáticas nativas de diferentes sistemas operativos.
- Diseño, desarrollo y creación de una herramienta de dominio Open Source basada en un enfoque máquina-hombre debido a la necesidad primordial de uso por parte de un usuario debidamente capacitado.
- Definición del modelo de almacenamiento de datos.
- Comprobar el correcto funcionamiento dentro del sistema operativo Windows integrando las fuentes de información brindadas por las herramientas software.
- Informe escrito, detallando el estudio y desarrollo del trabajo realizado.

Desarrollo teórico realizado —

- Se inició con el estudio bibliográfico de SEC (Simpe Event Correlator), sus técnicas, reglas de correlación y motor de correlación necesario para el desarrollo del trabajo.
- Se realizó un estudio de la problemática que aqueja al sistema operativo Windows el incluir herramientas naturales de Linux.
- Se efectuó el respectivo análisis del software libre a utilizar, tanto el funcionamiento, técnicas, resultado, ventajas y desventajas ante otras, para poder ser utilizadas en la recolección y generación de eventos, para su posterior tratamiento derivando en la generación de inteligencia para la gestión de eventos.
- Se desarrolló el diseño de una arquitectura que muestra la relación correspondiente entre las herramientas de software libre como también su respectiva integración.

Desarrollo de prototipos y trabajo de laboratorio —

- Para entender las técnicas de recolección de eventos a través de la generación de logs se montó un entorno de trabajo físico y virtual, mediante el uso de Nxlog como generador de eventos sintéticos, Syslog Watcher a cargo de recopilar los logs, el desarrollo de la interfaz visual a través de la herramienta de programación Python, el lenguaje de programación Perl para la extracción de información y definición de reglas de correlación y el almacenamiento de bases de datos en Postgres.
- Se creó reglas de correlación en Perl para la filtración de información, se ejecutó subrutinas basadas en el mismo motor de correlación para la coincidencia de patrones de los Logs generados por Syslog Watcher realizando varias pruebas de cotejo.

Resultados —

Al haber estudiado, analizado y entendido las técnicas de correlación de evento y a través del análisis de la información obtenida de los archivos de logs, se logró la integración de cada una de las herramientas, cada una de ella posee su propia y única función por lo que cada una de ellas se considera de suma importancia en el funcionamiento de la aplicación. Posterior a esto se considera la arquitectura máquina-hombre capaz de generar CiberInteligencia capaz de recolectar información, procesarla y filtrarla para su posterior visualización de una manera mejor legible e interpretable ante el ojo humano.

Abstract —

- El presente trabajo de investigación propone a usted una solución para la interpretación y manejo de la información extraída de archivos de logs de uno o múltiples eventos, mediante la creación y prueba de expresiones regulares REGEXP mediante su motor de correlación Perl, integrando herramientas de software libre, para la obtención y análisis de información presente en el ciberespacio para generar una arquitectura hibrida entre máquina-humano. El trabajo se enfoca en la correlación de eventos, recopilación y gestión de información que se manifiesta al encontrar vulnerabilidades de un sistema en uno o varios ordenadores conectados a internet y aún más importante la explotación de brechas de seguridad.
- A términos generales la herramienta realiza la visualización y manejo de la información System, Error y Critical, extraída con expresiones regulares programadas en subrutinas Perl perteneciente a SEC, manejando archivos .txt generados por la herramienta Syslog Watcher después de recolectar logs generados por la explotación de una vulnerabilidad o creación de eventos sintéticos por parte de Nxlog en una o más maquinas físicas o virtuales conectadas a la web.

Autor: Jhony Patricio Inca López, email: jhoinlo@teleco.upv.es

Director: Dr. D. Esteve Domingo Manuel, email: mesteve@dcom.upv.es

Fecha de entrega: 08/09/2020

INDICE

1. Introducción

En la actualidad ya sea que se trate a nivel doméstico o corporativo el sistema operativo Microsoft Windows es el más utilizado a diferencia de sus homónimos, a nivel corporativo la recopilación de eventos y registro de archivos vienen siendo parte fundamental en la gestión y mantenimiento de la red, ligado a esto está la evaluación de seguridad y las actividades forenses. Debido al crecimiento exponencial de las aplicaciones, necesidad de conectividad, teletrabajo, etc, producen una enorme cantidad de datos acerca de eventos, llegando así a crearse especializaciones en big data análisis, haciendo que el manejo de la información sea bastante difícil, por lo que es necesaria y vital la administración de registro y correlación de eventos mismas que son esenciales para las tares de administración, brindando una visión de los incidentes producidos dentro de una red.

Esto ayuda a poder detectar los problemas de seguridad, amenazas, productividad que brinden una acción de alerta es necesaria una herramienta de solución de correlación de eventos, misma que coincide con los eventos en base a los esquemas, patrones y reglas de correlación en un intervalo de tiempo determinado, con el objetivo de identificar una situación de alerta y desembocar en una acción predefinida.

1.1. Planteamiento del problema

Los productos ofrecidos por la empresa Microsoft son los mayor buscados y usados por muchas empresas pequeñas y medianas empresas, más aún para un ordenador para hogar, desconociendo e ignorando los recursos y capacidades de los sistemas operativos UNIX, debido que el manejo de estos sistemas requiere de recurso y talento humano para administrar dicha infraestructura. Desafortunadamente, muchas empresas y usuarios domésticos no implementan una solución para el monitoreo de registros y la identificación de acciones maliciosas, y dependen principalmente de una única solución antimalware. [1]

Actualmente se vive un tiempo muy diferente al acostumbrado, el COVID-19 ha hecho que la mayoría de la población mundial resida en sus hogares y labore de manera virtual es decir el teletrabajo, producto de esto se ha generado un enorme incremento en el consumo de recursos informáticos, como también el crecimiento exponencial de generación de datos, ligado al teletrabajo también han crecido un gran número de informes por alerta de seguridad, esto debido que los atacantes ven una oportunidad de obtener sus intereses de manera más amplia, ya que los ordenadores personales de los cuales son propietarios los trabajadores de las empresas, no poseen la seguridad necesaria y desconocen de los peligros que asechan en la red al trabajar con accesos remotos, dejando así un sistema vulnerable a cualquier tipo de ataque. Se recalca también que ningún sistema es seguro ya que la seguridad se basará en los protocolos y acciones que se toman para prevenir este tipo de conflictos.

La problemática abordada permite en este trabajo de titulación poder proveer de una herramienta informática open source, fácil de implementar y usar en el sistema operativo Microsoft office, debido que éste último carece de un motor PERL nativo de correlación, ayudando así en el monitoreo de registros y la correlación proactiva de eventos basados en reglas de correlación. La correlación de eventos es muy importante ya que ayuda en la detección de eventos de carácter malicioso, identificación, manejo de alertas criticas al desencadenar acciones predefinidas.

1.1.1 Problemática al ejecutar SEC en MS Windows

SEC, Simple Event Correlator [2] (Correlador simple de eventos) está establecido en el lenguaje de programación Perl, que tiene como característica el ser multiplataforma, dentro del sistema operativo Windows aparecen los siguientes problemas:

- SEC es una aplicación de Script Perl, no posee interfaz de usuario para proporcionar una manera fácil y rápida de establecer parámetros de comando requeridos.
- Anteriormente en un intento por ejecutar SEC como un servicio presentó varias complicaciones.
- SEC necesita que el servicio MS Windows se ejecute en el arranque sin interacción del usuario.
- Microsoft Windows no integra un motor Perl nativo [3], por lo que terceros han desarrollado varias distribuciones diferentes de Windows Perl.

1.1.2 Problemática en soluciones alternas y formato de eventos.

Hay que mencionar que existen diversas soluciones de monitoreo y de registro de eventos que capaces de ejecutar en el sistema Windows, éstas se centran en brindar informes analíticos, archivo de registros (logs), variedad de sondas de monitoreo y lo más importante la emisión de alertas en base a la operatividad de la correlación de eventos de manera muy básica. Es necesario comprender que la mayor problemática es la errónea confianza que poseen las empresas en sus sistemas nativos, por ello ignoran la mayoría de soluciones de gestión de eventos de dominio comercial debido a su alto costo ya que están orientadas a nivel empresarial.

Las soluciones gratuitas de código abierto pueden carecer de ciertas funciones y características. Las soluciones de gestión de eventos centralizadas enfocadas en bases de datos y registro de acciones consumen muchos recursos en hardware, software, humanos y financieros. Debido a estas razones surge la necesidad de una herramienta de identificación de incidentes y amenazas en tiempo real.

1.2 Apoyo y contribución del trabajo

Debido a la necesidad producida por la problemática, es necesario la implementación de un sistema confiable que sea centralizado o hibrido de correlación de eventos, destinado a usuarios del sistema operativo Windows a través del uso de Simple Event Correlator, este siendo uno de los primeros lenguajes de programación, de los más fuertes y robustos pero también de los más desconocidos a pesar de existir ya muchos años, se lo escogió como el motor de correlación predeterminado, con su extensa aceptación por parte de la comunidad académica e industrial, flexibilidad, capacidad y de código abierto.

Debido que se realizó una comparación entre distribuciones comunes de MS Windows Perl en cuanto se refiere a características y rendimiento, la cual aludió del uso de Cygwin Perl como emulador de las características del sistema UNIX, del cual dependen en especial operaciones para entrada y salida de disco. También se puede utilizar algunos otros binarios de Cygwin disponibles para acciones de SEC con el propósito de evitar la instalación de software adicional o escritura de scripts.

Un intento anterior de ejecutar SEC como un servicio MS Windows tuvo lugar en 2008 por uno de los miembros de la comunidad SEC y se publicó a través de la lista de correo SEC [4], desgraciadamente no obtuvo éxito, como consecuencia generó necesidad de desarrollo de una nueva herramienta capaz de correr el proceso SEC Perl como un servicio nativo de Windows convirtiendose en un requisito fundamental de para la ejecución de SEC en Windows.

Para lo cual el autor desarrolló una nueva herramienta de correlación de eventos basado en reglas de correlación basado en lenguaje Perl, con interfaz gráfica e instrucciones de código en Python, además de estos ha utilizado otras herramientas como Syslog-Watcher, Notepad++, servidor de Ubuntu, kali Linux y sus aplicaciones asociadas.

La herramienta presentó las siguientes características:

- Interfaz de usuario para configurar parámetros SEC
- Generación de eventos en archivos de texto plano
- Selección y extracción de información
- Control y monitoreo del estado del servicio
- Herramientas para visualización de datos
- Capacidad de exportación en diferentes formatos
- Búsqueda selectiva de información
- Visualización selectiva.

El paquete está disponible como un único archivo que debe ser instalado manualmente, la aplicación se ha compactado como un servicio de MS Windows, formularios de Windows y aplicaciones de consola, todo ello compactado en un ejecutable portátil

En cuanto se refiere a la recolección y transferencia de logs a través de la red, escogió el uso del Syslog-Watcher como la herramienta de registros, esto debido a su robustez sin costo de pago.
Se establecieron conjuntos de reglas de prueba de concepto para SEC destinado al monitoreo proactivo de eventos y la correlación de eventos en Windows.

2 Descripción general

Este capítulo describe la información de manera general para su mejor comprensión, basado en trabajos académicos y publicados en revistas de interés informático acerca de monitoreo de registros, correlación proactiva de eventos y balance de soluciones de monitoreo de registros disponibles que pueden ejecutarse en el sistema operativo MS Windows

2.1 Eventos

Un evento es un registro de un incidente o el informe de un estado que ocurre en un momento con un determinado tiempo que brinda información clara y precisa del acontecimiento, la información presentada en los registros se utiliza para observar el estado, pero en uso general se lo toma para encontrar y analizar anomalías, detectar amenazas, estudio de errores, fallos de sistema, seguridad y depuración. Con todas esas aplicaciones el registro de eventos juega un papel sumamente importante en la administración de sistemas informáticos, análisis forense y auditorias de seguridad desembocando en la solución de problemas de software.
Cada entrada de registro al sistema se considera como un evento único, que se registra y se almacena, esta investigación se enfoca en los registros de seguridad de la plataforma Windows, registros causados por algún incidente, que provocará un registro en el sistema con archivos de texto almacenados en el disco, que generalmente está en formato personalizado y ocasionalmente los eventos también se registran en las bases de datos, mismos que será generado por la herramienta de monitoreo Syslog-Watcher, para su posterior toma de decisiones en base a reglas de correlación programadas en lenguaje Perl que es nativo de Simple Event Correlator.
Microsoft define un evento como cualquier evento significativo en la computadora o en un programa que requiere que los usuarios sean notificados o que se agregue una entrada a un registro [5]. Los registros de eventos de Microsoft Windows [6] se clasifican en cinco niveles de gravedad: informativo, advertencia, error, éxito de auditoría y error de auditoría, donde los dos últimos son eventos de seguridad específicos.

- Aplicación: contiene eventos de la aplicación genérica, los eventos se clasifican como formativos, de advertencia o de error.
- Seguridad: contiene eventos de auditoría de seguridad que se clasifican como exitosos o fallidos
- Configuración: contiene eventos sobre la configuración de aplicaciones nativas de MS Windows, como roles, características, actualizaciones de Windows, etc.

- Sistema: contiene eventos relacionados con las operaciones internas del sistema y la operación de los servicios del sistema MS Windows.

Cualquier programa puede generar alertas en el registro de eventos de MS Windows y Syslog-Watcher adopta dentro de su estructura los cinco niveles de gravedad, a diferencia del registro de eventos del sistema operativo Windows, Syslog-Watcher va más allá, posee una auditoria más ruda y nada flexible, ya que esta es una solución ofertada al entorno corporativo y de empresas, se detalla en el apartado 2.6 la descripción y funciones de Syslog-Watcher.

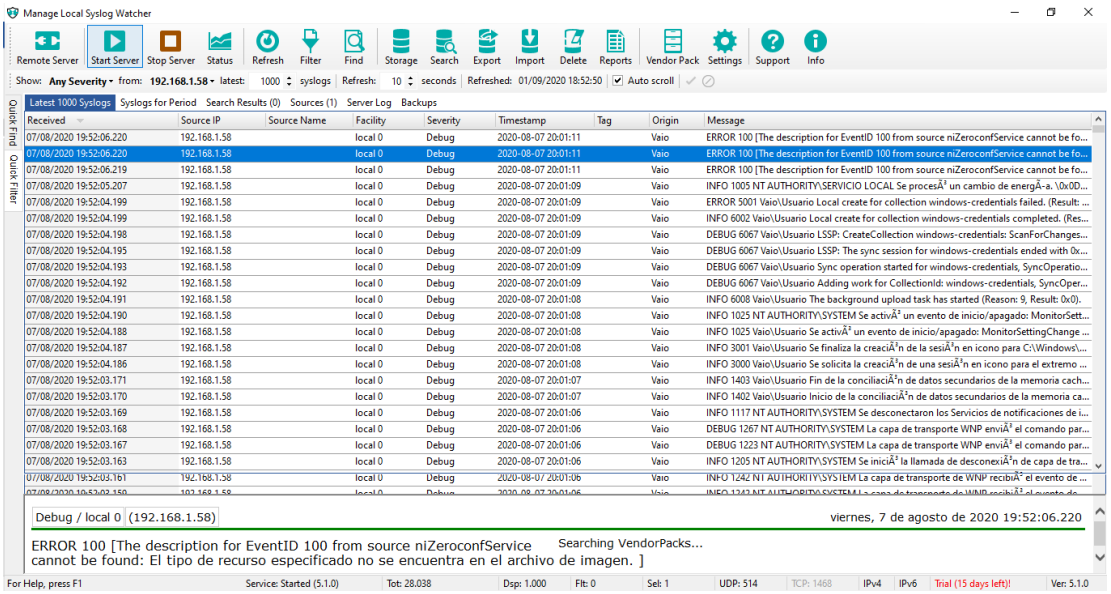

Figura 1. Entrada de registros de evento en Syslog-Watcher

La figura muestra la interfaz gráfica de Syslog-Watcher correspondiente al registro de eventos y emisión de alertas.

2.1.1 Formato de eventos.

Ya que existe variedad de formatos de registro proveniente de una amplia gama de sondas lo cual produce un problema al momento de recolectar y correlacionar eventos provenientes de distintas aplicaciones, existieron diversos puntos de vista y esfuerzos de investigadores para intentar solucionar esta problemática, proponiendo minería de datos basados en algoritmos, protocolos para normalización de registros o los experimentos para automatizar la normalización de registros con uso de protocolos genéricos de formato de registro. Prácticamente el problema persiste como resultado de la falta de reglas de gobierno para evaluar el cumplimiento de formato de eventos de las aplicaciones contra un conjunto de estándares unificados.

Soluciones de código libre y comerciales que efectúan análisis de registros necesitan de su analizador de estructura de eventos sin procesar y se encuentra pre-configurado. Eso evidencia ante la admisión de formatos de registro no determinados la búsqueda necesaria de interacción humana para puntualizar un analizador de registro actualizado, es necesario mencionar que una

herramienta de correlación de eventos y toma de decisiones por más potente y robusta que sea no significará nada si la persona a cargo de su uso no posee las habilidades y el conocimiento requerido para su correcto manejo, por lo que se establece la estricta relación de dependencia entre hombre-máquina y máquina-hombre. Si bien los investigadores han realizado grandes esfuerzos para utilizar estructuras de formato [7] [8]. Se realizó una investigación reciente [9] para definir algoritmos automatizados para extraer información de redes genéricas y eventos de seguridad utilizando un nuevo enfoque nombrado por los autores Log Template Extraction (LTE). Si bien varios investigadores realizaron esfuerzos notables y proporcionaron efectivamente algoritmos para la minería de registros y la identificación de formatos [17] [10] [11] [12] [13], hay esfuerzos continuos para encontrar un formato de registro unificado.

Otro formato de registro más maduro es Graylog Extended Log Format (GELF) [14], proporcionado por Graylog, un productor de software de gestión de registros, para superar la deficiencia de los protocolos syslog. Se han propuesto otros intentos, principalmente con fines específicos para servir tipos específicos de aplicaciones, como servidores web [8] o aplicaciones de seguridad [15] [16].

Uno de los formatos de registro comunes es IETF [17] - RFC5424, usado principalmente por sistemas basados en UNIX, este formato es la versión avanzada de syslog BSD-RFC3164 que es obsoleto, los avances de syslog IETF son en transporte seguro de registros mediante el uso de TLS sobre el protocolo TCP/IP y datos estructurados con extensiones específicas del proveedor, por lo que permite agregar campos adicionales a los eventos

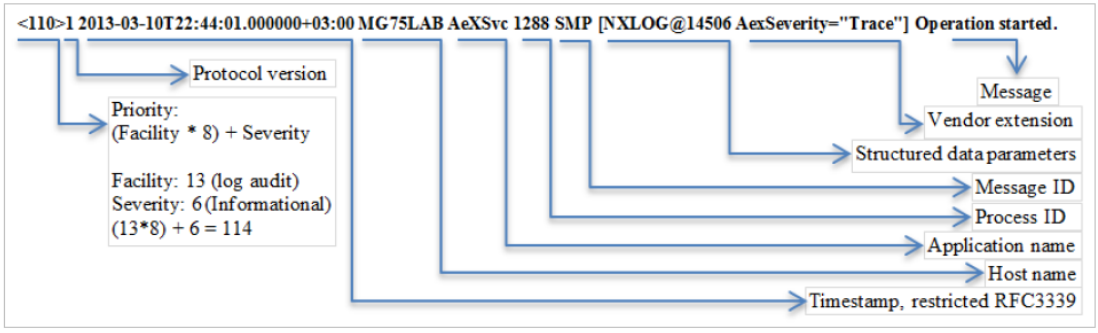

Figura 2. Formato syslog de IETF (RFC5424)

La figura 2 muestra una entrada de syslog IETF, su composición básica de la cual se derivan la mayoría de formatos, detallando cada uno de los campos que lo componen.

2.1.2 Formato en MS Windows

Para el sistema operativo Windows el formato que presenta es diferente [18]; posee un conjunto de campos diferentes basando el almacenamiento de eventos en archivos binarios y administrados con un servicio de registro dedicado nativo.

Los principales campos que presenta un evento en Windows son:

- Nivel: la gravedad del evento (informativo, advertencia o error) y (éxito o falla) para eventos de seguridad
- ID de evento: una identificación de evento única donde cada ID define una categoría específica.
- Registrado: indica hora y fecha de registró del evento.
- LogName: la categoría del registro (aplicación, seguridad, sistema, etc.)
- Fuente: la fuente es la aplicación o servicio de registro.

2.2 Recolección de Eventos

2.2.1 Herramientas de recolección de eventos.

Este apartado provee información acerca de herramientas de recolección de registros de uso de común, fáciles de configurar y gratuitas. Existen varias herramientas disponibles, algunas de ellas se las menciona a continuación con una breve descripción.

- NXLog-ce [20] es una herramienta gratuita de recopilación de registros de propósito general dirigida a varios sistemas operativos y capaz de recopilar eventos de varias fuentes. Su principal ventaja radica en tratar eventos basados en campos, lo que le permite admitir fácilmente varios formatos de registro y normalizar y filtrar eventos fácilmente.
- Beats [21] es una herramienta de recopilación de registros de código abierto, que admite varias fuentes. Beats se divide en cuatro aplicaciones separadas: Packetbeat recopila datos de paquetes de red, Topbeat recopila datos de utilización de recursos, Filebeat recopila eventos de archivos de registro y Winlogbeat recopila registros de eventos de Windows.
- Logstash [22] es otra herramienta de recopilación, normalización y reenvío de registros de código abierto de Elastic, con capacidades de canalización en tiempo real y soporte de complementos personalizados. Depende de los complementos para entrada, salida y filtración.
- Snare agent [23] es una herramienta de recopilación de registros presentada en dos versiones, una comercial que es capaz de normalizarse y una versión gratuita que se limita al formato de registro propio de Snare.
- El reenvío de eventos nativo sin agente [24] es un método nativo en el sistema operativo MS Windows para reenviar eventos de uno o más nodos a otro nodo único, se puede habilitar manualmente o mediante una política de grupo, y solo puede transportar eventos a través del Registro de eventos del sistema operativo Windows.

Destacándose entre las anteriores dos herramientas, que son muy flexibles, las cuales son NXLog-ce y Logstash, soportando varios formatos de registro, transporte y capacidad de normalización.

2.2.2 Recolección de eventos, almacenamiento y recuperación

Los eventos que se producen provenientes de las aplicaciones de manera general se escriben en archivos de texto plano en el disco ya sea en formato .txt, .json, .xml, en cambio otros archivos pueden ser almacenados de una manera diferente como el archivo de eventos de MS Windows que son almacenados en formato binario personalizado [18] en "% windir% \ System32 \ winevt \ Logs" y se consultan a través de API para recuperar valores. Otras aplicaciones poseen la capacidad de almacenar sus eventos en una base de datos, poseen una varias ventajas como lo son:

- Facilidad de opciones de búsqueda y consultas
- Disponibilidad y compartición de datos globalmente.
- Fácil y rápido acceso a los datos.
- Evita datos repetidos o duplicados.
- Escalabilidad.
- Ingreso ilimitado de datos.
- Aumento de rendimiento y productividad.
- Centralización de la información.

Un sistema de registro centralizado puede almacenar el evento recolectado en archivos planos en el disco o en una base de datos, como se menciona en las ventajas esto facilita las operaciones de búsqueda y la capacidad de crear informes. Una de las soluciones de recopilación de eventos conocidas basadas en una base de datos orientada a documentos que utiliza JSON es ElasticSearch [19], que resuelve los gastos generales mediante la detección de la estructura de datos de eventos y crea un índice personalizado.

2.3 Análisis de amenazas actuales de seguridad en la red.

Estudios recientes muestran que las amenazas cibernéticas están en continuo crecimiento, más aún en la pandemia del 2020, a día de hoy las amenazas en línea han aumentado hasta 6 veces sus niveles habituales, comparando medidas anteriores se observa un fuerte aumento en la actividad maliciosa, siendo el phishing la más explotada. La ciberdelincuencia profesional también ha utilizado el incidente global como pantalla para promover sus actividades, estos intentos de phishing se han elevado a niveles del 600% a inicios de marzo, entre las más importantes también se destacan los ataques de extorsión y el compromiso de correo electrónico comercial.

Además del crecimiento elevado de los niveles de amenaza, se observó un aumento en uso general de internet en un 17%, esto producido por el confinamiento y el teletrabajo, aumento en cual las visitas a los sitios de tutoría aumento un 400%, sitios políticos 320%, televisión 210% y jardinería 200%, siendo esto carnada muy deseada por los ciberdelincuentes, el nivel de ataque es alto, los ataques han incluido malware para robar información, como ataques a hospitales, organizaciones,

intentos de robo de información de las vacunas, etc. Son amplios los blancos que ellos poseen, son muchas las opciones que tienen por explotar de las vulnerabilidades creadas por el aumento del trabajo remoto, esto evidencia la necesidad de los sistemas de monitoreo y técnicas de análisis para comprendes las actividades producidas dentro de un sistema. Inicialmente, los especialistas de TI utilizaron los registros para el diagnóstico técnico [25], sin embargo, hoy en día, los registros de auditoría de seguridad se usan ampliamente en corporaciones con alta conciencia de seguridad, e incluso la ley requiere que algunos proveedores de servicios mantengan un archivo de registros.

2.4 Correlación de eventos

La correlación de eventos, según lo definido por Jakobson y Weissman [26], es una manera de interpretación conceptual, en la cual se brinda un nuevo significado a un conjunto de eventos generados por determinada acción durante un intervalo de tiempo predefinido. Esto también indica que se pueden generar eventos sintéticos y reemplazar el con junto original de eventos correlacionados. Dentro de las TICS están correlacionados dos o más eventos si entre si poseen una conexión causal, finalmente la comprensión clara de la causalidad que rodea la producción de un evento no procesado es fundamental para la construcción de reglas proactivas de correlación de eventos.

2.4.1 Técnicas y propiedades de la correlación de eventos

Estas dependen de los enfoques y objetivos deseados por el motor de correlación ya que puede utilizarlo para un uso en específico o para fines generales. Las técnicas generales para la correlación de eventos son:

- Gráfico de dependencia basado [27]: un método de correlación de eventos basado en gráficos, donde todo el sistema de TI se representa como un gráfico. Los dispositivos de red, servidores, aplicaciones y otros componentes del sistema se representan como nodos; mientras que las dependencias entre los componentes del sistema son los arcos del gráfico. Cuando un componente del sistema falla, el gráfico se utiliza para definir otros componentes del sistema afectados.
- Basado en un libro de códigos [28]: un experto humano crea un llamado libro de códigos que consiste en vectores. Cada vector describe una descripción común (o causa raíz) para condiciones de error específicas en el sistema de TI y los componentes del vector corresponden a síntomas de esta condición de falla. Cuando se observan fallas dentro de un sistema de TI, el vector se calcula en función de estas fallas y se busca en el libro de códigos para encontrar una coincidencia o una coincidencia parcial. La coincidencia se informa a los administradores.
- Basado en la red bayesiana [29]: un gráfico a cíclico dirigido, que modela las relaciones probabilísticas entre los componentes del sistema representados por variables aleatorias

- Red neuronal basada [30]: un modelo artificial de inteligencia creado por una red de nodos de procesamiento, que realiza operaciones en las entradas evaluadas para generar salidas, que se utilizan como entradas para otros nodos.
- Basado en reglas [26] [31]: las reglas especifican una relación de condición a acción, cuando uno o más eventos coinciden con una condición, se activa una acción o más.
- Modelo basado [32]: la representación de la estructura y los comportamientos de un sistema bajo observación en un modelo.

Se debe mencionar que no todas las propiedades se aplican a las técnicas y la mayoría de técnicas se pueden usar con diferentes propiedades. Entre las principales propiedades de los motores de correlación son:

- Conocimiento del dominio.
- Autoaprendizaje versus conocimiento externo.
- Datos en tiempo real versus datos almacenados.
- Sin estado vs. Con estado.
- Pasivo frente a activo.
- Centralizado versus distribuido.
- Política predeterminada.
- Pérdida de información.
- Transparencia.
- Robustez.
- Mantenibilidad.
- Conocimiento profundo versus conocimiento superficial.

2.4.2 Arquitectura de correlación de eventos

La correlación se enfoca en eventos centralizados y distribuidos, el enfoque distribuido ha sido adoptado utilizando SEC por J. Myers et al. [33], indica varias desventajas de la arquitectura. El diseño distribuido se basa en la correlación de eventos en el nodo que produce los eventos en sí. No es necesario decir que un sistema de gestión de registros centralizado requerirá amplios recursos de personal humano para poder realizar tareas de auditoría. Una visión más amplia de incidentes producidos posee la correlación de eventos centralizada, esta arquitectura está enfocada en el transporte de eventos con el uso de la red, misma que proviene de nodos que producen los registros, esto genera tráfico intensivo en la red, solucionándose en base al filtrado de eventos que posea cada nodo o mediante un servidor de registro, actuando como puerta de

enlace(GATEWAY), es necesario prever una alta demanda de recursos dentro del servidor correlador de eventos principal que ocasionaría una obstrucción ante la mejora en escalabilidad.

2.4.3 Enfoque híbrido

Éste enfoque se realiza combinando dos enfoques de correlación mencionados anteriormente como: centralizados y distribuidos, en dos fases. La primera sigue un punto de vista distribuido de correlación de eventos para cada nodo, la segunda a través del transporte de eventos sintéticos y críticos distribuidos a un servidor de registro en él cual se encuentra el motor de correlación con función de desarrollar acciones amplias. Como ejemplo a esto: una IP que se encuentra generando diferentes eventos derivando en fallas de autenticación en un lapso determinado de tiempo, se bloquea esa IP durante unos minutos por activación de una acción, a continuación, se produce un evento sintético y se traslada al motor de correlación centralizado, el cual valora el número de incidentes recibidos, fuentes, destinos y finalmente correlaciona con terceros eventos enviados para tomar una amplia operación.

2.4.4 Soluciones de monitoreo y correladores de eventos comunes.

El análisis comparativo entre las herramientas de correlación de eventos existentes ha recibido cierta atención de los investigadores en los últimos años [34] [39]. No obstante, se optó por el uso de sistemas basados en UNIX.

Con el fin de cumplir los objetivos de este trabajo de investigación de proveer de una solución de correlación de eventos proactiva, gratuita capaz de ser ejecutada en el sistema operativo MS Windows se ha realizado una comparación entre el monitoreo común y soluciones de correlación de eventos. Las comparaciones de estas soluciones presentan características que se basan en documentación que muestran las capacidades de cada herramienta como:

- LOGalyze [35] es un monitor de red y gestión de registros centralizado gratuito con capacidades de análisis de datos en tiempo real basadas en Java.

  Ventajas:

  - Recopilación de registros sin agente y sin agente
  - Capacidades de normalización
  - Conjunto de informes pre empaquetados
  - Gratis

  Desventajas:

  - Requiere amplios recursos
  - Características limitadas del motor de correlación.
  - Se sabe que el marco de Java carece de seguridad sólida.
- ElasticSearch ELK Stack [19] es un conjunto de recopilación de utilidades combinadas para crear una plataforma de análisis y búsqueda de extremo a extremo. Se considera

como una solución estable y hacen uso de esta Microsoft, Netflix, Adobe, CISCO, eBay y algunos otros más. Posee varias herramientas en su colección y las principales son:

Logstash: herramienta flexible de recolección y transporte de eventos de código abierto basada en Java.

ElasticSearch: motor de análisis y búsqueda de código abierto distribuido con características de alta escalabilidad.

Beats: conjunto de herramientas y marco de recolección de registros y transporte.

Otras utilidades de código abierto adicionales: Beats, Watcher, Shield, Elastic Cloud, Marvel, Elasticsearch para Apache Hadoop.

Ventajas:

- Gratis y de código abierto
- Capacidades de monitoreo y alerta
- Una colección bien diseñada de herramientas gratuitas, que se combinan para formar una plataforma poderosa para la gestión de eventos.
- Documentación y tutoriales precisos y fáciles de seguir.

Desventajas:

- Filtrado de registros, que no promueve el nivel del motor de correlación.
- Los módulos de motor de correlación disponibles son comerciales y costosos.
- Requiere amplios recursos
- Requiere especialistas calificados para el ajuste fino

- Esper / NEsper [36] son marcos de código abierto basados en Java y .NET para el procesamiento de eventos complejos (CEP). Los marcos de Esper y NEsper ayudan al desarrollo rápido de aplicaciones que procesan eventos de registro. No pueden actuar como correlacionadores de eventos listos para usar y también necesitan bibliotecas de terceros adicionales.

Para el avance del trabajo de investigación se han utilizado varias herramientas que han brindado el soporte requerido para las pruebas, por lo que es necesario su reconocimiento en el trabajo con su propio inciso.

2.5 Simple Event Correlator

Siendo ésta, parte de las soluciones de monitoreo mencionadas en el apartado anterior, es necesario el detalle de esta herramienta que fue escogida para el desarrollo del trabajo de investigación. Simple Event Correlation [2], SEC se trata de un motor de correlación en tiempo real muy poderoso, ligero para administración de redes, seguridad y monitoreo de archivos de logs, detección de fraude la cual es de mayor importancia y otras tareas que están involucradas en la correlación de eventos. Se encuentra escrita en lenguaje Perl, por tanto se basa en ese lenguaje

y requiere una instalación adicional de la distribución de Perl para el funcionamiento correcto en Windows. Perl otorga funciones adicionales como almacenamiento de eventos en base de datos.
Simple Event Correlator como motor de correlación predeterminado obtiene extensa aprobación académica e industrial debido a su flexibilidad, capacidades, madurez y mejor su código abierto, se considera a SEC como un script de Perl lo que resulta ventajoso ya que lo hace multiplataforma, como es de conocimiento MS Windows escasea de un motor Perl nativo, esto hace necesario el desarrollo de motores Perl perfeccionados por terceros.
Simple Event Correlator está codificado como un script de Perl, un lenguaje interpretado y las características requeridas del motor de correlación son:

- Procesado de ingreso de eventos en tiempo real.
- Flexible configuración.
- Capacidad de producir eventos sintéticos.
- Eficacia.
- Mantenimiento y actualización frecuente de decisiones de correlación.
- Menor consumo de recursos.
- Escalabilidad.
- Correlación activa.

2.5.1 Capacidades

SEC y sus capacidades podrán ser usadas y perfeccionadas en base a la capacidad de uso y desarrollo por parte del usuario, basándose en la capacidad de correlacionar eventos producidos en tiempo real, las capacidades de SEC:

- Clases de reglas: Los tipos de reglas del módulo del motor de correlación NXLog-ce son más o menos equivalentes a los tipos de reglas Single, Supress, Pair, PairWithWindow y SingleWithThreshold SEC. SEC tiene una rica colección de tipos de reglas adicionales, como EventGroup y Jump. Además, las reglas SEC pueden combinarse para operaciones de correlación más avanzadas.
- Eventos sintéticos: SEC es capaz de generar eventos sintéticos, que se utilizan para activar otras reglas.
- Unir reglas en esquemas de correlación de eventos: Utilizando contextos, eventos sintéticos y otras medidas de intercambio de datos. Las reglas pueden crear, modificar o eliminar contextos, mientras que otras reglas validan esos contextos lado a lado para la coincidencia de eventos. Otra forma es generar eventos sintéticos por conjunto de reglas que desencadena su conjunto de reglas.
- Coincidencia avanzada de eventos con la función Perl: El uso de expresiones regulares permite el análisis flexible de eventos, pero tiene inconvenientes, como la utilización

intensiva de recursos y la falta de capacidad de operaciones matemáticas. SEC permite el uso de la función Perl como tipo de patrón, esta característica permite una forma muy flexible de hacer coincidir eventos y aprovechar los módulos Perl, para realizar procesos de evaluación como la definición de la red de una dirección IP.

- Usar variables de coincidencia en nombre y almacenamiento en caché de coincidencias: SEC admite variables de coincidencia de nombre y almacenamiento en memoria caché de coincidencias, para minimizar la utilización de recursos mediante el uso de mapas variables y tipos de patrones en caché. Por ejemplo, una regla puede analizar un evento usando una función Perl y luego crea una tabla hash de pares de campo-valor. La tabla hash puede ser utilizada por otras reglas para la coincidencia. Este método evita el análisis redundante de eventos.

La capacidad de SEC para crear reglas le permiten una ejecución temporalizada y planificada, dicho de otra manera, posee capacidad de generar una correlación eventos automáticos, suponga la búsqueda y correlación eventos un fin de semana o festivo en la cual el usuario está libre, se podrá hacer uso de esta herramienta.

2.5.2 Fallos en intento de ejecución de SEC como servicio

Anteriormente se trató de ejecutar SEC como un servicio MS Windows, publicándose para la comunidad y sus miembros las razones por las cuales no tuvo éxito y fueron:

- Actualización para SEC solicita la edición manual de su archivo de script.
- Necesita de ActiveState Perl, ya que limita la interacción con el proceso como resultado de falta de características en los sistemas propietarios de UNIX, como envío de señales de interrupción.
- Depende del módulo personalizado ActiveState Perl Win32 :: Daemon aportado por el miembro de la comunidad Perl Dave Roth. La última actualización del módulo fue en junio de 2003 [37], mientras que la última actualización de ActiveState Perl fue en marzo de 2013; al momento de escribir este estudio.
- Problema popular de bloqueo con el uso de acción de comando en Shell: shellcmd.

Estas dificultades han hecho del intento algo no confiable, destacando la necesidad de una solución segura y confiable que permita ejecutar el proceso SEC Perl en MS Windows como un servicio.

2.5.3 Mecanismos de adquisición.

El mecanismo de adquisición se produce a través de archivos de configuración de SEC o por generación de expresiones por medio de la interfaz web, es decir por medio de instrucción directa

de REGEXP (Expresiones regulares) mediante la creación, edición o modificación de las mismas dentro de las cuales lleva parámetros como: tipo de entrada y acciones

Otro mecanismo es directamente o un generador de archivos de SEC, del mismo modo configurando o creando expresiones regulares para poder coincidir en la correlación de la información que se necesita extraer.

El módulo NXLog-ce (pm_evcorr) [20] es un módulo dedicado dentro de la herramienta de recopilación de registros NXLog-ce, que actúa como un motor de correlación. Está codificado utilizando lenguaje de programación objetivo C. Esta herramienta es de gran importancia debido que puede producir eventos sintéticos necesarios para un entorno de pruebas en conjunto con la herramienta Syslog Watcher. Ésta es una de las herramientas de software que contribuyen a la realización del trabajo de investigación.

2.6 Syslog-Watcher

2.6.1 ¿Qué es syslog?

Syslog es un protocolo estándar que se utiliza para el envío de mensajes de eventos o registros del sistema hacia un servidor syslog específico, del cual su función principal es recolectar diversos registros provenientes de dispositivos y varias máquinas diferentes hacia una unica ubicación central Este protocolo se encuentra habilitado en enrutadores, conmutadores, cortafuegos conocidos en su mayoría como equipos de red, inclusive se encuentra presente en algunos scaners e impresoras.

Syslog watcher incluye tres niveles de licencia, dos de ellos son versión pago que oscilan entre los 99 y 100 dólares americanos, el restante es una licencia gratuita de no uso comercial con limitación de hasta cinco fuentes de syslog, se mencionó que esta sería la versión a utilizar.

En su mayoría utiliza el protocolo UDP en el puerto 514 destinado para syslog, pero es configurable para cualquier puerto, además se permite utilizar en algunos dispositivos el puerto 1468 en TCP para confirmación de entrega de mensajes. Además, Syslog Watcher está disponible para sistemas basados en Unix.

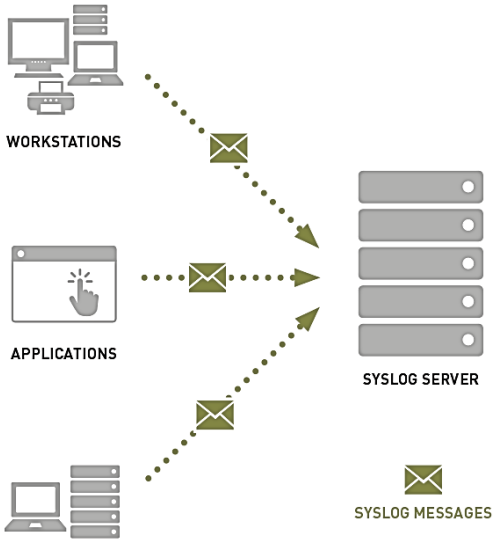

Figura 3. Entorno de función de syslog

El mensaje se conforma de tres partes:

PRI: el valor de prioridad, de 0 a 23, que categorizan el tipo de mensaje.

HEADER: cabecera con información de identificación, que clasifica por importancia o severidad del mensaje en un rango de 0 a 7.

MSG: cuerpo del mensaje, en el cual no suele tener más de 1024 bytes.

Código	Gravedad	Descripción
0	Emergencia	Sistema no disponible
1	Alerta	Tomar acciones urgente
2	Crítico	Condiciones de trabajo nivel crítico
3	Error	Condiciones de trabajo nivel error
4	Advertencia	Condiciones de advertencia
5	Aviso	Precaución de operación, tomar precauciones
6	Informativo	Mensajes de información
7	Depurar	Nivel de depuración, debug

Tabla 1. Valores de categorización para cabecera.

En general los mensajes varían de acuerdo a su tipo, pero mantienen su estructura definida por:

07/08/2020, 19:47,Debug,192.168.1.58,ERROR 100 [DESCRIPCION]

Las líneas anteriores muestran un ejemplo de un mensaje recibido, componiéndose de:

Fecha: 07/08/2020, 19:47

IP: 192.168.1.58

Tipo de error: ERROR 100

Descripción: The description for EventID 100 from source niZeroconfService cannot be found: El tipo de recurso especificado no se encuentra en el archivo de imagen.

El protocolo syslog no brinda algún mecanismo u acción de seguridad por lo existe una autenticación incorporada que brinde garantía de los mensajes entrantes sean provenientes de del

equipo o dispositivo que dice estar enviándolos, esto lo hace susceptible a los ataques de reproducción.

3 Correlación de eventos en Microsoft Windows y manipulación de información para filtración, extracción y envío a otras herramientas.

Este capítulo muestra una implementación propuesta para usar el motor de correlación SEC en Microsoft Windows. Se presenta la arquitectura en la cual se basa el desarrollo del trabajo de investigación misma que muestra la integración de las herramientas software de versión libre. Se cubren los aspectos principales de la aplicación desarrollada, que integra el proceso SEC Perl para ejecutarse como un servicio. El uso de NXLog como herramienta de recopilación de registros, que incluye asegurar el transporte de eventos de forma segura como también la integración de Syslog watcher como el instrumento generador de archivos txt contenedores de información, misma que se extrae y filtra con el uso del motor de correlación y lenguaje de programación Perl a través de creación de expresiones regulares REGEXP, se busca extraer la información que contenga “ERROR #”, “IP” y “DESCRIPCION”, desechando el resto, los datos se almacenan y recopilan en una base de datos y se exportan hacia otra herramienta que se encarga de brindar la interfaz visual con programación en Python, dando así una herramienta de correlación y visualización de eventos para el análisis respectivo por parte de usuarios entendidos en el tema.

3.1 Requisitos del motor de correlación y herramienta de recolección de eventos

Esta sección destaca los requisitos del motor de correlación y la herramienta de recopilación de registros necesarios para la implementación propuesta en este trabajo. Tomando en cuenta el caso de uso y la capacidad de proporcionar una solución de correlación de eventos multipropósito, entre las características requeridas del motor de correlación:

- Procesado en tiempo real de eventos entrantes
- Configuración flexible con expresiones regulares.
- Generación de eventos sintéticos.
- Mantenimiento, decisiones de correlación transparentes y actualizaciones frecuentes
- Ligero, mínimo consumo de recursos posible
- Eficacia.
- Escalabilidad
- Correlación activa
- Distribuible capacidad de centralización

Los requisitos para la herramienta de recopilación de registros son: se puede tomar esta sección.

- Posibilidad de recopilar registros de eventos de Windows
- Capacidades de normalización de registros

- Registre el transporte de manera segura, se favorece el cumplimiento de RFC5425
- Soporte de múltiples formatos de registro comunes en un formato de syslog particular
- Ligero
- Configuración bien documentada y fácil

El reenvío de eventos nativos del sistema operativo Windows no es fácil de configurar, no admite otras fuentes de registro y aún requeriría una herramienta para alimentar su contenido a la SEC, que se promovió anteriormente como motor de correlación.

3.2 Características y rendimiento de las distribuciones de Microsoft Windows Perl

Las principales distribuciones de Perl para MS Windows según la página de descarga de Perl.org son ActiveState Perl [38], Strawberry Perl [39] y DWIM, un derivado de código abierto de Strawberry Perl. Además de los mencionados, Cygwin [40], una colección de herramientas GNU y de código abierto que proporcionan una funcionalidad similar a una distribución de Linux en Windows, proporciona la distribución de Cygwin Perl. Cygwin Perl se ejecuta en Windows en un entorno UNIX prácticamente emulado con la ayuda de bibliotecas especiales de Cygwin. Hay disponibles otras distribuciones de Windows Perl, derivadas principalmente de las distribuciones principales mencionadas anteriormente. Esta sección proporciona una lista de características para cada distribución principal, en particular las características que afectan las operaciones de la SEC y la implementación propuesta.

Características de ActiveState Perl 5.22.1.2201:

- Fácil de instalar como un único paquete MSI
- Incluye la utilidad de administración de paquetes PPM, que permite la instalación de módulos adicionales y agregar repositorios adicionales
- Disponibilidad de soporte comercial
- Admite módulos de compilación de usuario
- El tamaño del paquete es 28.5 MB, en el disco 117 MB

Características de Strawberry Perl 5.22.1.2:

- Fácil instalación a través de un único paquete MSI
- Incluye el compilador gcc más herramientas relacionadas, todas las bibliotecas externas para compilar módulos adicionales
- Utiliza cpan para la instalación de módulos adicionales.
- El tamaño del paquete es 83 MB, en el disco 112 MB más la cadena de herramientas 311 MB

Características de Cygwin Perl 5.22.1:

- Fácil instalación a través del instalador de interfaz de usuario único

- Incluye cpan, pero los módulos se pueden compilar a través de Cygwin gcc
- Portabilidad: aunque por defecto Cygwin se proporciona como un instalador ejecutable, que a su vez instala los paquetes seleccionados. Se encontró que los archivos binarios eran totalmente portátiles y capaces de ejecutarse sin instalación siempre que se transporten con sus dependencias requeridas.
- El tamaño de la suma de Tarball es de 39 MB, en el disco 129 MB
- Cygwin como emulación avanzada de sistemas UNIX, es requerida por varias características SEC, como:
- Canalización con nombre: entrada SEC desde una tubería con nombre
- Bifurcación de proceso: separación de SEC y ejecución en segundo plano
- Señales: señales de interrupción utilizadas para varios comandos SEC
- Se pueden usar otros binarios de Cygwin para diversas operaciones.

La conclusión de comparar la lista de características anterior es que las distribuciones ActiveState Perl y Strawberry Perl pueden considerarse iguales desde la perspectiva de las características requeridas para ejecutar SEC.

3.3 Diagrama de relación e integración de herramientas software

Después del análisis y estudio de software existente, que poseen similares características, se optó por usar las herramientas presentes en la figura 4.

Se desarrolló una aplicación basado en el lenguaje de programación Python, la cual provee la interfaz gráfica a la herramienta, como se puede observar en la figura anterior, cada uno de los softwares tiene relación y estricta dependencia con los demás.

Todas las máquinas virtuales comenzaron y detuvieron las operaciones de correlación al mismo tiempo, mediante el envío de entradas de registro definidas, emparejadas por el motor de correlación NXLog que activó el inicio y la detención del servicio. Inició con la generación y recolección de eventos con Syslog Watcher, para esto se utilizaron dos máquinas físicas con sistema operativo Windows y Kali Linux.

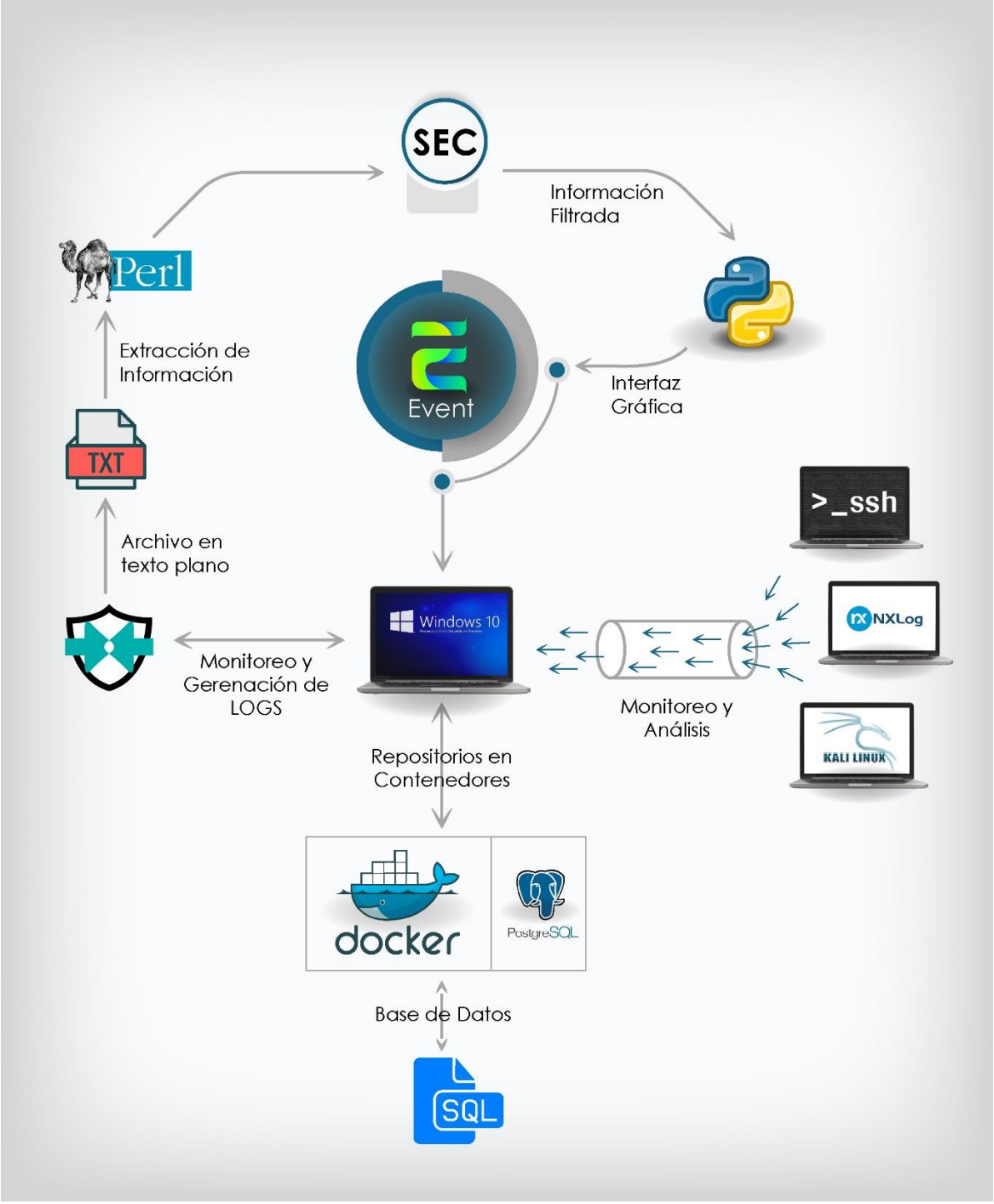

Figura 4. Esquema de integración de herramientas

Se buscó generar los eventos mediante intentos de intrusión y accesos remotos habilitando los puertos respectivos para cada protocolo, al producirse los eventos se monitorean y almacenan ordenados por hora y fecha de ejecución.

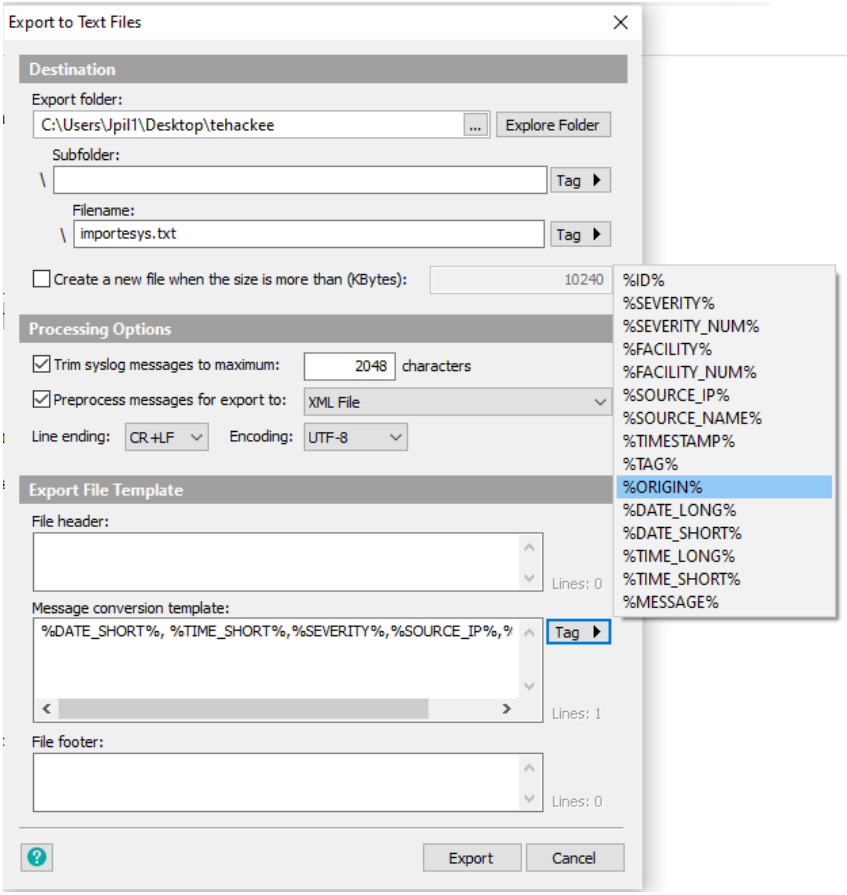

Figura 5. Syslog Watcher – Exportación de información.

A continuación, Syslog Watcher posee la función de exportar la información en distintos formatos, rango de tiempo seleccionado o mejor aún con los Tags preferidos, ya sea fecha, hora, ip, id, severidad, etc, estos tags dependerán de la información que el usuario necesite, se recomienda exportar el archivo en extensión .txt en la carpeta que se encuentran los scripts de perl, estos scripts poseen subrutinas que realizan la filtración y extracción de información en base a coincidencias de expresiones regulares, la información necesaria a extraer es: “ERROR #”, “IP” y “DESCRIPCIÓN”, estos datos se almacenaran en un array de 3 dimensiones para su posterior ingreso a la base de datos en SQL para su fácil acceso y manejo. Asegurarse que el formato de exportación sea el mismo, en este trabajo se utilizó el formato UTF-8. Los datos serán utilizados para presentarlos mediante la interfaz gráfica programada con el lenguaje Python.

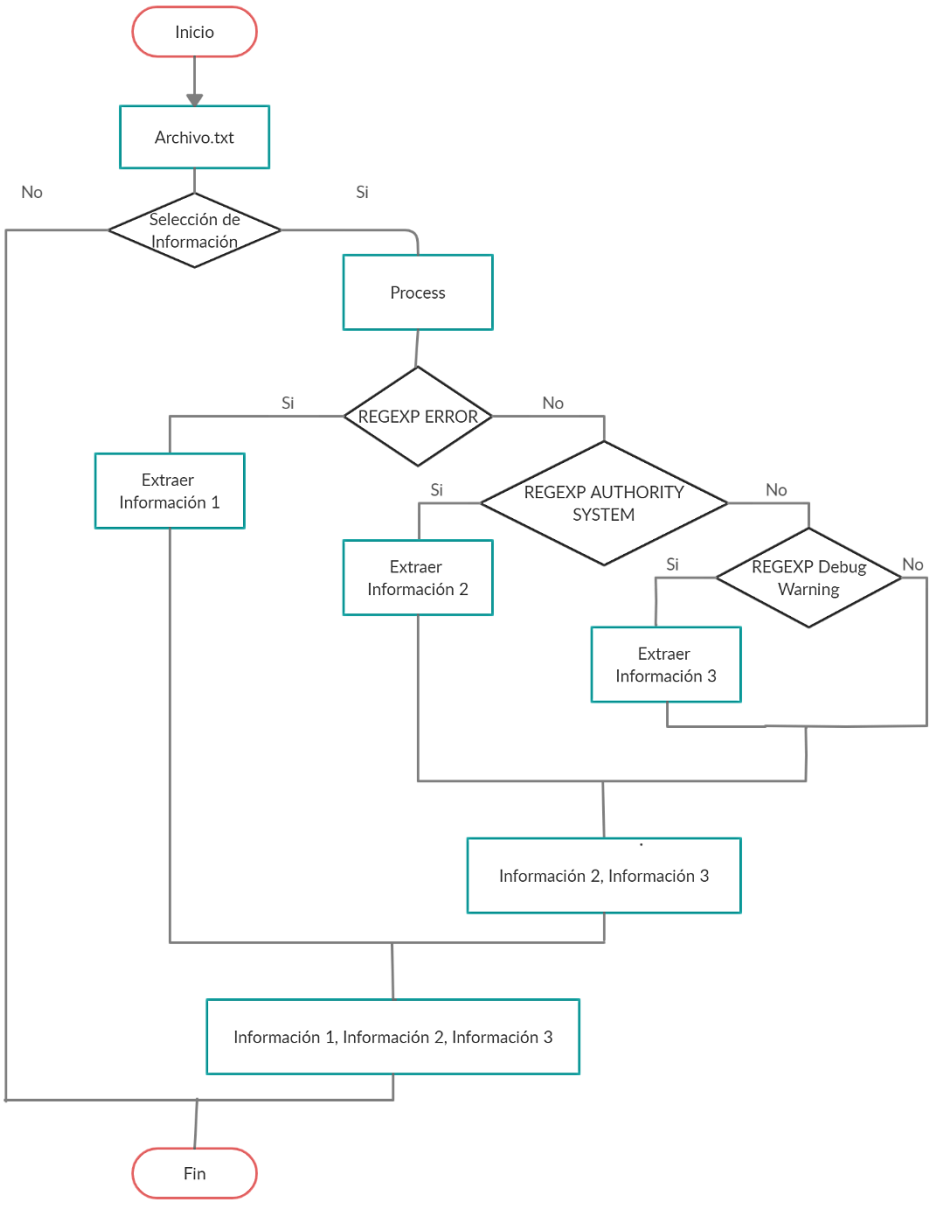

Figura 6. Diagrama de flujo para manejo de información en archivo texto plano

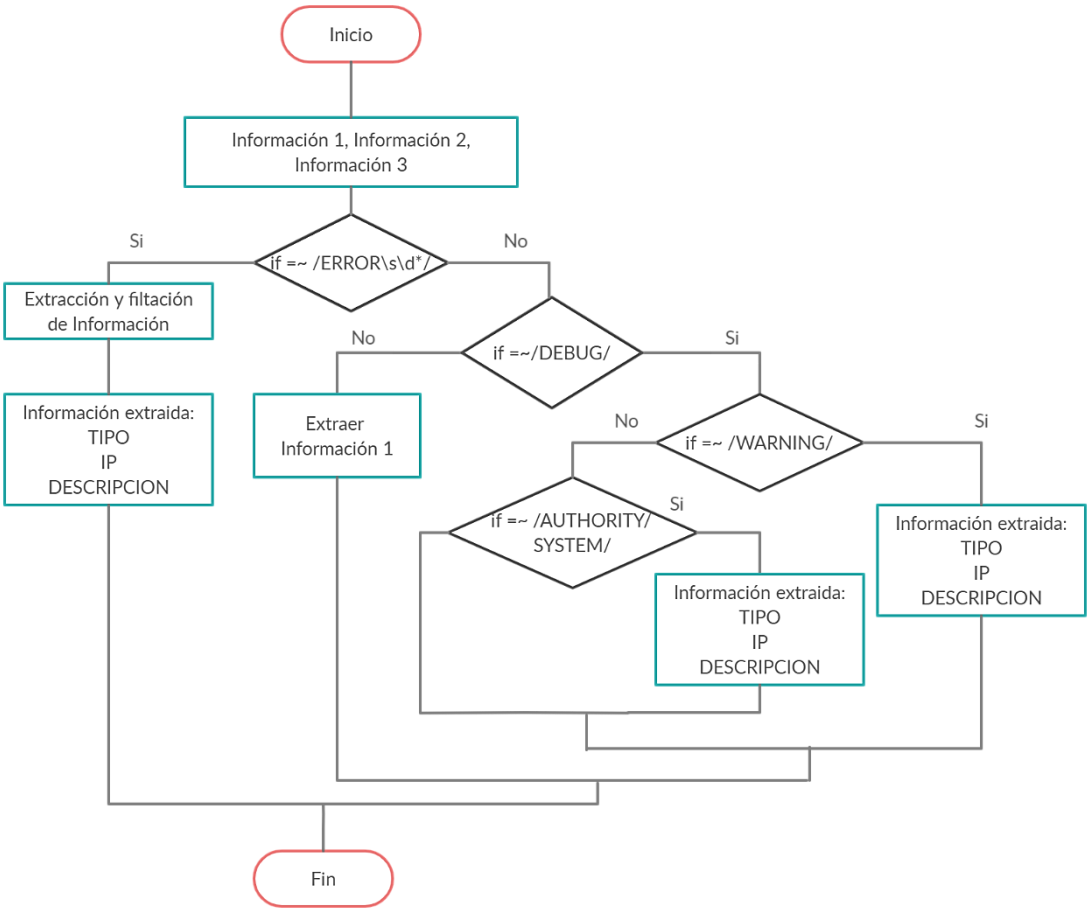

Figura 7. Filtrado de información con expresiones regulares

Los datos extraídos con el uso de expresiones regulares y las reglas de correlación de eventos en el lenguaje perl, motor de correlación de SEC, se añadieron a un array multidimensional [Tipo, IP, Descripción], y a su vez asignado a la base de datos por su facilidad de manejo, se manejó mediante una estructura [x, y, z] representando los valores anteriores, extrayéndolos secuencialmente.

El resultado de la prueba usando los conjuntos de expresiones regulares con una exportación en un rango limitado de veinte minutos proceso un total de 618 líneas con distinta información.

3.4 Módulo de Integración

En la figura 7 muestra la arquitectura de integración, misma que se encarga de adquirir y gestionar la información para su combinación y posterior almacenamiento en la base de datos.

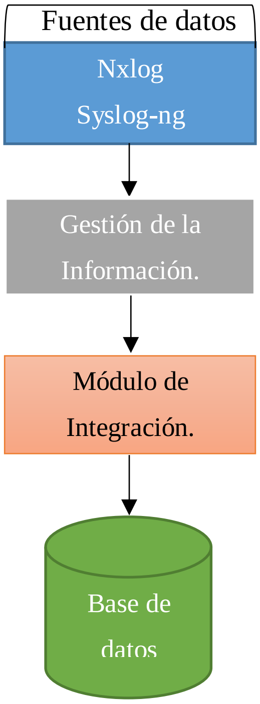

Figura 8. Módulo de integración.

3.5 Descripción general de interfaz de la herramienta

La herramienta inicia sus operaciones al manejar el archivo .txt generado a través del uso de Nxlog y Syslog Watcher, este archivo posee una serie de líneas de texto poco entendibles a simple vista como muestra la figura a continuación.

```
importesys.txt: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
,ERROR 100 [The description for EventID 100 from source niZeroconfService cannot be found: El tipo de recurso especificado no se encuentra en el archivo de imagen.  ]
,ERROR 100 [The description for EventID 100 from source niZeroconfService cannot be found: El tipo de recurso especificado no se encuentra en el archivo de imagen.  ]
,ERROR 100 [The description for EventID 100 from source niZeroconfService cannot be found: El tipo de recurso especificado no se encuentra en el archivo de imagen.  ]
,INFO 1005 NT AUTHORITY\SERVICIO LOCAL Se procesÃ³ un cambio de energÃ-a. \0x0D\0x0A\0x0D\0x0A Motivo: El sistema estÃ¡ suspendiendo la operaciÃ³n
,INFO 16 NT AUTHORITY\SYSTEM El historial de accesos en el subÃ¡rbol \??\C:\Users\Usuario\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Settings\settings.dat s
,AUDIT_SUCCESS 4672 Se asignaron privilegios especiales a un nuevo inicio de sesiÃ³n.\0x0D\0x0A\0x0D\0x0ASujeto:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-18\0x0D\
,AUDIT_SUCCESS 4624 Se iniciÃ³ sesiÃ³n correctamente en una cuenta.\0x0D\0x0A\0x0D\0x0AFirmante:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-18\0x0D\0x0A\0x09Nombre
GUID de inicio de sesiÃ³n:\0x09\0x09{00000000-0000-0000-0000-000000000000}\0x0D\0x0A\0x0D\0x0AInformaciÃ³n de proceso:\0x0D\0x0A\0x09Id. de proceso:\0x09\0x090x36c\0x0

,INFO 5520 NT AUTHORITY\SYSTEM La directiva de desbloqueo de dispositivo no se ha configurado en este dispositivo.
,AUDIT_SUCCESS 4798 Se enumerÃ³ la pertenencia a grupos locales de un usuario.\0x0D\0x0A\0x0D\0x0AFirmante:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-18\0x0D\0x0A\
,AUDIT_SUCCESS 5379 Las credenciales del Administrador de credenciales se leyeron.\0x0D\0x0A\0x0D\0x0AAsunto:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-21-27026750
,AUDIT_SUCCESS 5379 Las credenciales del Administrador de credenciales se leyeron.\0x0D\0x0A\0x0D\0x0AAsunto:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-21-27026750
,AUDIT_SUCCESS 5379 Las credenciales del Administrador de credenciales se leyeron.\0x0D\0x0A\0x0D\0x0AAsunto:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-21-27026750
,AUDIT_SUCCESS 5379 Las credenciales del Administrador de credenciales se leyeron.\0x0D\0x0A\0x0D\0x0AAsunto:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-21-27026750
,AUDIT_SUCCESS 5379 Las credenciales del Administrador de credenciales se leyeron.\0x0D\0x0A\0x0D\0x0AAsunto:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-21-27026750
,ERROR 3000 Vaio\Usuario onecoreuap\shell\roaming\cloudcommon\policies\cloudsyncpolicymanager.cpp(275)\OneDriveSettingSyncProvider.dll!00007FF8C275D26C: (caller: 00007F
,ERROR 1018 Vaio\Usuario Policy document failed to download. (Result: 0x80040410)
,ERROR 3000 Vaio\Usuario onecoreuap\shell\roaming\cloudcommon\liveapi\livestorage.cpp(400)\OneDriveSettingSyncProvider.dll!00007FF8C273A173: (caller: 00007FF8C275CCF4)
,ERROR 3000 Vaio\Usuario PDC deactivation not performed. Activation failed or activator was not initialized. PDC handle: 0000000000000000File onecoreuap\shell\roaming\c
,ERROR 3000 Vaio\Usuario onecoreuap\shell\roaming\cloudcommon\liveapi\livestorage.cpp(3713)\OneDriveSettingSyncProvider.dll!00007FF8C2742E89: (caller: 00007FF8C273A0E5)
,ERROR 3000 Vaio\Usuario onecoreuap\shell\roaming\cloudcommon\liveapi\livestorage.cpp(3538)\OneDriveSettingSyncProvider.dll!00007FF8C27426AC: (caller: 00007FF8C2742E53)
,ERROR 1008 Vaio\Usuario MSA ticket request failed for current user. (Result: 0x80040410)
,ERROR 3000 Vaio\Usuario onecoreuap\shell\roaming\cloudcommon\liveapi\msatoken.cpp(114)\OneDriveSettingSyncProvider.dll!00007FF8C275284B: (caller: 00007FF8C274260B) Ret
,ERROR 3000 Vaio\Usuario onecoreuap\shell\roaming\cloudcommon\liveapi\msatoken.cpp(239)\OneDriveSettingSyncProvider.dll!00007FF8C27530A0: (caller: 00007FF8C275286A) Ret
,ERROR 3000 Vaio\Usuario onecoreuap\shell\roaming\cloudcommon\liveapi\msatoken.cpp(385)\OneDriveSettingSyncProvider.dll!00007FF8C2753DA6: (caller: 00007FF8C275307F) Ret
,ERROR 3000 Vaio\Usuario PDC deactivation not performed. Activation failed or activator was not initialized. PDC handle: 0000000000000000File onecoreuap\shell\roaming\c
,ERROR 6113 NT AUTHORITY\SYSTEM La llamada RPC a la funciÃ³n WLIDAcquireTokensWithNGC devolviÃ³ el siguiente cÃ³digo de error: 0x8004882E.
,AUDIT_SUCCESS 5379 Las credenciales del Administrador de credenciales se leyeron.\0x0D\0x0A\0x0D\0x0AAsunto:\0x0D\0x0A\0x09Id. de seguridad:\0x09\0x09S-1-5-21-27026750
,INFO 3020 Vaio\Usuario Storage request: GET to https://go.microsoft.com/fwlink/?LinkID=279774 completed with status code 401.
,INFO 3020 Vaio\Usuario Storage request: GET to https://go.microsoft.com/fwlink/?LinkID=279774 completed with status code 302.
,INFO 8001 NT AUTHORITY\SYSTEM Skipping license manager: PFN Microsoft.Windows.Photos_2020.20070.10002.0_x64__8wekyb3d8bbwe\0x0D\0x0AFunction: InvokeLicenseManagerRequi
,INFO 1025 NT AUTHORITY\SYSTEM Se activÃ³ un evento de inicio/apagado: MonitorSettingChange [PowerEventType] false [Enabled].
,INFO 1025 Vaio\Usuario Se activÃ³ un evento de inicio/apagado: MonitorSettingChange [PowerEventType] false [Enabled].
,INFO 8001 NT AUTHORITY\SYSTEM Skipping license manager: PFN Microsoft.Windows.Photos_2020.20070.10002.0_x64__8wekyb3d8bbwe\0x0D\0x0AFunction: InvokeLicenseManagerRequi
,DEBUG 6067 Vaio\Usuario ComTaskPool created for SyncAtLogon context=-2147483624File onecoreuap\shell\roaming\settingsynchost\lib\settingsynctask.cpp line 59
,DEBUG 6067 Vaio\Usuario *** CSettingSyncTask startup ***File onecoreuap\shell\roaming\settingsynchost\lib\settingsynctask.cpp line 55
,INFO 1117 NT AUTHORITY\SYSTEM Se desconectaron los Servicios de notificaciones de inserciÃ³n de Windows debido al error: 0x880403EB y ahora se entrarÃ¡ en el modo de r
```

Figura 9. Información exportada por Syslog.

La información fue extraída en un intervalo de veinte minutos, generándose 618 eventos. Mediante el análisis y estudio de los principales eventos críticos para un sistema se crea reglas de correlación que permiten extraer la información importante, de acuerdo al estudio se determinó

que los eventos a filtrar serán de ERROR y WARNING. Las reglas de correlación permiten la extracción de hora, fecha, id de evento, dirección ip y descripción de evento.

Figura 10. Información extraída y filtrada.

Con el filtrado de información, se obtienen resultados del análisis, 73 líneas coincidentes con ERROR, 57 líneas de coincidencia WARNING y 488 descartadas, dan el total de 618.

Estas líneas de información extraída se descomponen en distintos arrays que se enviarán a la base de datos levantada en SQL que se encuentra en estricta relación de dependencia con la herramienta.

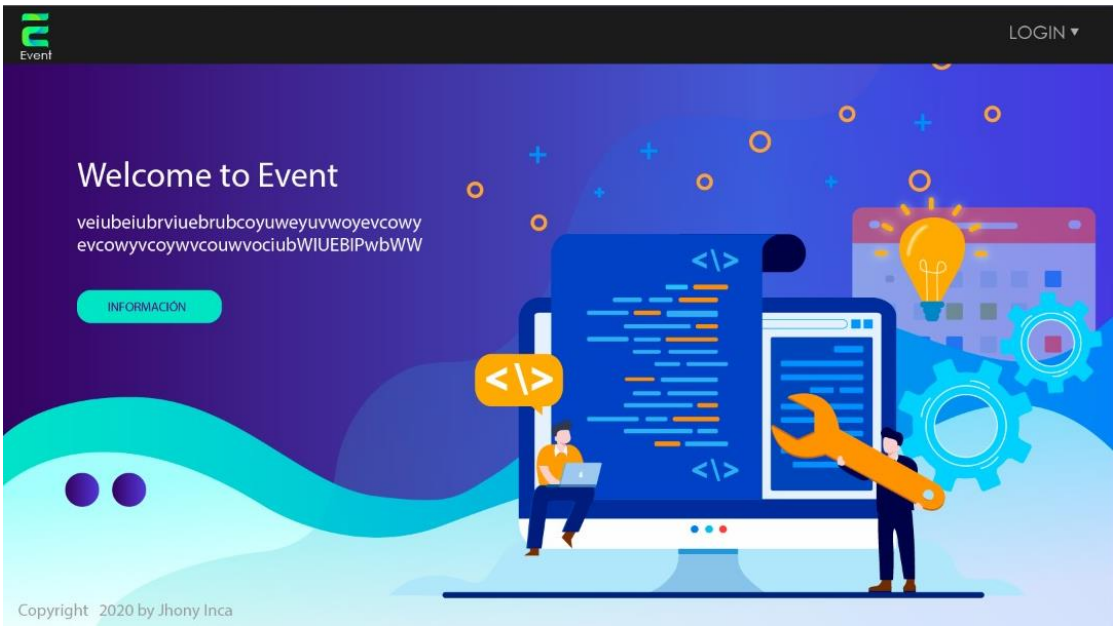

Figura 11. Interfaz inicio herramienta Event.

La herramienta brinda un mejor manejo y visualización de la información que se generan por los archivos de logs, permitiendo el almacenamiento en categorías, es muy importante señalar

destacar el entendimiento de la información y uso de la herramienta dependerá de la capacidad del usuario. Event provee varias f0hhunciones de trabajo y manejo como se detallan es las figuras:

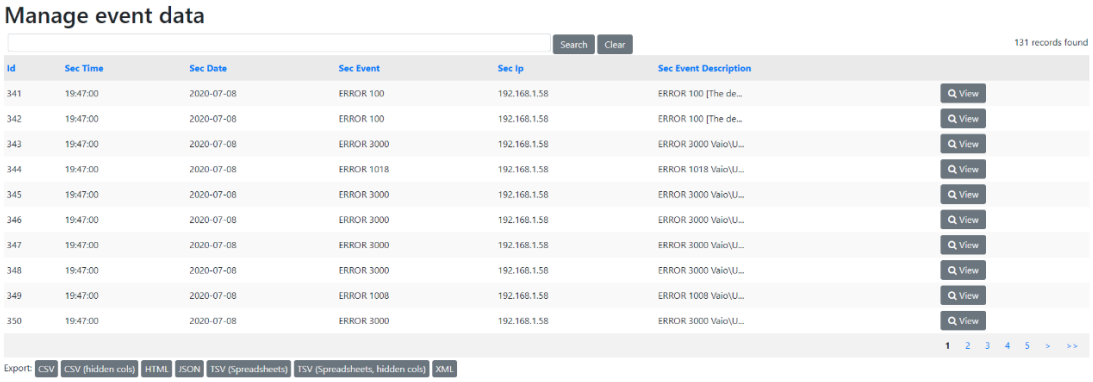

Figura 12. Información general de eventos

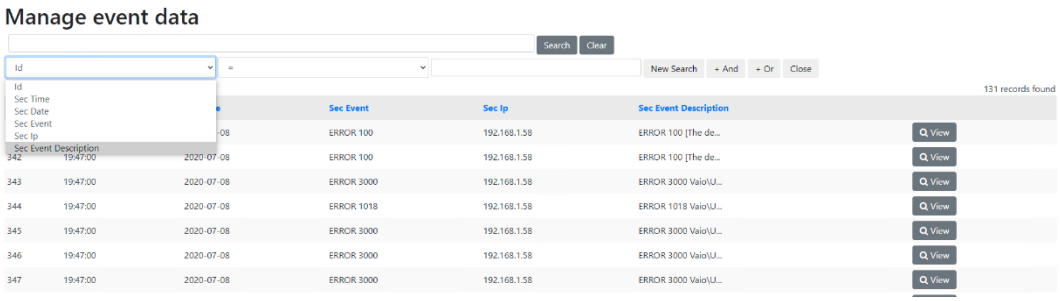

Figura 13. Función filtrado de eventos

Figura 14. Información de evento seleccionado.

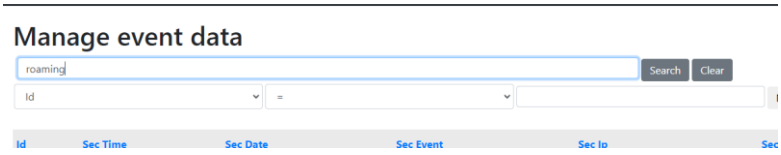

Figura 15. Función buscadora de eventos.

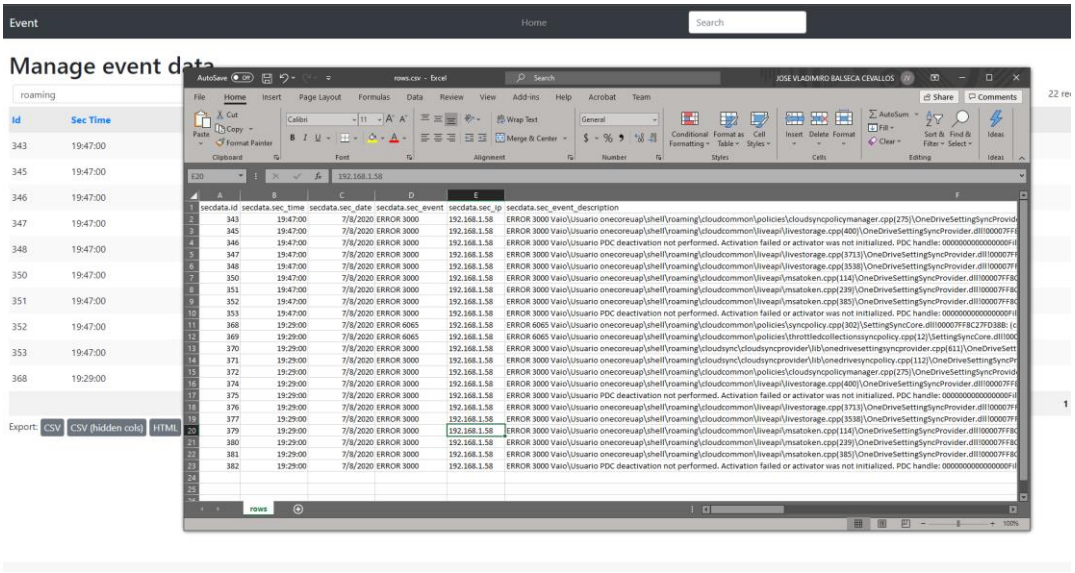

Figura 16. Función exportadora de eventos a formato CSV.

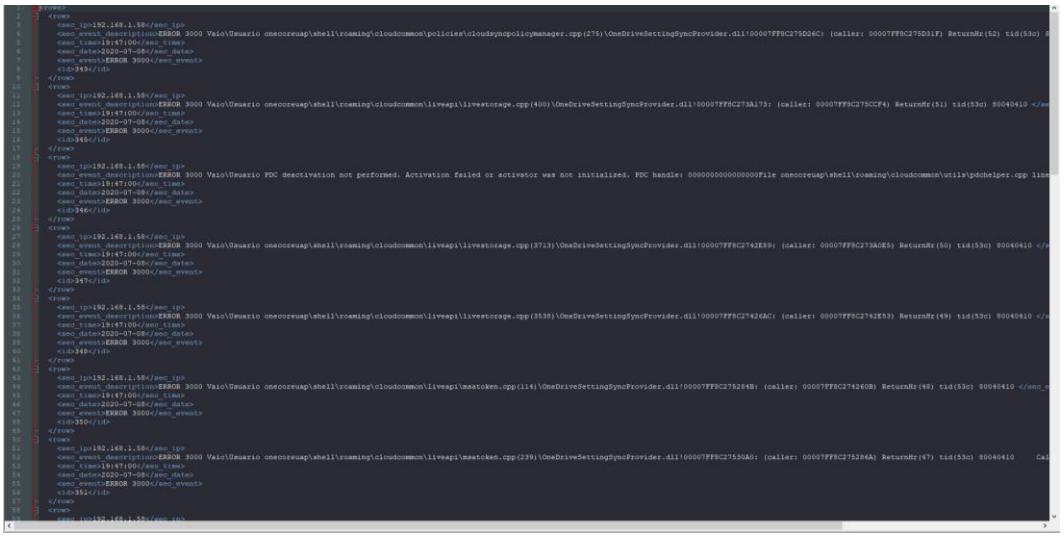

Figura 17. Función exportadora de eventos a formato XML.

También posee la función exportar en formato JSON, como también es adaptable al uso en teléfonos móviles o tabletas permitiendo movilidad y facilidad de acceso.

4 Conclusiones y futura línea.

Conclusiones —

- Existe una estricta dependencia hombre-sistema, esta herramienta es una muestra de ello, debido a la relación de dependencia entre ambos, por más avanzado sea el software sin la existencia de personas capaces de entenderla no podrá funcionar de manera correcta.
- Esta herramienta y estudio promueve el uso, desarrollo y mantenimiento de software libre que no necesite de hardware adicional o recursos dedicados.
- Se demostró el correcto uso de Simple Event Correlator dentro del sistema operativo Windows, pero es necesario buscar y continuar mejorar las prácticas de correlación de eventos y llevarlo a un nivel superior.
- La correlación de eventos representa una solución sólida y confiable en cuanto a detección de incidentes sin importar la clase, seguridad, sistema o alertas críticas.
- El uso de un enfoque híbrido de correlación de eventos representa una solución sólida y confiable para detectar varios tipos de incidentes, ya sean relacionados con la seguridad o alertas críticas ya que generalmente los usuarios no revisan con frecuencia los registros de los equipos y en su mayoría no poseen las habilidades para extraer información crítica. Por lo tanto, la correlación de eventos proactiva puede considerarse tan crítica como las soluciones antimalware.
- Debido la situación actual del planeta, ha promovido el aumento de teletrabajo y es necesario difundir el conocimiento de las amenazas indetectables como malware, destacando el uso de correlación de eventos proactiva para mejorar la seguridad en operaciones de TI. Este trabajo promueve el uso de correlación de eventos y el reconocimiento de patrones en la plataforma Microsoft Windows.

Futura línea —

- El desarrollo de la presente propuesta genera la idea de una arquitectura única de correlación de eventos a la que cualquier sistema operativo sea capaz de acceder promoviendo así entre ellos la interoperabilidad de módulos como también procesos.
- Una línea futura a considerar es la escalabilidad de la herramienta, así como la integración de herramientas inteligentes generadoras de archivos de logs, pero con la enorme responsabilidad de trabajar con el procesamiento de una enorme cantidad de datos lo cual podría ralentizar el proceso de filtrado y selección de información.

- Integración de esta herramienta a otros Sistemas Operativos.

- Integración de este trabajo de investigación a softwares de gestión de información en tiempo real.

5 Dedicatoria y agradecimientos.

Agradezco a Dios por siempre bendecirme y darme la fuerza de voluntad que necesitaba a lo largo de este año lejos de mi hogar y mi familia. Agradezco infinitamente a mis padres Carmita López y Bolívar Inca que al transcurrir de cada día me siguen enseñando que si deseas algo debes ir tras ello, trabajar y esforzarte por conseguirlo. Mi hermano Kevin que a pesar de ser menor me ha enseñado mucho y espero ser un ejemplo de superación para él. Mi prometida Daniela, su enorme paciencia, madurez y amor me brindó valor de lucha para levantarme con fuerzas todos los días. Mi querida familia, que supo recibirme con los brazos abiertos, Tíos Laura, Rodrigo gracias por cuidarme como un hijo más, mis primos Sara, Adrián, Josué y Bryan con todo el cariño de mi corazón Dios les pague a todos ustedes han hecho que los días no pasen tan lentos y me sienta como en mi casa. Mi familia y amigos a pesar de la distancia han estado pendientes a lo largo de este año.

Agradezco a mis amigos y colegas Mayrita y José, por compartir sus conocimientos y consejos.

Dedico este trabajo con mucho amor a mis 4 abuelitos, gracias a Dios aún los tengo conmigo, a pesar de estar lejos y en medio de esta pandemia los ha cuidado, quiero que sepan que nunca me he sentido tan orgulloso con este momento de llevar su sangre y tener esas raíces de campo las cuales me han mostrado que la vida es dura, pero con trabajo y sacrificio se pueden conseguir muchas cosas, tengan la seguridad que su futura generación tendrá los valores que me han inculcado. Dedico este trabajo a mi familia, mi pilar fundamental.

Mis más sincero agradecimiento y admiración al Dr. Manuel Esteve Domingo por crear en mí el gusto y orientación hacia la ciberseguridad y haberme aceptado como su dirigido para la realización de este trabajo.

BIBLIOGRAFÍA.

[1] J. Shenk, "Ninth Log Management Survey Report," SANS survey : InfoSec Reading Room, October 2014.

[2] R. Vaarandi, "SEC – a Lightweight Event Correlation Tool," in IEEE/IFIP Network Operations and Management Symposium, pp. 907-910, 2002.

[3] The Perl Programming Language, "Download Perl Distribution," Perl.org, [Online]. Available: https://www.perl.org/get.html#win32. [Accessed 2016].

[4] T. Beverly, "Windows version of SEC," SEC mailing list, April 2008. [Online]. Available: https://sourceforge.net/p/simple-evcorr/mailman/message/19156366/. [Accessed 2015].

[5] Microsoft, "How to use the event log management script tool," 2015. [Online]. Available: https://support.microsoft.com/en-us/kb/318763. [Accessed 2016].

[6] TechNet, "Event Log," Microsoft, October 2008. [Online]. Available: https://technet.microsoft.com/en-us/library/cc722385%28v=ws.10%29.aspx. [Accessed 2016].

[7] A. Sapegin, D. Jaeger, A. Azodi, M. Gawron, F. Cheng and C. Meinel, "Hierarchical object log format for normalisation of security events," in 9th International Conference on Information Assurance and Security (IAS), 2013.

[8] P. Sharma, S. Yadav and B. Brahmdutt, "A Review Study of Server Log Formats for Efficient Web Mining," in International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.

[9] J. Ya, T. Liu, H. Zhang, J. Shi and L. Guo, "An automatic approach to extract the formats of network and security log messages," in Military Communications Conference, 2015.

[10] J. H. a. M. Kamber, in Data mining concept and technology, 2007, p. 3.

[11] J. Lv, "Research on the application of web log mining," Journal of Chonqqing Normal University, vol. 12, no. 23, pp. 39-44, 2006.

[12] J. Kezhong and W. Chengwen, "An improved algorithm with key attributes constraints for mining interesting association rules in network log," in Business Management and Electronic Information (BMEI), 2011.

[13] M. P. Yadav, P. K. Keserwani and S. G. Samaddar, "An efficient web mining algorithm for Web Log analysis: E-Web Miner," in Recent Advances in Information Technology (RAIT), 2012.

[14] "GELF - Graylog 2.0.0 documentation," Graylog, [Online]. Available: http://docs.graylog.org/en/latest/pages/gelf.html. [Accessed 2016].

[15] A. Sapegin, D. Jaeger, A. Azodi, M. Gawron, F. Cheng and C. Meinel, "Hierarchical object log format for normalisation of security events," in 9th International Conference on Information Assurance and Security (lAS), 2013.

[16] F. Cheng, A. Azodi, D. Jaeger and C. Meinel, "Pushing the Limits in Event Normalisation to," in International Conference on Advanced Cloud and Big Data, 2013.

[17] R. Gerhards, "RFC5424 - The Syslog protocol," March 2009. [Online]. Available: https://tools.ietf.org/html/rfc5424. [Accessed 2016].

[18] MSDN: Developer technologies, "Event Log Format (Windows)," [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/bb309026(v=vs.85).aspx. [Accessed 2016].

[19] "ElasticSearch | Elastic," Elastic corp., [Online]. Available: https://www.elastic.co/products/elasticsearch. [Accessed 2016].

[20] NXLog.co, "NXLog community edition," [Online]. Available: http://nxlog.org/products/nxlog-community-edition. [Accessed 2016].

[21] Elastic, "beats | Elastic," [Online]. Available: https://www.elastic.co/products/beats. [Accessed 2016].

[22] Elastic, "Logstash | Elastic," [Online]. Available: https://www.elastic.co/products/logstash. [Accessed 2016].

[23] intersectalliance, "Snare agent for Windows," [Online]. Available: https://www.intersectalliance.com/our-product/snare-agent/operating-system-agents/snare-agent-for-windows/. [Accessed 2016].

[24] Microsoft MSDN, "Configure computers to forward and collect events," February 2015. [Online]. Available: https://msdn.microsoft.com/en-us/library/cc748890.aspx. [Accessed 2016].

[25] A. Sah, "A New Architecture for Managing Enterprise Log Data," in LISA, 2002.

[26] G. Jakobson and M. Weissman, "Real-time telecommunication network management: Extending event correlation with temporal constraints," in International Symposium on Integrated Network Management, pp. 290, 1995.

[27] B. Gruschke, "Integrated Event Management: Event Correlation using Dependency Graphs," in 9th IFIP/IEEEInternational Workshop on Distributed Systems: Operations and Management (DSOM), 1998.

[28] S. A. Yemin, S. Kliger, E. Mozes, Y. Yemini and D. Ohsie, "High speed and robust event correlation," IEEE Communications Magazine 34(5), pp. 82-90, May 1996.

[29] M. Steinder and A. S. Sethi, "End-to-end Service Failure Diagnosis Using Belief Networks," in IEEE/IFIP Network Operations and Management Symposium, 2002.

[30] H. Wietgrefe, K.-D. Tuchs, K. Jobmann, G. Carls, P. Froehlich, W. Nejdl and S. Steinfeld, "Using Neural Networks for Alarm Correlation in Cellular Phone Networks," in International Workshop on Applications of Neural Networks in Telecommunications, 1997.

[31] R. N. Cronk, P. H. Callahan and L. Bernstein, Rule-based expert systems for network management and operations: an introduction, IEEE, 1988.

[32] R. Davis, H. Shrobe, W. Hamscher, K. Wieckert, M. Shirley and S. Polit, "Diagnosis based on description of structure and function," in American Association for Artificial Intelligence, 1982.

[33] J. Myers, G. R. Michael and R. F. Mills, "Log-Based Distributed Security Event Detection Using Simple Event Correlator," in 44th Hawaii International Conference on System Sciences, 2010.

[34] M. Kont, "Comparative analysis of open-source log collection and correlation tools," in Event Management and active defense framework for small companies, MSc Thesis, Tallinn University of Technology, 2014, pp. 24 - 44.

[35] ZURIEL Kft., "LOGalyze - Open Source Log Management Tool, SIEM, Log Analyzer," ZURIEL Kft., [Online]. Available: http://www.logalyze.com/. [Accessed 2016].

[36] EsperTech, "EsperTech - Esper," EsperTech, 2006. [Online]. Available: http://www.espertech.com/esper/. [Accessed 2016].

[37] Roth Consulting, "Official Win32::Daemon home page," 12 2001. [Online]. Available: http://www.roth.net/perl/Daemon/. [Accessed 2016].

[38] A. Perl, "Active Perl," ActiveState, 2015. [Online]. Available: http://www.activestate.com/activeperl. [Accessed 2016].

[39] StrawberryPerl, "The Perl for MS Windows, free of charge!," StrawberryPerl.com, 2015. [Online]. Available: http://strawberryperl.com/. [Accessed 2016].

[40] "Cygwin," [Online]. Available: https://www.cygwin.com/. [Accessed 2015].