BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN

Ingeniería en ciencias de la computación

IMPLEMENTACIÓN MODULAR DE UN SISTEMA DE CENTRALIZACIÓN Y CORRELACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN (SIEM)

Tesis presentada para obtener el título de:

LICENCIATURA EN INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

PRESENTA:

DÍAZ LIMA FRANCISCO DE JESÚS
201016544

ASESORES DE TESIS:

M.C. YALÚ GALICIA HERNÁNDEZ

M. C. CARLOS DOCE REYES

Puebla, Pue., México Agosto 2018

Página dejada en blanco intencionalmente

TABLA DE CONTENIDO

LISTA DE FIGURAS

AGRADECIMIENTOS

El autor desea expresar sus más sinceros agradecimientos a las personas que han contribuido a la realización de este proyecto:

Al M.C. Carlos Doce Reyes y a la empresa MCSec S. C. por las facilidades prestadas durante la realización del presente proyecto.

A mi madre y mi tía Ana por su ardua labor durante mi formación personal y profesional.

A mi familia por su inmensurable amor y respaldo en todos los aspectos de mi vida.

A mis amigos, que, si bien yo los incluyo en el grupo anterior, merecen una mención explícita debido a su incondicional lealtad, paciencia y apoyo.

“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.”

– Kevin Mitnick

Página dejada en blanco intencionalmente

RESUMEN

Implementación modular de un sistema de centralización y correlación de eventos de seguridad (SIEM)

Como una capa extra de seguridad de la información se han desarrollado sistemas de análisis y correlación de eventos cuya funcionalidad está basada en el análisis de los registros generados por los dispositivos de una red. Estos sistemas ayudan a dar respuesta a los incidentes de seguridad cuando ocurran.

En las organizaciones, es común que no exista un sistema de análisis o manejo de registros, y en las organizaciones dónde se implementan sistemas SEM, SIM, o SIEM el principal motivante a implementarlos son los requisitos de cumplimiento especificados en normativas a la que están sometidas, certificaciones, o requerimientos gubernamentales. El despliegue de aplicaciones manejadoras de eventos y registros basados en cumplimientos de normativas, comúnmente es realizado sin una planeación apropiada, por lo cual es común encontrar errores durante el despliegue de estos sistemas, estos errores principalmente son debidos a una mala planeación y o unas ideas equivocadas sobre las bondades que ofrecen las diversas tecnologías disponibles en el mercado.

Además, existen complicaciones intrínsecas de este tipo de herramientas, como son la complejidad técnica, el tamaño del despliegue, el tiempo que toma el despliegue, los costos de instalación y operación, la poca integración con tecnologías de terceros, o el ruido de las alertas generadas. Todo esto resulta en más carga para los responsables de la seguridad, en vez de aliviar su trabajo.

Como consecuencia, se dan casos donde la solución SIEM es despreciada o considerada inútil, puesto que no está diseñada para cumplir las funcionalidades necesarias, o bien la implementación no está adecuada a cumplir los propósitos para los que fue instalada.

Para ayudar a solucionar esta problemática se inspeccionan las mejores prácticas recomendadas durante el despliegue del SIEM, buscando reducir las complicaciones comunes que se encuentran durante la implementación de las soluciones de análisis de eventos. Aunado a lo anterior, también se analizan las principales herramientas que permiten el análisis y la correlación de los eventos de la seguridad, identificando las piezas claves que permiten administrar, controlar y dar seguimiento a los incidentes de seguridad, además de explorar las capacidades de éstos sistemas y la integración de agentes externos que ayudan a la recolección y correlación de la información obtenida.

En función de los datos recolectados y las correlaciones generadas por el SIEM, se busca resguardar la información clasificada o de importancia para la organización, priorizando la funcionalidad y efectividad de los sistemas a desplegar.

Durante la realización de este proyecto, se instaló un laboratorio de pruebas en donde se probaron 3 soluciones comerciales y de código abierto, en sus diferentes versiones considerando el tamaño del despliegue, las cuales son: AlienVault, ArcSight, y Splunk que se considera, están diseñados para apegarse a los estándares y regulaciones más importantes en el cumplimiento de normativas. Estas soluciones ayudan a los profesionales de la seguridad a detectar, investigar y solucionar los eventos pertinentes para asegurar la protección del entorno informático de su organización, al igual que se indagan las prácticas recomendadas para consolidar una respuesta efectiva ante los incidentes identificados a través de las herramientas expuestas.

Con base en los resultados obtenidos en el laboratorio, se han logrado identificar una relación entre las herramientas y algunos sectores para las cuales se cubren las necesidades más comunes que pueden requerir durante el despliegue de un SIEM, de esta forma, se pueden recalcar los siguientes puntos sobre las herramientas seleccionadas:

La solución AlienVault, puede ser recomendada para casi cualquier empresa, en especial pequeñas y medianas empresas donde puede encajar fácilmente en el plan de ciberseguridad debido a los costos de licenciamiento asequibles o de código abierto, además de una relativa simplicidad operativa. Dependiendo de los requerimientos especificados en las normativas a las que están suscritos, como por ejemplo el almacenamiento gestionado de los registros, podrán decantarse por la versión de código abierto OSSIM (Open Source Security Information Management), o la versión con soporte del fabricante, licenciada con base en el número de activos a monitorear, denominada USM (Unified Security Management).

ArcSight está enfocada al mercado de empresas con grandes volúmenes de datos que desean realizar una sustanciosa inversión en ciberseguridad, o que no están dispuestas a usar soluciones de código abierto, en especial aquellas que requieran gran soporte por parte del fabricante. Aquellas organizaciones pueden optar por implementar soluciones maduras de amplio soporte comercial como es el caso de la solución estudiada en el presente proyecto: ArcSight de HP, la cual presenta 2 versiones de licenciamiento: ArcSight Express y ArcSight ESM, siendo la principal diferencia entre ellas el tamaño del despliegue para el cual están enfocados, ambas basándose en el tráfico de red medido en cantidad de Gb por día registrado.

Organizaciones que requieren análisis de información basada en patrones o minería de datos, que basan sus operaciones en el análisis masivo de múltiples fuentes de

información y con grandes necesidades de investigación y gestión de datos, pueden considerar Splunk como una de las herramientas que pueden aportar la solución de SIEM que necesitan.

No obstante, existen muchas otras soluciones que deben ser consideradas como IBM QRadar o LogRhythm, que presentan grandes funcionalidades con valor agregado y deben ser tomados en cuenta al decantarse por un SIEM.

CAPÍTULO 1 - INTRODUCCIÓN

En el marco de la seguridad informática, cada día surgen nuevas amenazas cada vez más complejas y con mejores mecanismos de evasión que resultan en graves riesgos para las redes de comunicaciones y los servicios de tecnologías de la información como los conocemos hoy en día. Es por esto que, de igual manera, se crean nuevas tecnologías de defensa y protección que buscan salvaguardar el buen funcionamiento de los sistemas. Pero como ha sido demostrado a través de la historia moderna, ningún sistema es inmune a fallos, y siempre es necesario tener un plan de respaldo, motivo por el cual, dentro de una arquitectura de red de alta seguridad el área de detección de intrusiones representa un aspecto vital de defensa ante posibles brechas de seguridad, siendo uno de los principales actores, los mecanismos de recolección y manejo de eventos de seguridad, mejor conocidos como SIEM.

1.1.1 PLANTEAMIENTO DEL PROBLEMA

“Un SIEM es costoso en términos de tiempo, dinero y esfuerzo, también, muchas veces no ofrece la solución que se estaba buscando”

Actualmente los entornos y las infraestructuras de las tecnologías de la información crecen a pasos agigantados, convirtiendo el rol de la implementación de seguridad un factor cada vez más crucial en los entornos de las organizaciones que utilizan recursos informáticos para desempeñar sus labores del día a día. Este crecimiento en la infraestructura ocasiona que el volumen de datos que se debe analizar aumente en la misma proporción que los recursos que se intenta proteger, limitando la capacidad de respuesta por parte de los responsables de resguardar la seguridad de la información. Aunado a esto, los profesionales de la seguridad deben de dar

respuesta a los incidentes registrados, al mismo tiempo que buscan satisfacer el cumplimiento de las normativas especificadas en su organización.

Consolidar un plan de seguridad que se adecue a las necesidades de una organización no es una tarea sencilla, y esta puede complicarse en medida del tamaño de la infraestructura de la organización para la cual se esté desarrollando la planeación. Esta labor es especialmente ardua en organizaciones donde no poseen un centro de operaciones de la seguridad (*Security operations center* SOC) o personal especializado que cumpla las funciones de un SOC. La tarea se obstaculiza aún más cuando no existe documentación sobre la implementación de las prácticas internas de seguridad.

Un análisis efectivo de las bitácoras de información no es fácil, requiere bastante trabajo, y una amplia comprensión del entorno que se planea analizar, en específico, es necesario conocer qué es bueno y qué es malo en la actividad de la red.

Una organización puede albergar en su red interna una enorme diversidad de dispositivos de muchas marcas diferentes, y cada fabricante crea sus propios formatos de bitácoras (logs), por consecuente, los mensajes se generan en una vasta cantidad de formas y tamaños, ocasionando que la tarea del análisis se vuelva intensamente complicada; resulta evidente que garantizar la seguridad de la organización no va a ser una tarea trivial. Hay que añadir que puede resultar difícil extraer información de los logs, ya que algunos registros pueden ser especialmente malos, debido a que en muchos casos los datos que se presentan no son tan descriptivos como se desea.

Existen complicaciones que deben ser atendidas específicamente por personal que conozca la organización, especialmente cuando es necesario comprender el contexto

en el que se generan las bitácoras; esto es debido a que existen eventos que en algún entorno pueden considerados como tráfico normal mientras que en otros sería una señal de alarma para la seguridad de la información, por ejemplo, en una unidad académica detectar a un usuario comunicándose usando el protocolo IRC (*Internet Relay Chat*) o usando un cliente BitTorrent para compartir archivos puede ser catalogado como tráfico normal, mientras que en un entorno bancario cualquiera de los dos escenarios puede ejercer como un indicador de compromiso o representar una amenaza para la integridad de los datos de la organización.

Para ayudar al equipo de seguridad a manejar los eventos de seguridad registrados, se implementan soluciones de manejo y correlación de eventos, mejor conocidas como SIEM; que basan sus operaciones en el análisis de los registros generados por los dispositivos de una red. Estas soluciones proveen de herramientas de análisis y retención de eventos que alivian la carga que enfrentan los empleados en su tarea de descubrir amenazas y dar tratamiento a los incidentes cuando surjan.

Existe una gran cantidad de herramientas de análisis de eventos al alcance de los profesionales de la seguridad. La elección de un sistema que cumpla con las funcionalidades que la organización requiere, debe ser examinada minuciosamente puesto que existen una enorme cantidad de herramientas y fabricantes de dispositivos y aplicaciones de seguridad, y no es sencillo encontrar una solución especifica que cubra todas las necesidades existentes, especialmente a un precio que la organización pueda invertir.

Adicionalmente, una instalación de SIEM tradicional presenta ciertas características puntuales que entorpecen el despliegue correcto de la solución. Éstas características pueden ser meras trivialidades o complejas limitaciones difíciles de escalar o mitigar

según sea necesario (Barraco, 2014). A continuación, se exploran las principales adversidades que se enfrentan al desplegar una instalación funcional de SIEM

- **Un SIEM es demasiado complejo**. Recolectar datos, agregarlos, normalizarlos, y generar correlaciones no es una tarea simple. Alimentar un SIEM con datos de registros es una tarea ardua que requiere de varias horas de trabajo entre el personal de administración de sistemas y el personal responsable de la seguridad. Dependiendo de la extensión de la organización para la cual se implemente el SIEM, enrutar todo el tráfico de los registros a la consola central puede tomar una cantidad de tiempo considerable. Algunas veces, existen dispositivos cuyos formatos de registros no son soportados por el SIEM en el proceso de normalización, de hecho, en algunos casos el fabricante espera que el cliente o el proveedor de servicios sean quienes tomen la peor parte del desafío que implica integrar estos componentes faltantes en la solución. Técnicamente, el proceso de integración no presenta un reto monumental, sin embargo, escalando el problema a organizaciones con cientos o miles de dispositivos de diversos fabricantes, la tarea de integración y despliegue puede demorar incluso meses en completarse.

- **El despliegue de un SIEM toma cierto tiempo para completarse**. Usualmente, cuando una organización decide invertir en una solución SIEM, es porque necesita respuestas rápidas o urgentes sobre los eventos de seguridad que se registran en la red, sin embargo, las reglas de correlación de eventos que proveerán la “inteligencia de la seguridad” que ofreció el fabricante, no serán de mucha utilidad hasta que las fuentes de datos sean finamente ajustadas.

- **Un SIEM puede llegar a ser demasiado caro**. Un SIEM no funciona de forma adecuada con solo colocar el equipo en línea. Lo más probable es que para

obtener una funcionalidad óptima en un SIEM, las organizaciones necesiten contratar consultores y arquitectos para que diseñen e implementen la integración de los componentes, afinen y ajusten las fuentes de datos, y programen la importación de datos externos a través de todas las diversas fuentes disponibles. Además de costo de licenciamiento de la aplicación, a menudo elevado, el hecho de requerir personal especializado o proveedores que se encargarán de realizar los ajustes correspondientes en el sistema, representa una inversión extra que debe ser considerada al desplegar este tipo de tecnologías.

- **Poca integración**. Existen soluciones que además de ser complejas, no tienen una amplia variedad de dispositivos soportados, lo que obliga al personal de seguridad a escribir el código para recuperar la información que se quiere. En redes amplias, esto puede convertirse en una tarea monumental.

- **Ruido**. Más importante aún, una vez que todos los componentes han sido desplegados y sus activos importados, un SIEM sin ajustes ni refinamiento en sus reglas, puede llegar a ser demasiado “ruidoso” en términos de alertas y alarmas. Es normal que un SIEM sin afinar genere una multitud de alertas, alarmas, o falsos positivos en su primer acercamiento al tráfico de la organización. En gran parte, la multitud de eventos que genera un SIEM sin afinar son provocados por las reglas predefinidas por el fabricante, y requieren intervención de personal especializado para ajustarlas a informar sobre lo que de verdad es de particular interés de la organización. Muy a menudo las alarmas predefinidas carecen de inteligencia procesable, y no sirve de nada saber que se ha producido un evento en particular, si no se sabe qué hacer al respecto. Los analistas de seguridad necesitan más información que se genera a partir de las reglas de correlación con el fin de responder e investigar ante los incidentes detectados.

Estructura del Documento

En este primer capítulo se presenta una introducción a la terminología de SIEM y se plantean las bases de la investigación realizada, describiendo los antecedentes en el campo de la seguridad informática y las defensas que se plantearon para asegurar la integridad de la información, se explora el estado del arte de las soluciones SIEM, así como la problemática actual y los objetivos que plantea cubrir el presente proyecto buscando resolver algunos de los problemas que se han identificado.

En el capítulo 2 se describen las bases teóricas necesarias para la implementación de un SIEM, y se estudian casos puntuales de herramientas que ayudan a un SIEM a recolectar registros e indexarlos en su base de datos. Con base en las principales funcionalidades que se identificaron deben poseer estas herramientas, se seleccionan los casos de estudio que se investigan en este proyecto.

Durante el capítulo 3 se describen las herramientas que integran los SIEM seleccionados y como fueron usadas al montar el laboratorio de pruebas para cotejar 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 se identifican sus fortalezas y precauciones a considerar a la hora de implementarlas.

En el capítulo 5 se presentan las conclusiones y el trabajo futuro a desarrollar.

1.1.2 ANTECEDENTES

Desde sus orígenes, la seguridad de la información se ha visto amenazada por diversos tipos de ataques que buscan corromper su integridad; estos ataques tienen una cantidad monumental de variantes que van desde adolescentes con mucho tiempo libre realizando denegaciones de servicio, hasta organizaciones criminales con gran poder, dedicadas a realizar todo tipo de actos deplorables en la Internet.

Los primeros ataques a la seguridad de la información se remontan a la segunda guerra mundial, en diciembre de 1932 cuando Marian Rejewski, matemático y criptoanalista polaco, por primera vez rompió el código de un mensaje militar alemán que fue encriptado con una máquina enigma (Wilcox, 2001). A partir de este descubrimiento creó una máquina llamada “bomba”, cuya función consistía en desencriptar los mensajes alemanes cifrados con máquinas enigma. Más tarde, en 1939, esta implementación sería mejorada por el mismo Alan Turing para crear una nueva máquina llamada “bombe”. Se presume que estos dispositivos fueron decisivos en la victoria de los aliados (Winterbotham, 1974).

En 1940, René Carmille, sabotea el censo Nazi en Francia para localizar judíos que serían enviados a campos de concentración modificando las tarjetas perforadas usadas por los alemanes, también modifica las máquinas perforadoras de tarjetas para que no marquen el identificador de religión, salvando una cantidad incalculable de vidas que de otra manera hubieran sido enviadas a los campos de concentración (Davis, 2015).

A finales de la década de los 50 y durante los años 60 la principal amenaza a la seguridad de la información radica en un concepto nombrado *‘phreaking’*, que consiste en el hacking de los sistemas de telecomunicaciones, en particular las líneas

telefónicas, con el objetivo específico de usar la línea de comunicación sin costo. El phreaking se convierte en una práctica extendida gracias a las cajas de phreaking que automáticamente producen tonos que son interpretados por el switch de comunicaciones y tendrían diversas funciones como: hacer llamadas gratis, desviar llamadas, interrumpir el funcionamiento normal de la línea, entre otras. A comienzos de la década de los años 70 el phreaking ya es un problema para compañías como AT&T quienes comienzan a monitorear las llamadas para atrapar a estos hackers denominados “phreakers”, con esto logran más de 200 arrestos, entre ellos John Draper, mejor conocido como “Captain Crunch”. (Price, 2008)

En 1971 Bob Thomas crea un programa llamado *Creeper*, diseñado para copiarse entre computadoras. Debido a que hasta este entonces no se habían creado programas informáticos de este tipo, no fue clasificado como tal, pero actualmente es aceptado años más tarde como el primer gusano de computadora. Su función no era activamente maliciosa pues no causaba daño alguno a los datos o sistemas, simplemente desplegaba un mensaje en pantalla que dice: *"I'm the creeper: catch me if you can".*

La década de los años 80 fue particularmente marcada por el auge de profesionales de tecnología, técnicamente expertos, con grandes habilidades en programación, quienes activamente prueban las defensas de sistemas de cómputo, buscando los límites y posibilidades de una máquina. Así es como el New York Times definió a los Hackers en 1981 (The New York Times, 1981). A pesar de su papel aparentemente peligroso, los Hackers, o piratas informáticos, son un activo reconocido en la industria informática, y a menudo muy apreciado. Aquí nacen dos grandes amenazas para la seguridad de la información, los virus, y los grupos de hackers maliciosos.

A principios de 1980 John Shock y Jon Hepps, investigadores en el centro de investigación de Xerox en Palo Alto, comienzan a experimentar con programas conocidos como gusanos. Los gusanos son programas diseñados para replicarse una vez que logran ejecutarse. Esta es la primera vez que se le atribuye el término *gusano (worm)* a un programa de computadora. Algunos de estos gusanos eran relativamente simples e inofensivos, estaban diseñados para ayudar a realizar tareas en la red, pero también existían algunos bastante complejos. Aunque intrínsecamente estos programas eran inofensivos, rápidamente se notó el potencial destructivo que tendrían si se usaban incorrectamente. Esto se descubrió cuando uno de estos programas tuvo un fallo durante la noche y cuando los empleados llegaron al día siguiente, diversos ordenadores habían fallado; cuando intentaban reiniciar el sistema, el gusano los hacia fallar nuevamente. Fue necesario programar una "vacuna" contra el gusano.

En 1988, Robert Tappan Morris, lanza uno de los primeros programas de gusano que se propaga a través de Internet, y uno de los primeros programas conocidos por explotar vulnerabilidades de *buffer overflow*. En concepto, el programa originalmente no estaba diseñado para causar daño, sino para medir el tamaño de Internet, sin embargo, un supuesto error de diseño permitía que el programa se propagara nuevamente a una víctima anterior, incluso si el equipo ya estaba infectado, causando que funcionara como una especie de "fork bomb" replicable. Este gusano se propaga a 6,000 computadoras pertenecientes a la red del gobierno de los Estados Unidos de América, ARPAnet, causando un daño estimado entre $10,000,0000 y $100,000,000 dólares americanos (Maynor, 2011).

El gusano de Morris orilla a DARPA a crear el CERT-CC (http://cert.org/about/, 2015) (Computer Emergency Response Team Coordination Center) para investigar posibles fallos en la seguridad los sistemas que puedan impactar en el software y la seguridad

de Internet. El CERT publica información sobre sus investigaciones y sus hallazgos, y trabaja en conjunto con empresas y gobierno para mejorar la seguridad del software e Internet (Jackson, 2005).

Con el tiempo, los gusanos evolucionan y son cada vez más complejos y más destructivos, por ejemplo, Christmas Tree, o WANK worm, entre otros. La única forma en que se pudo crear software malicioso tan complejo es con el nacimiento de los grupos de hackers y ciberorganizaciones criminales.

Desde inicios de 1980 los grupos delictivos crecieron en número y recursos, y para la década de 1990 la palabra hacking ya era sinónimo de delito, grupos como The 414, un grupo de seis adolecentes que se infiltró en decenas de computadoras de alto valor, orillaron a la cámara de representantes del gobierno de los Estados Unidos a realizar audiencias para discutir la creación de leyes respecto a la seguridad de la información.

En materia defensa perimetral, los firewalls fueron los primeros sistemas diseñados para proteger los sistemas de las amenazas externas. Los primeros firewalls controlaban el acceso a la red a través de un rudimentario filtrado de paquetes que consistía en un simple conjunto de reglas que filtraban atributos básicos del paquete, como el número de puerto y la dirección de destino.

La necesidad inherente de seguridad en las comunicaciones lleva a desarrollar nuevas herramientas para actuar contra las diversas amenazas, siendo la primera herramienta avanzada el Sistema de detección de intrusiones o IDS por sus siglas en inglés.

El primer acercamiento a la detección de intrusiones se le atribuye a James Anderson en sus publicaciones a inicios de 1980 donde señala la importancia de reconocer las amenazas que asechan en la red y la necesidad de implementar un plan de protección para la seguridad de la información (Anderson, 1980). En años anteriores y durante los primeros años de la década, la única forma que tenían los profesionales era esnifar las comunicaciones y manualmente revisar la información recibida, comúnmente, debido a los altos costos de los sistemas de almacenamiento, el análisis se hacía sobre inmensas pilas de papel que contenían los registros de eventos impresos (Kemmerer & Vigna, 2002). No fue hasta que entre 1984 y 1986 Dorothy Senning y Peter Neumann desarrollaron el primer prototipo de un IDS, sin embargo, este prototipo requeriría de algunos años para madurar sus herramientas y métodos de detección, hasta mediados de los años 1990, cuando las primeras soluciones comerciales de IDS estuvieron a disposición en el mercado. Algunos ejemplos de las primeras soluciones comerciales de IDS pueden ser Stalker, o NetRanger. Los primeros IDS implementaban nuevas reglas de detección en base a tráfico anómalo en la red, estas reglas no eran del todo certeras y podían llegar a presentar una gran cantidad de falsos positivos. La constante evolución de las redes durante los años 1990 y 2000 empeoró la detección de falsos positivos. Cuando esto sucedió muchos administradores de red llegaron a pensar que los IDS no eran confiables (Schwab, 2015).

El Laboratorio Nacional Lawrence Berkeley anunció “Bro” en 1998, un software que utilizaba su propio lenguaje de reglas para el análisis de paquetes de datos usando libpcap. “Network Flight Recorder” (NFR) en 1999 también utilizaba libpcap para efectuar su análisis de paquetes. Una evolución en esta rama del software se suscitó con APE que fue desarrollado como un analizador de paquetes. En noviembre de 1998 integra funcionalidades extra utilizando libpcap, y recibe el nombre de “Snort” un mes más tarde cuando fue liberado por Sourcefire como un proyecto de código

abierto. Snort llega a cambiar la escena de los sistemas de detección de intrusiones gracias a su versatilidad y efectividad en la aplicación de reglas para detectar tráfico malicioso o anómalo en la red. Rápidamente se extiende su uso haciendo que la misma comunidad de usuarios mejoren la eficacia de sus reglas y el activo desarrollo de las mismas. Gracias a la a funcionalidad de actuar como un IPS además de un IDS Snort se populariza hasta convertirse en la herramienta de detección de intrusiones más usada a nivel mundial (SourceFire, 2012).

Durante años, Snort ha sido la herramienta de facto para realizar un análisis de IDS/IPS sin recurrir a comprar una solución comercial. Su motor combina los beneficios de las reglas mantenidas por la comunidad, inspección de protocolos, e inspección basada en anomalías, esto lo ha llevado a ser uno de los IDS/IPS más usados en el mundo. Snort entró en el salón de la fama del software libre en 2009, al ser declarado como una de las más grandes piezas de software libre de todos los tiempos, por la revista InfoWorld. En 2013 Cisco compra Sourcefire, y el software Snort se ofrece de manera pública y también privada con funcionalidades extra.

En los últimos años entró en escena Suricata, otro IDS de código abierto que presenta las mismas bondades de Snort, es compatible con la mayor parte de sus reglas y análisis de paquetes y además tiene soporte multi-hilo para analizar grandes cantidades de datos en tiempo real, así como análisis para ciertos protocolos de capa siete en el modelo OSSI.

Los firewalls también evolucionaron hasta que se crearon los *Next Generation Firewalls* (NGF), que son aplicaciones de red que hacen un análisis más detallado de los contenidos de un paquete como *Deep Packet Inspection* (DPI), filtrado web, de aplicaciones y de malware, inspección SSL, y defensas activas con función de IPS. Es usual que también permitan la implementación de VPN.

Los sistemas de detección y prevención de intrusiones, de la mano con los NGFW fueron la principal línea de defensa ante las amenazas externas en Internet durante varios años, pero debido a la constante evolución de las amenazas y el crecimiento continuo de los actores maliciosos en Internet, no basta con defenderse ante posibles ataques, también es necesario estar preparado cuando una intrusión pueda ocurrir.

Ante las limitantes que presentan los dispositivos de defensa perimetral, y para responder a los ataques cuando provienen del interior, en los últimos años, las tecnologías de la información, se ha optado por la implementación de herramientas de análisis y correlación de eventos de la seguridad, que buscan ayudar a los equipos de seguridad a reducir el ruido generado por los sistemas de defensa, y a responder adecuadamente en la investigación de incidentes. En respuesta a esta problemática se crean los SEM (Security Event Managment), herramientas enfocadas a la recolección, monitoreo y análisis de los registros de información generados por los dispositivos de red. La idea de implementar estos equipos es recopilar registros de los dispositivos de red y correlacionar la información obtenida mediante el análisis de los registros para generar alertas más certeras, y que estas se generen únicamente cuando se encuentren verdaderos indicadores de compromiso en una red.

Con el tiempo los primeros sistemas de manejo de información de la seguridad (SIM) necesitaron ser escalados a poder procesar todo tipo de eventos provenientes de todo tipo de dispositivos, procesar los registros en tiempo real, y generar un análisis de amenazas en base a estos, visualizar estadísticas, y manejar la respuesta a incidentes. Lo más importante, tomar las decisiones correctas. Aquí es cuando nace el concepto de SEM, un manejador de eventos de la seguridad, a diferencia de un SIM, se enfoca a realizar las funciones de análisis en tiempo real y al manejo de los eventos registrados. En vez de ser una unidad de almacenamiento a largo plazo, un

SEM provee una interfaz de análisis rápido sobre los eventos actuales de la red, y permite a los encargados de seguridad responder oportuna y adecuadamente ante estos.

A medida que se incrementan los ataques informáticos, y que la ciencia forense de sistemas toma más importancia en la respuesta a incidentes, se crearon estándares que especifican una serie de normas a cumplir con el objetivo de proveer un mínimo estándar de seguridad, y de respuesta a los incidentes que pueden registrarse en una organización. Por ejemplo, el estándar PCI-DSS, que desde su versión 1.0 especificaba el requisito de mantener un registro de los eventos de seguridad, fue una gran pauta a la evolución de estos sistemas de recolección y observación, en una unidad integrada de análisis y correlación de eventos que se denominaría SIEM.

1.1.3 ESTADO DEL ARTE

La tecnología de SIEM recopila y agrupa los datos producidos por los dispositivos de seguridad, la infraestructura de red, sistemas y aplicaciones finales. La principal fuente de esta información son los logs (registros), pero muchas tecnologías SIEM también pueden procesar otras formas de datos, como los son los analizadores de tráfico como NetFlow y directamente esnifar paquetes de red o registrar desde SPAN Ports. Una particularidad de gran valor en las actividades diarias de la correlación de eventos está provista por estas herramientas dado que los eventos registrados son combinados con información contextual acerca de los activos, por ejemplo, los relaciona con vulnerabilidades identificadas.

Existen soluciones que incorporan escáneres de vulnerabilidades para aumentar la certeza de seguridad o riesgo en los activos que monitorea, con esto añade a la inteligencia de amenazas, riesgos particulares y otros datos disponibles en la red que le servirán para detectar conductas anómalas.

Un “Activo” se refiere a cualquier dispositivo con una dirección IP única dentro de la red de la organización. Ejemplos de activos pueden ser; routers, firewalls, impresoras, computadoras, servidores, entre otros.

Los datos provenientes de los activos son normalizados de tal forma que los registros, eventos, y la información contextual puedan ser correlacionados y analizados para los propósitos específicos para los que se ha implementado el SIEM. Las tecnologías que proveen correlación de eventos en tiempo real para el monitoreo de la seguridad de activos, ofrecen un valor agregado a la solución, si la aplicación de manejo de eventos implementa funcionalidades extra como consultas avanzadas y análisis histórico de los eventos, se cubren amplios criterios de cumplimiento de normativas,

además de para proveer fuertes referencias que serán de utilidad en la investigación y respuesta a incidentes. Es usual que las herramientas incluyan componentes para la generación de informes sobre las actividades registradas.

Un SIEM basa sus operaciones en torno a una gestión de los eventos y registros generados por los activos de una red. Se espera que posea la capacidad de implementar una infraestructura de gestión de registros, que normalmente se compone de tres niveles:

- Generación de registros
- Análisis y archivo de registros
- Revisión de registros

La adquisición de logs típicamente se efectúa mediante dos técnicas:

- La recolección mediante *sniffing* de la red, es análogo al análisis que realizan los NIDS, monitorean la red en busca de tráfico malicioso o que viola las políticas de la institución.
- La centralización mediante agentes encargados, entre otras funcionalidades, de la recolección de los registros, su función es comparable con un HIDS. Algunos de estos agentes pueden incorporar funcionalidades extra como antivirus o administración remota para proveer una respuesta activa ante un posible incidente.

La integración de las herramientas de IDS e IPS con la tecnología de SIEM provee un valor agregado en el análisis de los registros.

La combinación de estos aspectos en un SIEM es de particular relevancia puesto que complementan mutuamente las deficiencias que puedan presentar otros

componentes; juntos ofrecen una mejor visibilidad sobre lo que está sucediendo en las actividades de los sistemas, incluso cuando alguna intrusión no es detectada inmediatamente, si se presenta conducta anómala se posee suficiente información para investigar el incidente. La necesidad de una detección temprana de los ataques dirigidos está definiendo el rumbo de las nuevas instalaciones de SIEM e incluso las ya existentes.

Las necesidades de las organizaciones de aplicar políticas de análisis en los eventos de seguridad están cada vez más dirigidas al análisis en tiempo real, y la detección temprana de ataques dirigidos, o de violaciones a las políticas de seguridad existentes. Una de las principales motivaciones para realizar el despliegue de un SIEM es cumplir las regulaciones aplicables.

Un aspecto importante a tener en cuenta es que la recolección, almacenamiento, y manejo de los eventos crece rápidamente al mismo ritmo que los sistemas de la información. Lo cual también repercute en la complejidad de generar el análisis y los informes correspondientes de la actividad registrada.

1.1.4 JUSTIFICACIÓN

Las razones que llevan a la implementación de un SIEM en una organización pueden ser diversas, lo correcto debería de ser como una herramienta de refuerzo al alcance del personal de seguridad para ayudarles a detectar incidentes de seguridad y dar respuesta a estos. Especialmente en entornos donde el personal de seguridad tiene que controlar una gran cantidad de activos.

Algunas organizaciones están obligadas a cumplir regulaciones y estándares diseñados para asegurar su correcta operación, e implementación de los recursos de TI, un ejemplo de estas regulaciones es PCI DSS. También, para ganar y/o retener diversas certificaciones es necesario cumplir una serie de requerimientos de protección de la información, como ISO 27001 e ISO 27002, entre otros.

Algunos términos de estas normativas de requerimientos tienen que ver con la administración y retención de los registros generados por los dispositivos tecnológicos.

En muchos casos, los registros son poco apreciados, particularmente en entornos empresariales dónde el cumplimiento de las regulaciones no es de relevancia o nadie los obliga a guardar estos registros. En estos entornos las recomendaciones sobre el almacenamiento de los registros son completamente ignoradas o vistas como una molestia, y los registros únicamente son tomados en cuenta cuando los discos están llenos. Algunas veces simplemente son eliminados sin un tratamiento propio. Es frecuente que, durante un análisis forense, al buscar por registros de información, estos registros simplemente no existen debido a malas prácticas de almacenamiento y menospreciar la información que estos pueden proveer, en muchos casos, este es fin del análisis forense dado que no hay suficiente información para investigar lo

sucedido. Los logs son la principal fuente de información sobre lo que ocurrió durante un incidente de seguridad.

Un administrador de seguridad de sistemas puede ver la importancia de tener un registro de eventos funcional y eficiente. Sin embargo, la tarea de recolectar y analizar estos mensajes puede ser confusa, y agobiante; esto aumenta proporcionalmente conforme al tamaño de la organización.

Cuando se toma la decisión de implementar una solución SIEM, muchas veces trae más problemas que soluciones debido a la poca planeación para implementarla o el poco refinamiento con el que es puesta en marcha. Si no se afinan las reglas de detección y correlación, un SIEM puede generar alertas indiscriminadamente, lo que resulta en más carga para el personal y en vez de reducir su carga de trabajo, solo aumentará. Esto puede llegar a generar pérdidas significativas para la organización que debe invertir una gran cantidad de recursos en la compra de hardware dedicado y de licencias para el software a utilizar, más el sueldo de los empleados que se contratarán para implementar la solución, dependiendo del tamaño de la red, el tiempo destinado al despliegue puede ser igual de costoso que los otros componentes del SIEM.

1.1.5 OBJETIVO

El objetivo del presente proyecto consiste en dar pauta a un debido proceso en el despliegue de soluciones SIEM, buscando realizar este proceso desde un enfoque modular que permita que estas tecnologías sean asequibles por todas aquellas organizaciones que lo requieran.

Esto se ha logrado con base en la investigación del estado del arte de estas soluciones, y mediante el estudio y refinamiento de las mejoras practicas a seguir durante el proceso de selección de una solución y su respectiva implementación apegándose a un enfoque modular, con el objetivo de que la selección de una solución SIEM cubra las necesidades de una organización y que la inversión destinada al despliegue sea acorde a un presupuesto adecuado para las entidades interesadas en implementar un SIEM

Objetivos generales:

- Estudiar el estado del arte de las soluciones SIEM. Analizar los módulos que implementan y reconocer las fortalezas de las diferentes aplicaciones con el objetivo de seleccionar e implementar una solución SIEM a un costo moderado que se enfoque a las necesidades reales de una organización

Objetivos específicos:

- Entender las soluciones SIEM líderes del sector, las características básicas y los casos de uso de estas.
- Comprender los requisitos de hardware, software, humanos y organizativos para una implementación exitosa.

- Implementar un laboratorio de pruebas con diversos equipos de clientes y servidores que serán monitoreados por una solución SIEM para analizar el desempeño de la solución y examinar las características ofertadas por esta.

- Implementar funcionalidades adicionales en función de las capacidades de las soluciones SIEM como análisis de vulnerabilidades, o monitoreo del estado de los equipos en el laboratorio.

2 CAPÍTULO 2 - MARCO TEÓRICO

La importancia de la seguridad de los recursos de los sistemas de TI cada vez es más reconocida, y una compañía debe asegurar la integridad de la información que contienen a toda costa.

En la actualidad existen diversos dispositivos cuya función principal es asegurar los recursos internos de la organización, sin embargo, las amenazas a la información crecen y mejoran a pasos agigantados, y en entornos críticos de alto riesgo, toda medida de precaución resulta insuficiente. Es bien sabido entre los profesionales de seguridad que ningún sistema es a prueba de fallo, y que los atacantes cada día desarrollan técnicas y metodologías de ataques más complejas que ponen en riesgo estas infraestructuras que se busca proteger, y la única manera de estar preparado para responder cuando las defensas caigan, es tener un conocimiento pleno de cómo es que han logrado infiltrarse en la organización, y que acciones han realizado para tomar las medidas necesarias para contrarrestarlo.

La principal arma de defensa en estos casos dónde se han presentado brechas en la seguridad, son los logs o registros.

2.1.1 REGISTROS

Los registros, mejor conocidos como “logs”, en las operaciones de los sistemas de TI, son archivos que graban en disco los eventos o mensajes generados por las actividades suscitadas en un sistema.

La palabra “log” es un término anglosajón, equivalente a la palabra 'bitácora' en español. Sin embargo, se utiliza en los países de habla hispana como un anglicismo derivado de las traducciones del inglés en la jerga informática.

Un log o registro es la respuesta que genera un sistema de cómputo, dispositivo, software, etc. ante algún tipo de estímulo. Estos estímulos dependen en gran medida de la fuente de donde provienen los mensajes de registro, por ejemplo, los sistemas Unix tendrán almacenados mensajes de inicio y cierre de sesión de usuarios, de la misma forma los cortafuegos tendrán mensajes de aceptación y rechazo con base en sus listas de acceso, sistemas de almacenamiento de disco generarán mensajes de registro si se producen fallos. En general, un log se genera para denotar que algo ha sucedido y la información que poseen es la base de su existencia.

En seguridad informática, los logs se usan para registrar datos o información sobre quién, qué, cuándo, dónde y por qué ocurre un evento para una aplicación o dispositivo en particular. Esto con el objetivo de que, en caso de ser necesarios, puedan ser recolectados y analizados con herramientas y técnicas especiales (Chuvakin, Schmidt, & Phillips, 2013).

Un mensaje de log debe contener información descriptiva sobre el evento, principalmente el tipo de evento, el contenido, y la fecha y hora en que aconteció el evento.

Clasificación de los logs

Informativos: Los mensajes de este tipo están diseñados para permitir a usuarios y administradores saber que ha ocurrido algo. Por ejemplo, al reiniciar un sistema se generan mensajes informativos al respecto. Si un reinicio se produce fuera de las horas normales de mantenimiento o de negocios, es posible que tenga razón para alarmarse, y un mensaje que simplemente se generó para ser informativo se convierte en una parte crucial dentro de una investigación o respuesta a incidentes.

Depuración: Los mensajes de depuración se generan en los sistemas de software con el fin de ayudar a los desarrolladores de software a solucionar e identificar problemas con el funcionamiento de código de la aplicación.

Advertencia: Los mensajes de advertencia se producen en situaciones en las que algo puede fallar. Por ejemplo, si a un programa no se da el número correcto de argumentos de línea de comandos, pero todavía puede funcionar sin ellos, es algo que el programa puede registrar simplemente como una advertencia al usuario.

Error: Los mensajes de error se utilizan para transmitir los errores que se producen en varios niveles de un sistema informático. Por ejemplo, un sistema operativo puede generar un mensaje de error cuando no es posible realizar escritura en disco. Por desgracia, los mensajes de error sólo dan un punto de partida en cuanto a porqué se produjeron. A menudo se requiere investigación adicional para llegar a la raíz de la causa del error.

Alerta: Una alerta se genera para indicar que algo interesante ha sucedido. Las alertas, en general, son el dominio de los dispositivos de seguridad y los sistemas

relacionados con la seguridad. Por ejemplo, los mensajes que genera un IPS cuando detecta una actividad que podría ser maliciosa.
Esta diversidad en los mensajes de registro da pauta a una post-categorización en base a la relevancia de estos mensajes en base la prioridad que presentan.

Para cada organización, la noción de prioridad es algo que hay que estandarizar, puesto que cada entorno es diferente, un mensaje que puede ser perfectamente normal en un sitio se seguridad media, en entornos de alta seguridad puede ser motivo para desencadenar una alerta critica. De igual manera, en base a la diversidad de los tipos de mensajes que se generan, es necesario crear un modelo que permita analizar la información que presentan.

Básicamente, la prioridad de los mensajes de registro está basada en 3 categorías principales, baja media y alta.

Baja: eventos de prioridad baja son los que son básicamente informativos y no necesitan ser tratados a medida que ocurren, pueden ser investigados en el tiempo libre o simplemente ser almacenados sin mayor tratamiento.

Medio: los eventos de prioridad media tienden a ser cosas que pueden necesitar ser analizados de una manera oportuna, pero no necesariamente de inmediato. Por ejemplo, los IPS tienden a tener la capacidad de bloquear el tráfico de red cuando el motor detecta actividad con intención maliciosa. Al suceder esto, un IPS emite un mensaje de registro. Al revisar el registro se puede saber que el tráfico fue bloqueado y se puede investigar más tarde.

Alta: eventos de prioridad alta son los que requieren una intervención inmediata. Ejemplos de eventos de alta prioridad puede ser un DLP que alerta de una posible

fuga de información, o un dispositivo de red troncal que deja de responder por un período prolongado de tiempo. (Chuvakin, Schmidt, & Phillips, 2013)

Existen autores que prefieren extender la clasificación de prioridad a 5 categorías, añadiendo: Muy baja o Informativo, y Muy alta o Crítica; siendo la principal función de estas clasificaciones extender la categorización para una mejor distribución del tiempo invertido en cada alerta.

Ante la información clave que ofrecen los logs, un administrador de sistemas puede ver la importancia de tener un registro de eventos funcional y eficiente. Sin embargo, la tarea de recolectar y analizar estos mensajes puede ser confusa y agobiante.

Complicaciones referentes a los registros

Un análisis efectivo de los registros no es fácil puesto que requiere bastante trabajo. Cada fabricante crea sus propios formatos de mensajes de registro, esto produce que los logs se produzcan en una cantidad de formas y tamaños tan diversa que la tarea del análisis se vuelva incomoda. A esto hay que añadir que a veces puede ser difícil extraer información de ellos dado que los datos de registro del sistema pueden ser especialmente malos, ya que muchos de los datos que presentan vienen en un formato de texto libre y no siempre son tan descriptivos como se desea.

Esto conlleva que, para hacer un análisis efectivo, sea necesario tener un conocimiento extenso del entorno en el que se trabaja. En específico, conocer que es bueno y que es malo en la actividad de la red. Lo que en un entorno como una unidad académica puede ser normal, por ejemplo, un cliente de BitTorrent para compartir

archivos, en un entorno bancario representa una amenaza para la integridad de los datos de la organización.

Desafortunadamente, se ha identificado que, durante las investigaciones forenses de filtraciones de datos, muchas organizaciones continúan operando completamente inconscientes de que sus datos han sido comprometidos, principalmente a causa de que los logs se han desactivado por problemas de rendimiento en los sistemas, o fueron sobrescritos debido a la rapidez con la que se generan los mensajes, o en casos donde si existen logs, pero no eran monitoreados, o no se registraban los eventos que eran de importancia en el sistema (Visa Europe, 2012).

En muchos casos, los registros son poco apreciados, particularmente en organizaciones dónde las regulaciones sobre el almacenamiento de estos no son tomadas en cuenta, los logs son ignorados o vistos como una molestia, y únicamente son tomados en cuenta cuando los discos están llenos. Algunas veces simplemente son eliminados sin un tratamiento propio. Es frecuente que, durante un análisis forense, al buscar por registros de información, estos simplemente no existen debido a malas prácticas de almacenamiento de los registros y/o menospreciar la información que estos pueden proveer, en muchos casos, este es el fin del análisis forense dado que no hay suficiente información para investigar el incidente. Los logs son la principal fuente de información sobre lo que ocurrió durante un incidente (Chuvakin, Schmidt, & Phillips, 2013).

Procesamiento de los registros

Los mensajes de registro deben ser tratados de acuerdo a políticas de seguridad o estándares de cumplimientos de normativas. Aunque existen diversas variantes del tratamiento que deben recibir estos mensajes, existen fases fundamentales que aplican por igual para efectuar las mejores prácticas de tratamiento de estos mensajes.

Las principales fases en el ciclo de vida de un log son:

- Generación
- Recolección/Centralización
- Normalización
- Almacenamiento
- Análisis/Correlación

Generación: Un evento pude originarse en una gran cantidad de dispositivos, y la eficiencia del mensaje generado se define en base a la información que aporta para reconocer el evento que suscita la generación del mensaje.

Recolección/Centralización: Cuando se genera un evento, es necesario que éste sea enviado a una consola de centralización de la información con el objetivo de que sea procesado y almacenado de forma que sirva para un posterior análisis.

Normalización: Debido a la amplia variedad de fabricantes, la sintaxis de los mensajes de registros es aún mayor dado que cada fabricante define un formato específico para el formato de los mensajes generados por sus dispositivos. Por esto,

es necesario estandarizar y normalizar la información recopilada para que sea posible almacenarlos y efectuar un análisis de la información recopilada.

Almacenamiento: Una vez que los mensajes de registro han sido normalizados, se deben de almacenar en un lugar seguro para que puedan ser recuperados en caso de ser requeridos, esto ayuda a investigar incidentes de seguridad o eventos dónde por algún motivo los mensajes originales no están disponibles. Algunas normativas indican que se deben almacenar tanto el mensaje original como el mensaje normalizado, por esto es importante realizar una buena planeación del manejo de registros en base a las necesidades de la organización.

Análisis/correlación:

En el proceso de análisis de un log, es necesario identificar el tipo de registro que se está tratando, por lo general, de forma coloquial se clasifican en alto medio y bajo, aunque dependiendo de las plataformas de análisis se añaden clasificaciones extra como “informativo” y “muy alto”, esto con objetivo de clasificar mejor los incidentes que no tienen una relevancia significativa y aquellos que deben ser tratados inmediatamente o presentan un fallo fatídico para el sistema a monitorear.

Syslog

Syslog es un estándar definido para la gestión de bitácoras de eventos, el cual permite el manejo de los mensajes generados por los dispositivos en la red. Estos dispositivos pueden ser desde impresoras y cámaras, hasta routers, firewalls y todo tipo de dispositivos computacionales.

Habilita la separación de los sistemas que participan en el ciclo de vida de los registros. Los principales actores en este ciclo son: el sistema que genera los mensajes, el sistema que los almacena, y el software que los almacena y los analiza.

Los diseñadores de sistemas usan los registros generados por syslog en una amplia variedad de escenarios como pueden ser: la administración de sistemas, auditorias de seguridad, revisión de eventos informativos, análisis e inspección de mensajes de error, etc. En general, syslog puede informar sobre cualquier anomalía en el funcionamiento del sistema.

El funcionamiento del protocolo syslog se basa en el modelo de cliente servidor, dónde el cliente envía pequeños mensajes de una longitud menor a 1024 bytes. Los mensajes de syslog por lo general se suelen enviar por el protocolo UDP en el puerto 514 en formato de texto plano. Pensando en las implicaciones de seguridad que puede presentar el uso del protocolo syslog, se han creado mejoras en la implementación del protocolo, como syslog-ng que permite usar TCP en vez de UDP, y ofrece soporte para que los datos viajen cifrados mediante SSL/TLS.

El mensaje de syslog se compone de 3 campos principales

- Marca de tiempo
- Prioridad

- Texto del mensaje

Syslog emplea un código de severidad que se denota en los 3 bits menos significativos del campo de prioridad se define en el RFC 3164 y categoriza los mensajes en 8 posibles grados según sea pertinente:

- 0 Emergencia: el sistema está inutilizable
- 1 Alerta: se debe actuar inmediatamente
- 2 Crítico: condiciones críticas
- 3 Error: condiciones de error
- 4 Peligro: condiciones de peligro
- 5 Aviso: normal, pero condiciones notables
- 6 Información: mensajes informativos
- 7 Depuración: mensajes de bajo nivel

Syslog puede ser configurado para enviar mensajes repetitivos cada cierta periodicidad de tiempo, y este factor puede ser crucial a la hora de analizar los registros, muy poco tiempo hará que se genere una multitud de mensajes saturando el servidor, y muy poco puede hacer que se pierdan mensajes de registro que pudieron haber sido importantes o se caiga en incumplimiento de normativas

2.1.2 ANÁLISIS DE REGISTROS

Logs en el análisis forense

Un análisis forense consiste en construir una imagen sobre lo ocurrido después de que se suscita un incidente. Esta imagen es construida a partir de información que la mayoría de las ocasiones está incompleta, y la credibilidad de esta información disponible es crítica. Los logs ayudan a dar validez a este proceso.

Una vez almacenados, los logs no son alterados durante el funcionamiento normal de una aplicación, de esta forma, pueden proveer una manera fiable de comprender y complementar los datos alojados en el sistema al que se le realiza un análisis forense.

Cualquier actividad de hacking por su propia naturaleza de interacción con un sistema produce mensajes que son registrados por una variedad de sistemas. Idealmente, estos mensajes deberían detonar una alerta que permita detectar el ataque y mitigar sus consecuencias.

El hecho de que los logs posean una marca de tiempo, provee de una secuencia cronológica de los eventos suscitados, mostrando no solo lo que pasó, sino también el orden en que sucedieron los hechos. Esto da pauta a construir una línea del tiempo sobre la cual es más fácil comprender lo sucedido.

Los atacantes conocen bien un sistema y saben que los logs guardan registro de sus movimientos en cada paso que dan, por esto muchas veces los atacantes hábiles buscan corromper los registros almacenados en los sistemas que logran comprometer.

El análisis de los logs en el trabajo diario

El objetivo de implementar un análisis de los logs varía en cada organización. Una institución bancaria tiene una meta diferente que una cadena de restaurantes. Sin embargo, ambos buscan tener un mejor nivel de comprensión más alto de la información que proveen los registros, y este factor aplica para casi todos los actores involucrados en los sistemas de información. Estos niveles generalmente se refieren a la detección de errores, la depuración de estos errores, y la generación de alertas.

Referente al análisis de los logs, generalmente se va a buscar, además de reconocer las cosas malas que suceden, reconocer cosas que aún no sabemos que son malas, nunca se han visto antes o no se tenía idea de que sucedían, pero eventualmente podrían convertirse en la forma en la que un atacante logre inmiscuirse en el entorno de la organización. La dificultad de esto reside en que, por lo general, este tipo de análisis no es fácil de realizar haciendo una revisión manual de los logs, siempre requiere el uso de técnicas más sofisticadas.

Planeando el análisis

La mayoría de las brechas en la seguridad tienen algo en común, no siempre son eventos excesivamente técnicos, de hecho, en la mayoría de los casos podrían haberse detectado fácilmente mucho antes de lo que usualmente son detectadas. La evidencia disponible de investigaciones forenses indica que un 40% de las brechas en la seguridad permanecen sin ser detectadas inclusive durante meses (Visa Europe, 2012).

Al desarrollar una estrategia del manejo de registros se debe buscar obtener el máximo beneficio del análisis, para lo cual es necesario implementar una solución que ayude a manejar y relacionar los eventos registrados y para esto es necesario conocer los sistemas que se planean monitorear.

Para hacer una planeación del análisis de los logs es necesario identificar diversos puntos, siendo los más inmediatos:

- Que información debe ser capturada y de que sistemas.
- Cuanto tiempo es necesario mantener la información almacenada, ya sea por requerimientos o certificaciones.
- Cómo y dónde se van a almacenar los registros.
- Definir el equipo encargado de revisar las alertas, generar los reportes y escalar los incidentes según sea necesario.

De la misma forma, es necesario identificar los datos que serán registrados

- Identificar cuentas de usuarios y los sistemas involucrados.
- Definir las categorías de los tipos de eventos.
- Resultados y acciones ante un evento.
- Origen y localización de un evento.
- Detalles de los datos, sistemas componentes o recursos afectados por un evento.

Una de las principales dificultades en el análisis de los logs es la precisión y esta se refiere a que los datos sean enviados, recibidos, procesados, y almacenados de la forma que se desea, sin sufrir defectos y/o alteraciones, o bien que presenten información engañosa o errónea que enturbie el análisis como es deseado.

2.1.3 MEDIDAS DE SEGURIDAD QUE COMPLEMENTAN EL ANÁLISIS DE LOGS

Los primeros pasos para asegurar la información en una compañía consisten en identificar los recursos que se quieren asegurar, identificar qué son, dónde se encuentran, para qué se usan, y quiénes los pueden usar. Una vez que se han identificado es necesario diseñar un plan de seguridad para estos activos. Dependiendo del activo a proteger será necesario tomar acciones particulares para asegurar los recursos que se desean proteger. Las herramientas que proveen las medidas más importantes a considerar en el proceso de proteger recursos de TI, suelen ser:

- Sistemas de protección y detección de intrusiones.
- Contrafuegos de nueva generación.
- Escaneo de vulnerabilidades.

IDS

La detección de intrusiones es el arte de detectar actividad inapropiada, incorrecta o anómala, y dos herramientas que ayudas a lograrlo son los sistemas de detección y prevención de intrusiones (Holland, 2004).

Las herramientas como los IPS e IDS ofrecen una primera capa de defensa ante posibles amenazas en la red interna. Ambos detectan actividad maliciosa por parte de malware, spyware, virus, gusanos y otros tipos de ataques como DoS e intentos de fuerza bruta. Los IDS monitorean pasivamente y reportan actividad sospechosa,

mientras que los IPS monitorean activamente la línea y previenen ataques mediante el análisis de las comunicaciones (Scarforne & Mell, 2001).

Los sistemas de detección de intrusiones son dispositivos o aplicaciones que monitorean la red o las actividades de un sistema en busca de actividad maliciosa o violaciones en la política de uso, y producen reportes sobre las alertas generadas, las alertas se almacenan para ser desplegadas en una interfaz de administración. Están diseñados para recolectar y analizar la información que se transmite entre hosts a través de la red con el objetivo de identificar posibles brechas en la seguridad, en específico intrusiones o intentos de intrusión, permitiendo tomar las medidas pertinentes para que el equipo del SOC pueda realizar las actividades de mitigación y remediación del ataque. Un IDS no va a prevenir ataques, pero ayudará a reconocer cuando ocurran y ofrecerá información sobre como remediarlo.

Para asegurar una cobertura de seguridad mayor se han desarrollado diversas variantes de IDS, cada una enfocada a ofrecer un valor específico a la funcionalidad que cumple, existiendo dos tipos principales de IDS:

- Sistema de detección de intrusiones basados en red (NIDS).
- Sistema de detección de intrusiones basados en hosts (HIDS).

Las principales características de los NIDS y los HIDS incluyen:

- NIDS
    - Monitorear y analizar la red y las actividades de los sistemas.
    - Reconocer patrones típicos de un ataque de red.
    - Analizar patrones anormales de tráfico en la red.
- HIDS
    - Analizar las configuraciones y vulnerabilidades de un sistema.

- Evaluar la integridad del sistema y los archivos.
- Analizar patrones de actividad anormal por parte de los usuarios.
- Seguimiento de violaciones en la política de usuarios (uso).

Los IDS tradicionales han estado en funcionamiento por varios años y forman parte central de cualquier buena práctica de seguridad. Pero en años recientes, parecer que las capacidades tradicionales de un IDS no son suficientes para entregar una solución completa de seguridad.

Una instalación autónoma de IDS provee de una visión muy reducida de los vectores de amenaza que asechan una organización, los IDS necesitan ser complementados con otras capacidades de seguridad para alcanzar un buen nivel de detección de amenaza y respuesta ante los diferentes ataques que puede sufrir una organización. Las organizaciones necesitan una solución de IDS capaz de priorizar alertas y proveer un cierto nivel de contexto para cada alerta. Cuando una alerta muestra un nivel de contexto que denota su origen, permite que los equipos de seguridad se enfoquen en resolver el problema que está causando estas alertas en vez de desperdiciar tiempo y esfuerzo en identificar qué es lo que está sucediendo.

Otro componente crucial para analizar la eficacia de un IDS tiene que ver con la “Inteligencia sobre Amenazas” (Threat Intelligence), que es la información con la que el IDS identifica a los actores maliciosos, sus herramientas, infraestructura y métodos. La inteligencia de amenazas efectiva es esencial para hacer que las montañas de datos internos y externos tengan sentido de manera significativa con el objetivo de ofrecer una detección de amenazas eficiente y priorizar la respuesta.

Para implementar un programa de seguridad efectivo, es necesario encontrar una solución que ofrezca estas funcionalidades clave.

- Funcionalidades que hacen un IDS efectivo
    - Enfoque basado en red y Hosts NIDS, y HIDS.
    - Enfoque basado en firmas.
    - Funcionalidades de detección de intrusiones distribuido (DIDS) para entornos extensos.

IPS

Un IPS funciona de forma análoga a un IDS, con la principal diferencia que un IPS se coloca en medio del tráfico, y es capaz de prevenir activamente intrusiones cuando se detectan.
dispositivos de IPS puede tomar acciones de respuesta como generación de alarmas, anulación de paquetes maliciosos detectados, abortar conexiones sospechosas, o bloqueo de tráfico basado en direcciones IP o físicas. El IPS también puede corregir errores de registro de errores (CRC) errores, desfragmentar flujos de datos, mitigar problemas referentes a las secuencias de TCP, y limpiar datos y las opciones de red de las aplicaciones finales.

Además de la respuesta activa, cualquier ocurrencia de actividad sospechosa o que incumpla las reglas de actividad permitida, suele informarse mediante una interfaz de gestión a un administrador o mediante registros a un sistema de administración de eventos de seguridad de la información (SIEM).

Rendimiento del IDS/IPS

Un factor fundamental para evaluar el rendimiento de un IDS/IPS es el análisis de protocolos que efectúa sobre los paquetes que recibe. Este análisis está basado en

las reglas que sean definidas, y dependiendo de la extensión y complejidad del conjunto de reglas especificado, un sistema de detección o prevención de intrusiones puede ser sobrecargado en tareas de análisis y puede comenzar a perder tráfico de red. Para evitar esto se recomienda optar por soluciones que tomen un enfoque multi-hilo para que la tarea de análisis no presente pérdidas de paquetes si el análisis que se requiere es muy intensivo. Hay situaciones, por ejemplo, instituciones financieras, dónde el análisis debe ser riguroso, y en estos entornos de alta seguridad, dónde no es posible reducir la cantidad de reglas de detección, y frecuentemente tiene muchas sucursales remotas, puede ser necesario evolucionar el sistema de detección de intrusiones a un entorno distribuido, para lo que se debe considerar que el sistema de detección de intrusiones sea escalable a la arquitectura de implementación que se planea.

Si el entorno no es de alta seguridad, y se detectan niveles altos en la carga de la CPU, hay que verificar si en verdad se está analizando lo que es de interés para la organización, y en caso de que no, se puede contemplar la posibilidad de usar un conjunto de reglas de detección más pequeño, o más enfocado a los intereses particulares de la organización.

Agregación

Para esta investigación, el principal factor de inclusión se basa en las capacidades de integración con otras tecnologías o plataformas. En específico, las tecnologías de IDS que tienen mejoras de contexto, esto es, capacidad de integración con un SIEM.

NGF NEXT GENERATION FIREWALL

Una medida extra de seguridad en el análisis de paquetes consiste en usar un Next-Generation Firewall o contrafuegos de nueva generación, que es una plataforma integrada que combina las funcionalidades de un firewall tradicional, con algunas de las funcionalidades de un IPS, e integra funcionalidades extra de detección en la capa de aplicación usando diferentes técnicas de inspección como: DPI (*Deep Packet Inspection*), intercepción de SSL, filtrado web, administración de QoS y ancho de banda, inspección antivirus e integración a herramientas de terceros.

Una ventaja enorme de usar un NGFW como frontera a Internet en una organización es su filtrado de aplicaciones, de esta manera se ayuda enormemente a asegurar el cumplimiento de las políticas de la institución sobre el uso de los recursos de red. Además de que una gran parte de los NGFW ofrecen capacidades de integración con SIEM, lo que ayuda al sistema de correlación a ser más preciso en el número de alertas que se generan, permitiéndole a los encargados de la seguridad a enfocarse en las verdaderas amenazas para la organización.

WAF

Los firewalls de aplicaciones web (Web Application Firewall) protegen aplicaciones web internas de una amplia gama de ataques externos. Proporcionan una detección avanzada de seguridad para proteger recursos web contra las principales amenazas a las aplicaciones hoy en día: Inyección SQL, Cross Site Scripting, ataques de inyección, entre otros.

2.1.4 CASOS DE ESTUDIO

Durante la investigación de herramientas IDS, se identificaron dos soluciones NIDS con funcionalidades de IPS, Snort, y Suricata, ambas de código abierto, y un HIDS, OSSEC que también está basado en licencias de código abierto. Todas ellas con capacidad de integración a un SIEM.

Snort

Snort es un NIDS que posee la capacidad de analizar tráfico en tiempo real, y registro de paquetes en redes IP. Snort efectúa análisis de protocolos en búsqueda de coincidencias en el contenido de los paquetes con sus reglas de detección de intrusiones. Las reglas de detección de Snort pueden detectar desde simples violaciones en las políticas de uso como redes sociales, hasta ataques de desbordamiento de buffer. Snort puede ser configurado en 3 funcionalidades:

- Sniffer:
    - El programa lee paquetes desde una o varias interfaces de red y los muestra en consola.
- Packet logger:
    - Lee paquetes en las interfaces de red configuradas y los guarda en el disco duro.
- NIDS:
    - El programa analiza y compara el paquete contra reglas definidas por el usuario, después ejecuta una acción en base a lo que se ha identificado.

Cuando Snort trabaja en modo NIDS puede operar en 2 modos: activo o pasivo, siendo la principal diferencia que, al funcionar en modo activo, Snort se ubica en mitad

de la línea entre dos dispositivos de red, actuando como un IPS, inspeccionando el tráfico cuando viaja de una interfaz de red a otra, Snort puede tomar decisiones sobre el tráfico que lo atraviesa según las configuraciones que le hayan sido efectuadas. De otra manera, cuando Snort se encuentra en modo pasivo, únicamente escucha y alerta sobre las coincidencias del contenido de los paquetes contra las reglas definidas.

La principal debilidad de Snort, está en su arquitectura mono proceso, esto implica que, bajo cargas de trabajo altas, aunque Sourcefire anunció que la versión 3.0 de Snort tendrá soporte multiproceso, actualmente, de forma nativa, Snort no tiene la posibilidad de efectuar un análisis concurrente en múltiples núcleos de un procesador.

Suricata

Suricata es un software relativamente nuevo, desarrollado y mantenido por la Open Information Security Foundation (OISF). Recientemente ha comenzado a tomar auge en la escena de los IDS/IPS y sus resultados son muy prometedores. El funcionamiento de Suricata es muy parecido a Snort, y al igual que él está basado en firmas y reglas, pero integra funcionalidades y técnicas revolucionarias. El motor de análisis incluye diversas mejoras que lo convierten en una herramienta con gran potencial, integra un normalizador y analizador sintáctico de HTTP basado en la librería HTP que provee un procesamiento avanzado de flujos de HTTP, detecta automáticamente el protocolo usado y tiene soporte para TLS, FTP y SMB, también el analizador HTP puede descomprimir y decodificar flujos comprimidos con Gzip. Este conjunto de características permite el entendimiento del tráfico en la séptima capa del modelo OSI.

Parámetros	Suricata	Snort
IPS	Opcional mientras se compila (`--enable-nfqueue`)	Snort_inline (`snort -Q`)
Reglas	VRT::Snort EmergingThreats	VRT::Snort EmergingThreats SO rules
Hilos (*Threads*)	Multi-Thread	Single-Thread
Instalación	No disponible desde paquetes o repositorios (instalación manual)	Relativamente sencillo, disponible en paquetes.
Documentación	Algunos recursos en Internet	Ampliamente documentado
Soporte para IPv6	Completamente soportado	Soportado si se compila con la opción –enable-ipv6
Aceleradores de captura de paquetes	PF_RING capture accelerator	Ninguno, usa libpcap
Configuración	suricata.yaml clasification.config reference.config threshold.config	snort.conf threshold.conf

Ilustración 1 - Comparativa entre Snort y Suricata

OSSEC

OSSEC es un software de detección de intrusiones basado en host (HIDS), que realiza análisis de los registros, comprobación de integridad en los archivos, monitoreo del registro de Windows, detección de *rootkits*, y respuesta activa permitiendo ejecutar acciones ante una alerta detectada. Está disponible para Linux, OpenBSD, FreeBSD, OSX, Solaris, y Windows. Su arquitectura de múltiples plataformas con un control centralizado permite que entornos heterogéneos de sistemas sean fácilmente monitoreados.

El Manager, o servidor central es la pieza central del despliegue de OSSEC. Se encarga de almacenar las entradas de las bases de datos, registros, eventos, etc. Todas las reglas, parsers, y grandes opciones de configuración son almacenadas en el servidor central, haciendo relativamente sencillo administrar un gran número de agentes.

Un agente es un programa instalado en los sistemas a ser monitoreados. El agente recolectará información y la reenviará al manager para su posterior análisis y correlación. Algunas piezas de la información son recolectadas en tiempo real, mientras que otras periódicamente, lo que permite mantener un impacto bajo en el desempeño del sistema.

Integración de las herramientas estudiadas

Reenviar los logs a un recolector centralizado, provee una fuente de evidencia que está separada de la fuente de origen. Si los registros originales se ven corrompidos, esta información queda inalterada y puede ser considerada una fuente mucho más fiable de información para su análisis.

De igual manera, los registros provenientes de diferentes fuentes, pueden corroborar otra evidencia y reforzar la exactitud de cada fuente. Por ejemplo, un firewall de aplicación que registra conexiones entrantes y rechaza múltiples ataques hasta que uno tiene éxito, comparando los registros contra los almacenados en el DBMS se puede conocer con precisión las técnicas empleadas durante el ataque.

Los logs refuerzan la evidencia recolectada en cada dispositivo, a menudo recreando con exactitud la secuencia de los eventos, en especial cuando provienen de diferentes fuentes: ficheros y sus marcas de tiempo, datos de la red, el historial de los comandos ejecutados en un sistema, etc. De igual manera pueden ayudar a indicar si otras áreas han sido atacadas por algún intruso.

Una posible evolución de los logs puede estar dada por un HIDS, como OSSEC, que además de analizar los logs, tiene la capacidad de reenviarlos a un concentrador central dónde se guardará una copia en caso de que el host presente fallas o alteraciones de sus registros.

Las ventajas de usar un sistema centralizado de logs son las siguientes:

- Se obtienen los registros de diversas ubicaciones en una única ubicación centralizada.
- Es un lugar para guardar una copia de respaldo de los logs.
- Se tiene un lugar para realizar un análisis de los datos registrados.

Las herramientas de detección y prevención de intrusiones, y los NGFW, proveen de un análisis profundo del tráfico, y son de vital importancia en los mecanismos de defensa de una red, pero aún son susceptibles a ataques de evasión y no garantizan por completo la seguridad.

Para tener una adecuada respuesta ante un incidente de seguridad es necesario tener la mayor cantidad de información posible. Esto puede ser proporcionado mediante la integración de herramientas de análisis y correlación de eventos de la seguridad de la información, un SIEM.

2.1.5 SIM, SEM, y SIEM

Los conceptos de SEM, SIM, y SIEM a menudo son utilizados indistintamente para referirse a las herramientas de recolección y análisis de eventos de seguridad, pero existen características puntuales que permiten definirlos

Security Event Manager (SEM)

Son herramientas computaciones que se usan en las redes para centralizar el almacenamiento, normalización, e interpretación de registros o eventos de seguridad generados por otros sistemas en la red. Proveen monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de consolas.

Usualmente se basan en bases de datos SQL y en algunos casos implementan gestión de incidentes y de operaciones de seguridad.

Security Information Management (SIM)

Es un tipo de software que automatiza la recolección de eventos y registros de dispositivos de seguridad como firewall, proxies, IDS y antivirus. Después traduce y normaliza los datos recolectados en formatos simplificados que permiten generar correlaciones, reportar los hallazgos y en algunos casos realizar acciones proactivas de acuerdo a los eventos detectados.

SIEM &LOGS

Dentro del análisis de la información, Un evento es una ocurrencia individual en un entorno, usualmente de relevancia, que implica un cambio de estado. Los logs son

una colección de eventos presentados en un formato particular de acuerdo al dispositivo que los genera. Dentro de un SIEM, como su nombre lo indica, se busca recolectar eventos de seguridad que describan incidentes de seguridad.

Un incidente de seguridad se produce cuando uno o más eventos de seguridad indican que algo malo ha ocurrido en el entorno. La definición de algo malo, varía enormemente de organización a organización, puede implicar desde un acceso a un sistema en una hora irregular, robo de información, denegaciones de servicio, o un rango infinito de posibilidades que únicamente las partes internas de la organización están habilitadas para considerarla un incidente de seguridad o un evento que no implica mayores riesgos para el correcto funcionamiento de su entorno.

Bases para la implementación de un SIEM

Existen diversas motivaciones para desplegar una solución SIEM. A continuación, se exploran algunas de las principales necesidades en las organizaciones que los motivan a implementar un SIEM.

Cuando es necesario mejorar la inteligencia de amenazas que ponen en riesgo los activos de una organización, o bien para tener un respaldo durante investigaciones forenses que ofrezcan más detalles sobre posibles incidentes de seguridad.

Un factor más es la capacidad de ofrecer respuestas automáticas cuando se detectan brechas en la seguridad. Usualmente estas brechas solo pueden ser detectadas a través de la correlación de diversos eventos, y los SIEM pueden integrar capacidades de detección y respuesta automática, alertar a los administradores y/o bloquear el origen del ataque.

Algunos SIEM incluyen motores de escaneo y gestión de vulnerabilidades que ayudan a detectar riesgos y gestionar su mitigación antes de que ocurren incidentes.

Es importante mencionar que este tipo de funcionalidades, si no están incluidas en el licenciamiento base del SIEM, suele incrementar los costos de la implementación final.

Otro factor se refiere a las normativas y los requisitos de cumplimiento a los que deben adaptarse ciertas organizaciones para cumplir ciertas regulaciones. Por ejemplo, poseer informes que demuestran que se está registrando eventos como el acceso a los activos críticos por ejemplo sistemas contables, sistemas de procesamiento de tarjetas de crédito, etc. Otra prueba se presenta en forma de auditores que se arrastran a través de diversas partes de su entorno, como registros de configuración del dispositivo, Los sistemas de control de errores, sistemas de control de código fuente, etc., y aunque existen soluciones DLP (*Data Leak Prevention*) que proveen estas funcionalidades, no siempre son suficientes para satisfacer un cumplimiento total de las regulaciones.

Tener un almacenamiento a largo plazo de estos registros puede convertirse en un problema a medida que los discos se llenan de mensajes, además del problema que implica recuperar estos log en grandes despliegues de sistemas informáticos.

En el caso del análisis de esta información, es de vital importancia poseer un lugar de almacenamiento dónde estos mensajes puedan ser filtrados y normalizados en una base de datos relacional, para proceder con el análisis y posteriormente el reporte de qué es lo que está sucediendo exactamente en una organización.

2.1.6 SELECCIÓN DE SOLUCIONES SIEM

Actualmente existen diversas soluciones SIEM comerciales con un grado de madurez significativo, sin embargo, existe un gran desconocimiento de estas herramientas, tanto en la iniciativa privada como en el sector público, en especial en la PYME. En la gran empresa, proyectos de este tipo no han sido exitosos por que las expectativas de lo que se puede conseguir no son correctas, porque no se ha realizado un dimensionamiento correcto antes de iniciar el proyecto, o simplemente porque la herramienta seleccionada no estaba diseñada para cumplir las necesidades por las que se le buscaba.

Existen diferentes factores que influyen en la toma de decisiones sobre qué solución SIEM implementar, a continuación, se listan los puntos más importantes a considerar para reducir los costos de implementación:

Tamaño de la organización:

Cuando se exploran soluciones SIEM, es necesario considerar el tamaño del despliegue, pues esto influye enormemente en el precio del licenciamiento de las diversas soluciones. Existen soluciones que basan sus precios en la cantidad de tráfico generado, y otras más que lo hacen en base al número de dispositivos a monitorear. Además de que el tamaño de la red de destino influye en la complejidad de instalación de los sensores y agentes que recolectarán los registros.

Presupuesto

Debido a que el principal factor limitante al momento de implementar soluciones de tecnología es el presupuesto económico, no se puede ignorar en el despliegue de las soluciones SIEM, en especial por que como se mencionó anteriormente, el volumen

de datos y el tamaño de la organización son la base del precio de las principales soluciones comerciales.

Objetivo particular de la implementación

Uno de los factores decisivos para optar por una u otra solución es el objetivo particular por el cual se está implementando. Diferentes fabricantes ofrecen diferentes enfoques a los que están orientado sus productos, algunos buscan ofrecer una completa suite de gestión de riesgos con sistemas de gestión de tickets, y manejo de respuesta a incidentes, mientras otras se enfocan en profundidad al análisis de la información recolectada. Sólo el cliente final sabe con exactitud para que quiere usar el producto.

Para elegir las soluciones SIEM se tomaron en cuenta todos los componentes que se han expuesto a lo largo de este documento. Haciendo énfasis en la integración de un sistema modular a bajo costo, se buscaban soluciones que implementaran las siguientes funcionalidades:

- Capacidades de detección de intrusiones a nivel de red, y de hosts.
- Integración con otras plataformas.
- Tipo de licenciamiento.
- Cumplimiento de normativas.

Como resultado de la investigación realizada, se pudieron identificar 3 soluciones líderes en el mercado que destacan por una madurez significativa en el cumplimiento del objetivo para el que están diseñadas.

2.1.7 SOLUCIONES SIEM SELECCIONADAS

Basados en un análisis de requerimientos debe ser posible integrar un prospecto de soluciones que efectúen las características necesarias para un despliegue de SIEM. Es particularmente útil considerar como funcionan algunas soluciones bajo ciertos escenarios. Algunas de las consideraciones más recalcables son:

- La complejidad de integrar las fuentes de eventos.
- Definir los formatos de los logs.
- Describir reglas de correlación complejas.
- Integración a otras plataformas.
- Cantidad de activos.
- Eventos a analizar.
- Regulaciones aplicables.

Con base en estos análisis se han identificado una gran cantidad de soluciones SIEM líderes en el marcado, que implementan las principales funcionalidades descritas con anterioridad, y de acuerdo a las necesidades de una empresa cumplen los requerimientos con una proporcionalidad entre costo y beneficio adecuada, de ellas han sido seleccionadas 3 soluciones que se enfocan a cubrir diferentes aspectos a considerar al implementar un SIEM, fue posible obtener licenciamiento y documentación de las soluciones que se describen a continuación:

- AlienVault USM y OSSIM.
- Splunk.

- HP ArcSight ESM y Express.[1]

AlienVault USM/OSSIM

La solución de AlienVault Unified Security Management provee de un SIEM, descubrimiento y manejo de activos, escaneo y administración de vulnerabilidades, sistema de detección de intrusiones a nivel de hosts y de red, y monitoreo de integridad de archivos y del registro de Windows, así como recolección y monitoreo de registros.

En su principal componente de SIEM, AlienVault ofrece un análisis basado en reglas que implementa su propio método para calcular el riesgo que representa un evento para algún activo en la red, el personal de seguridad puede definir sus intereses particulares, por ejemplo, disminuir el nivel de riesgo para un equipo con malware en la red wifi, pero desatar una alerta máxima con envío de notificaciones al detectar comunicaciones no permitidas en el segmento de red de servidores.

Para complementar su manejador de riesgos utiliza OpenVAS como componente para el escaneo y análisis de vulnerabilidades.

Para la detección de intrusiones AlienVault implementa tanto HIDS como NIDS. Para la detección de intrusiones a nivel de red integra Suricata con un set de reglas actualizadas por Emerging Threats gratuitamente y en su versión comercial ofrece soporte integrado con la versión Pro. Además de soportar la carga de algunas reglas de Snort como las provistas por Talos (VRT). A nivel de HIDS usa OSSEC, el cual se encarga de la recolección y gestión de los registros, detección de *Rootkits*, monitorea la integridad de archivos y el registro de Windows, y permite respuesta activa ante

[1] Durante todo el documento se hace referencia a este documento como HP Archsight

incidentes que puede lanzar aplicaciones en el servidor en caso de detectar cierto nivel de alerta.

La interfaz web de configuración y administración centralizada de todos los componentes de AlienVault, combina todos estos elementos con un manejo de Tickets para ayudar al personal de seguridad a dar respuesta a las alarmas registradas, esto provee una solución unificada.

Existen 2 versiones de AlienVault, OSSIM (*open source security information management*), y USM (*unified security management*).

AlienVault USM

AlienVault Unified Security Management (USM) es una plataforma todo-en-uno con un precio accesible, orientada al mercado de la mediana empresa para asegurar que estas organizaciones puedan defenderse eficazmente contra las amenazas avanzadas de la actualidad. Su modelo de licencia basado en dispositivos le permite adecuarse a un presupuesto más fácilmente que el modelo basado en volumen de datos.

AlienVault USM provee de:

- Monitoreo coordinado y unificado de la seguridad.
- Manejo de eventos de seguridad y generación de reportes.
- Inteligencia de amenaza continua.
- Un despliegue rápido.
- Múltiples consolas para diferentes funciones de seguridad.

Las 5 funcionalidades clave que ofrece AlienVault son:

- Descubrimiento de activos.
    - Escaneo activo y pasivo de la red.
    - Inventario de hardware y software.
- Monitoreo de actividades.
    - Análisis de flujos de red (Netflow).
    - Monitoreo de disponibilidad (Nagios).
    - Captura de paquetes completos.
- Evaluación de vulnerabilidades.
    - Pruebas de vulnerabilidades en la red (OpenVAS).
    - Continuo monitoreo de la red.
- Manejo de eventos y la información de seguridad
    - Manejo de logs.
    - Correlación de eventos.
    - Asistencia en la respuesta a incidentes.
- Detección de intrusiones
    - NIDS y HIDS (Suricata y OSSEC).
    - Monitoreo de integridad de archivos (OSSEC).

(AlienVault, AlienVault Unified Security Management™: Better Threat Detection for Effective Response, 2016)

Como un complemento a la inteligencia de la seguridad, AlienVault provee del intercambio abierto de amenazas OTX de AlienVault. La comunidad de intercambio abierto de amenazas de AlienVault permite compartir la información sobre la reputación de direcciones IP o URLS, y otros indicadores de compromiso como firmas de detección de amenazas en el tráfico de red.

Para sus versiones comerciales, los laboratorios de AlienVault proveen de un canal integrado de información sobre amenazas que incluye actualizaciones para el contenido de reglas, firmas, vulnerabilidades, correlación de eventos, informes y respuesta a incidentes.

AlienVault está disponible como un *appliance* físico, como software y en imágenes virtuales, también ofrece una solución para aplicaciones en la nube vía Amazon Elastic Compute Cloud EC2, con soporte exclusivo para AWS.

AlienVault OSSIM

AlienVault también ofrece una solución gratuita en versión open source con un conjunto de funcionalidades limitadas, la más importante la falta de la funcionalidad para recolección y gestión centralizada de logs. AlienVault implementa las mismas funcionalidades que USM, a diferencia de que USM implementa un conjunto de características mejoradas, como recolección, gestión y administración consolidada de los logs, e informes mejorados.

La Arquitectura de AlienVault está distribuida por 3 componentes principales

- Sensor
    - Se distribuyen a través de la red para recolectar registros y proveer descubrimiento de activos, escaneo de vulnerabilidades, detección de intrusiones, y monitoreo de operaciones.
- Logger
    - Almacena todos los logs que se detectan o reciben por parte de los sensores y de los agentes en su formato nativo.
- Servidor

- Sirve para configurar, administrar y controlar las capacidades de seguridad provistas por la solución. Unifica todos los componentes y provee las consolas de monitoreo y generación de informes.

Estos componentes pueden ser implementados en un sistema combinado (arquitectura todo en uno), o bien desplegados de forma distribuida en niveles horizontales y verticales para escalar a las necesidades del cliente.

También existe AlienVault USM para AWS, la cual es una implementación nativamente construida para proveerle servicios de SIEM a un entorno EC2, de la misma forma que sus ediciones locales, ofrece descubrimiento de activos, infraestructura AWS y evaluación de vulnerabilidades, y capacidades de monitoreo de Amazon CloudTrail, entro otros.

El mercado objetivo del fabricante está conformado por medianas empresas con conjuntos de equipos relativamente pequeños y programas de seguridad que necesitan integrar múltiples capacidades de seguridad a un costo relativamente bajo, y para organizaciones que aceptan un producto con soporte comercial basado en licencias de código abierto (Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2015).

Requisitos para la implementación:
Las ilustraciones que se presentan a continuación listan el Hardware recomendado para instancias de AlienVaultOS:

CPU	Intel® Xeon E5620
RAM	DDR3 1333 MHz
Disco	SAS 10000 RPM (204 MB/s)

Desempeño de la memoria (MEMCPY)	3310.32 MiB/s
Desempeño del disco (lectura/escritura aleatoria)	15.97 Mb/s

Ilustración 2 – Hardware Recomendado AlienVault 5.2 (AlienVault, Solutions for Every Eviroment!, 2016)

Recomendaciones para máquinas virtuales:

	USM Todo-en-Uno		Sensor remoto		USM Estándar		
	1TB	500GB	1TB	250GB	Server	Logger	Sensor
Núcleos Virtuales	81		4		8		
RAM (GB)	16		8		24		
Almacenamiento (TB)	1.0	0.5	1.0	0.25	1.2	1.8	1.2
Entorno de Virtualización	VMware ESXi 4.x, 5.x, and 6.x						

Ilustración 3 – Recomendaciones para máquinas virtuales AlienVault 5.2 (AlienVault, Solutions for Every Eviroment!, 2016)

Fortalezas detectadas a través de los años:

Las capacidades de seguridad integradas por AlienVault USM abarcan gran parte de los requerimientos para el cumplimiento de normativas: SIEM, monitor de integridad de archivos, evaluación y manejo de vulnerabilidades, descubrimiento de activos, y sistemas de detección de intrusiones tanto basados en red como para hosts, recuperación, análisis y almacenamiento de registros.

AlienVault ofrece un modelo de licencia simplificado basado en la cantidad de dispositivos desplegados, en vez de la cantidad de eventos por segundo. Las referencias de los clientes indican que las ofertas por parte del software y las implementaciones son mucho menos costosas que los productos correspondientes ofertados por la mayoría de los competidores en el mercado de SIEM.

El promedio de los referentes en cuanto a la satisfacción de los usuarios para las reglas de correlación predefinidas, informes, y la capacidad de crear reglas de correlación personalizadas, es mayor que el promedio de las puntuaciones para todas las otras referencias de los clientes en estas áreas.

Precauciones detectadas a través de los años:

El soporte para OSSIM generalmente proviene de terceros (foros), es limitado y gran parte del soporte durante del despliegue se refiere a la documentación de las herramientas en las que está basado. Frecuentemente puede requerir scripting a medida para las necesidades de la organización. Esto no debería representar un reto para el personal adecuado, sin embargo, contratar este personal incrementa los costos operativos de la solución. Las capacidades integradas, en muchos casos son de código abierto y éstas no son lo mejor del mercado.

La integración por defecto para la administración de identidad es de acceso limitado (LDAP y Active Directory) (Gartner, Magic Quadrant for Security Information and Event Management, 2016).

La integración de las aplicaciones está dada principalmente para aplicaciones de código abierto. Para aplicaciones de código cerrado se implementan algunos plugins de traducción para los fabricantes más reconocidos, aunque dependiendo del dispositivo o aplicación a integrar, es probable que se requiera hacer el traductor a medida.

Las capacidades del entorno de administración ofrecen un entorno básico para planificar la toma de acciones ante posibles alarmas, pero este marco de gestión de trabajo no incluye integración con frameworks externos como gestores empresariales de ticketing para asignar otros flujos de trabajo.
(Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2015)

HP ArcSight ESM/Express

HP ArcSight ESM es una aplicación de gestión de seguridad integrada que combina la correlación y análisis de eventos de seguridad enfocada en identificar y priorizar las amenazas en tiempo real para que se pueda responder y remediar rápidamente.

La solución SIEM de HP ArcSight incluye un software administrador de seguridad empresarial (ESM Enterprise Security Manager) para implementaciones de SEM (Security event management) a gran escala, y ArcSight Express, una oferta de aplicación basada en hardware y/o software para proveer funciones de recolección y administración de registros que puede ser implementada por sí sola, o bien en combinación con ESM.

ArcSight soporta la carga de módulos que permiten orientar la usabilidad de algunas áreas del sistema a cumplir propósitos específicos. HP provee de algunos módulos adicionales, como Application View, que proporciona visibilidad de las aplicaciones en tiempo de ejecución basado en la tecnología de HP Fortify, y HP User Behavior Analytics, que proporciona un análisis integrado del comportamiento del usuario basado en una tecnología producida en asociación tecnológica con Securonix.

La licencia de ArcSight está basada principalmente en el consumo de GB por día, por lo que su implementación no es de fácil acceso para organizaciones pequeñas.

ArcSight Express debe ser considerado para implementaciones de SIEM de tamaño medio. ESM es más apropiado para implementaciones a gran escala mientras existan suficientes recursos para su implementación, y para organizaciones que buscan construir un SOC dedicado.

ArcSight Express

ArcSight Express es una solución SIEM Todo-en-Uno que ofrece una herramienta fácil de desplegar con funcionalidades como detección de amenazas, respuesta a incidentes, y generación de reportes para cumplimientos. Está disponible en modelo de software y/o hardware dedicado.

Los appliances comerciales de ArcSight Express tienen la posibilidad de analizar hasta 2,500 eventos por segundo, y su licencia al igual que ESM está basada en eventos por segundo, tiene como mínimo 250 eventos por segundo, y escala en múltiplos de 50 para ofrecer una flexibilidad competente en el licenciamiento para empresas medianas (Hewlett Packard Enterprise, HPE Security ArcSight ESM Express All-in-one SIEM appliance, 2016).

En la siguiente tabla se muestra el hardware ofrecido por el fabricante de los appliances de ArcSight Express:

Modelo	EE7600-250	EE7600-1000	EE7600-2500
Capacidad de eventos	250 EPS	1,000 EPS	2,500 EPS
Capacidad de complementos	50 EPS	50 EPS	
Familia del dispositivo	HPE DL380 Gen9 ZE5-2680v3 Kit		
Procesador	2 x Intel Xeon E5-2680v3, 2.5GHz, 12-core		
Dimensions (H x A x L)	8.73 x 44.55 x 73.02 cm		
Memoria	6 x 32 GB, 2133 MHz RAM		
Tamaño de Disco	8 x 600 GB (2.4 TB RAID 10 con capacidad de almacenamiento de hasta 1.2 TB de logs comprimidos)		
Sistema Operativo	Red Hat Enterprise Linux 7.1 64-bit		
Administración	Navegador Web, CLI, Web Services API		
Interfaces Ethernet	4 x 10/100/1000		
Chassis	2U Rack		
Alimentación	2 x 800W CS Platinum Power Supply		

Ilustración 4 –Appliances de HP ArcSight Express (HP Enterprise, 2016)

ArcSight ESM

ArcSight ESM es una poderosa y completa herramienta de gestión y correlación de eventos de seguridad para los centros de operación. Es parte de la solución de HP ArcSight, diseñada como una plataforma escalable de detección e identificación de amenazas, con una arquitectura flexible que permite a las organizaciones escalar sus soluciones de SIEM existentes conforme crece su infraestructura de red.

El múltiple nivel de la arquitectura de la solución implementa una serie de monitores de datos, filtros, reglas, interfaces de análisis y administración, y reportes de los datos obtenidos.

ArcSight ESM ofrece:

- Monitoreo de sistemas e infraestructura de red en tiempo real para detectar posibles amenazas a la seguridad.
- Identificar verdaderas amenazas en minutos para tomar acciones antes de que sean comprometidos recursos críticos.
- Entender información contextual acerca de los eventos para tomar decisiones informadas.
- Mejorar la eficiencia de las actividades en el manejo de incidentes.
- Automatizar y coordinar reportes para el cumplimiento de normativas.

En 2014 HP Añadió diversas mejoras, como alta disponibilidad para ArcSightESM, actualización de su interfaz web para ArcSight logger, y mejoras al centro de administración como monitoreo del estado de sistemas, y características específicas para la administración de sistemas distribuidos y en 2016 promete una actualización de las interfaces de administración para mejorar la experiencia del usuario, además de ofrecer consultas un 48% más rápidas que su versión predecesora, y más

poderosas con capacidades de capturar logs en bruto a un ritmo de 400,000 eventos por segundo, con capacidad de almacenamiento de hasta 480 Tb de datos comprimidos (Hewlett Packard Enterprise, HPE ArcSight SIEM solution, 2016).

Requerimientos del sistema:

Recomendaciones del sistema	Pequeño	Mediano	Grande
Procesadores	8 cores	16 cores	32 cores
Memoria	36 GB RAM	64 GB RAM	128 GB RAM
Almacenamiento	250 GB disk space RAID 10 15,000 RPM	1.5 TB disk space RAID 10 15,000 RPM	<= 8TB RAID 10 15,000 RPM

Ilustración 5 – Requisitos recomendados para ArcSight ESM (Hewlett Packard Enterprise, HPE Arcsight Enterprise Security Manager, 2016)

Fortalezas

ArcSight ESM provee una colección extensa de herramientas de SIEM que pueden ser usadas por el personal del SOC para ofrecer una amplia cobertura de su plan de seguridad.

Incluye una completa interfaz de administración para investigación y respuesta a incidentes, mejorados por los plugins disponibles en el Marketplace que adaptan la solución a necesidades más específicas de la organización.

HP ArcSight User Behavior Analytics provee de un set completo de herramientas con capacidad para analizar el comportamiento de los usuarios y estadísticas de comportamiento completamente integrados con el SIEM (Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2015).

Precauciones

La principal desventaja de implementar ArcSight en cualquiera de sus modalidades es el precio. Puede llegar a ser una solución cara y fuera del presupuesto para muchas organizaciones.

Una implementación completa de HP ArcSight ESM incluye herramientas y servicios profesionales más complejos que la competencia, esto puede ser contraproducente, pues se requiere de un profesional capacitado y a menudo certificado, para una completa usabilidad de estas.

La retroalimentación de los usuarios indica que la interfaz de usuario para la consola central de ArcSight ESM es anticuada, y ante estas retroalimentaciones, HP planea liberar una actualización de la interfaz web en el año 2016 (Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2015) (Hewlett Packard Enterprise, HPE ArcSight SIEM solution, 2016).

Además, los usuarios de ArcSight ESM califican como un problema la atención al cliente y la puntuación que ellos ofrecen a la satisfacción con el producto, efectividad de las reglas de correlación predefinidas, la personalización de las herramientas, la creación y modificación de reportes, calidad y estabilidad de producto está calificada con puntuaciones inferiores que el promedio de otras herramientas SIEM analizadas por Gartner (Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2015).

Splunk

Splunk Enterprise es una utilidad de análisis de datos que integra un set de herramientas para facilitar la recolección, análisis y respuesta sobre los datos generados en el big data de una organización.

El software de Splunk promete ofrecer una forma fácil, rápida y segura de almacenar, analizar y visualizar cantidades masivas de información generada por los sistemas de TI y la infraestructura tecnología de la organización. Ya sea físicamente o en la nube. Splunk ofrece un nivel extra de visibilidad y percepción de la inteligencia de la información en una empresa. (Splunk, Splunk Enterprise and Splunk Cloud, 2016)

En muchos casos, la presencia de Splunk para el soporte de operaciones lleva considerar la implementación de la herramienta para SIEM.

Splunk provee de búsquedas, alertas, y correlación en tiempo real, además de un leguaje de consulta que soporta visualización usando más de 140 comandos estadísticos. El lenguaje de búsquedas de Splunk, *Search Processing Language* (SPL) es un poderoso lenguaje de consulta que permite interactuar con los datos recopilados con base en 5 tipos diferentes de correlaciones: Tiempo, Transacciones, Búsquedas, Sub-búsquedas (Drill-Down), y Conjunciones.

Estas correlaciones permiten generar un seguimiento de las transacciones, por ejemplo, el envío de un email, la generación de una orden, o una llamada de voz IP generarán diferentes tipos de eventos a través de los sistemas en la red, Splunk permite buscar estas colecciones de eventos que son parte de la misma transacción identificando problemas u oportunidades en estas transacciones. Además, integra

aprendizaje de máquina con más de 15 analizadores de patrones que ayudan predecir y detectar anomalías que indiquen algún riesgo para la organización.

Uno de los componentes más poderosos de Splunk es su análisis estadístico de la información recopilada. Permite crear interfaces personalizadas de visualización de la información para diversos propósitos, técnicos y no técnicos como identificar problemas, oportunidades, y posibles riesgos. Tiene una amplia variedad de gráficos y visualizaciones que hacen de los resultados de las búsquedas información entendible para tomar acciones. Es especialmente útil para extraer información de valor de grandes volúmenes de datos complejos a través de sus interfaces de despliegue de la información, ya sea para fines administrativos, de negocios, desarrolladores, de auditoria o de análisis de seguridad (Splunk, Splunk Enterprise and Splunk Cloud, 2016).

Splunk es ampliamente desarrollado por operaciones de TI y equipos de soporte para el manejo de logs, análisis, monitoreo, y búsquedas avanzadas y correlación de eventos.

La aplicación de Splunk para seguridad empresarial provee de reportes predeterminados, interfaces, búsquedas, visualizaciones, y monitoreo en tiempo real para implementar un monitoreo de la seguridad y reportes de casos de uso en el cumplimiento de normativas y regulaciones.

Splunk continúa mejorando la aplicación de seguridad empresarial, sus indicadores de seguridad, sus interfaces y visualizaciones, así como mejora el soporte para capturar datos desde interfaces de red y el posterior análisis. De igual forma mejora sus búsquedas avanzadas y el pivoteo de datos mediante el uso del lenguaje de

consulta SLP. Splunk puede ser desplegado como un servicio, en una nube privada o pública, o también en la nube de Splunk, o en una combinación de las anteriores.

Las instituciones que deberían considerar Splunk como una solución SIEM para su entorno son aquellas que requieren una plataforma de SIEM que pueda ser personalizada para soportar un análisis extensivo de una gran variedad de formatos de logs, así como las que posean un uso extenso de su infraestructura de TI.

Fortalezas

La fuerte presencia de Splunk en las operaciones de los grupos de TI puede proveer a las organizaciones con información de primera mano que les resultara muy útil en su manejo de registros, y una amplia capacidad de análisis de estos. Además, ofrece un despliegue de pre-SIEM para recursos críticos y operaciones en el SOC para despliegues enfocados en la seguridad.

Los clientes de Splunk se refieren a la visualización y comportamiento, análisis predictivo y estadístico como elementos avanzados y efectivos en los casos de uso de monitoreo, como lo son la detección de acceso anómalo a datos sensibles.
Splunk tiene soporte incorporado para un gran número de fuentes de datos de inteligencia sobre amenazas, tanto privativas como de código abierto.

Según Gartner, la calificación promedio otorgada por los clientes de Splunk en lo referente a escalabilidad, desempeño, efectividad y usabilidad de las reglas predefinidas, creación de reportes, facilidad y efectividad de las consultas a medida, estabilidad y calidad del producto, y experiencia de soporte técnico al usuario, es más alta que el promedio de las puntuaciones de referencia para todos los demás

competidores en estas áreas (Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2015).

Precauciones

La aplicación de Splunk para seguridad empresarial provee un soporte básico para correlaciones definidas para el monitoreo de usuarios. Los compradores potenciales de esta solución deben anticiparse al hecho que deberán modificar estas reglas predefinidas para construir las propias que se adapten de acuerdo a las necesidades de su implementación de monitoreo de usuarios.

El flujo de trabajo y manejo de casos parecen estar un poco rezagadas a comparación las herramientas ofrecidas por la competencia. Organizaciones que implementen procesos de SOC más complejos pueden requerir personalización o la integración de tecnologías de terceros para cubrir las funciones más avanzadas del manejo de casos e incidentes.

El modelo de licencia de Splunk está basado en el volumen de datos indexado por día. Algunos clientes reportan que la solución podría resultar más costosa que otros productos de SIEM en entornos dónde se esperan recibir altos volúmenes de información (Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2015).

CAPÍTULO 3 - DESARROLLO DEL PROYECTO

Para evaluar las soluciones SIEM seleccionadas, se implementó un laboratorio virtual de pruebas, dónde se instalaron máquinas virtuales ejecutando diversos sistemas operativos. El objetivo de este ejercicio consiste en probar la integración entre los elementos de los SIEM con los activos disponibles en una típica arquitectura de red.

Hardware utilizado:

- Workstation
    - Intel Core i5 6500 @ 3.3 GHz
    - 32 GB RAM
    - 512 Gb SSD
    - 2.0 Tb HDD
- Firewall Fortinet 60C Firmware 5.4.2

Software utilizado:

- VMware Workstation 12.0

Sistemas operativos:

- Debian GNU/Linux 6.0, 7.0, 8.X
- CentOS GNU/ Linux 6.7, 7.0
- Ubuntu 14.10, 15.04 LTS
- Red Hat Enterprise Linux 6.5
- Windows 7
- Windows 10

Software de SIEM:

- AlienVault OSSIM 5.2
- HP ArcSight 6.5c

- Splunk 6.4

Con objetivo de simular el proceso de integración de las tecnologías SIEM en entornos reales, se simuló el despliegue de los respectivos servicios recolectores de datos para los sistemas operativos comúnmente encontrados en los centros de datos. Los sistemas operativos usados como activos generadores de eventos durante la instalación fueron seleccionados pensando en cubrir las posibles diversidades de los entornos reales, por esto los sistemas usados fueron basados en las grandes familias de los sistemas operativos actuales, Windows, .deb, y .rpm. (Windows 7, Debian 8 y CentOS 7).

2.1.8 AlienVault OSSIM 5.2

Para el laboratorio de AlienVault en su versión open source se creó una máquina virtual con las siguientes características:

- 2 Núcleos de procesamiento
- 8GB de RAM
- 180Gb de Disco Duro para el sistema operativo
- 2 Interfaces de red
- Sistema Operativo AlienVaultOS

En lo referente a la recolección de información, esta máquina hace uso de módulos de detección de intrusiones desde 2 fuentes disponibles, HIDS y NIDS. El HIDS implementado es OSSEC HIDS, el cual está disponible para muchas plataformas incluidas Windows y Linux.

Para probar el agente OSSEC se instalaron tres máquinas virtuales generadoras de eventos, con sistemas operativos: Windows 7, CentOS 7, y Debian 8. El agente de OSSEC instalado recopila información desde diversas fuentes en el sistema operativo incluyendo los registros y bitácoras disponibles y envía los datos recopilados al servidor AlienVault OSSIM donde se procesa y se analiza el tráfico en base a reglas de detección de amenazas.

Para el NIDS se configuró la instalación de Suricata que se incluye en AlienVault, para adecuarse a un conjunto de reglas extendido donde se añadieron las fuentes de inteligencia de SourceFire VRT. Este NIDS recolectó eventos a través de una de las interfaces de red la cual estaba conectada a un “tap” pasivo de red que duplicaba todo tráfico generado por las máquinas de activos para ser analizado por el SIEM.

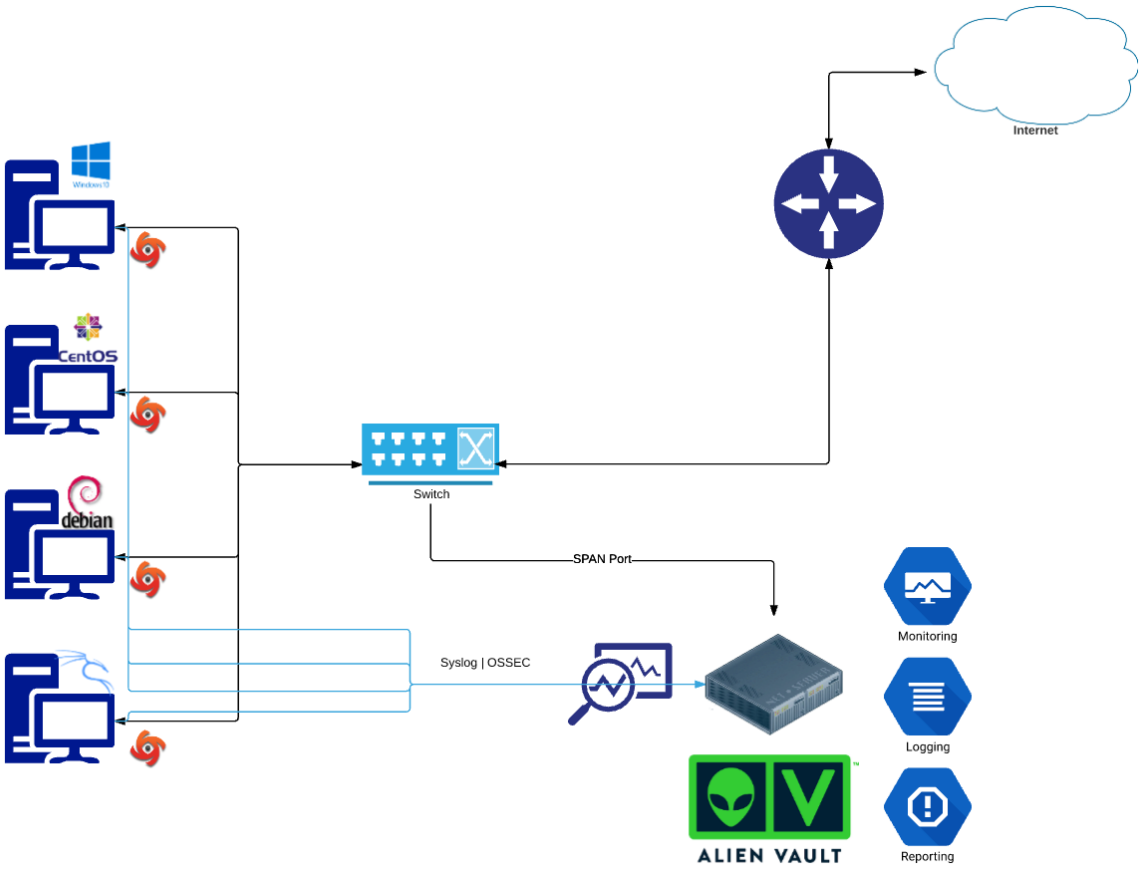

Ilustración 6 – Arquitectura de red del laboratorio de AlienVault

Para probar la generación de eventos se realizó una serie de actividades que tenían como objetivo detonar eventos de seguridad. Simulaciones de ataques de red e infecciones de malware obteniendo un desempeño satisfactorio.

Si la taxonomía de algún paquete de red o un registro coincide con las reglas de detección, se genera un evento. En base al valor del activo y la gravedad del evento se calcula un indicador de riesgo sobre el cual se genera una alerta. De esta forma, y configurado correctamente, el equipo de seguridad se asegura de sólo recibir alertas bajo las circunstancias que se desean.

Si fuera necesario el almacenamiento a largo plazo de los registros y los eventos se debe considerar la implementación de la versión USM de AlienVault.

Usando la arquitectura recomendada por AlienVault basada en módulos de sensores y una agregación final en el servidor de AlienVault, se obtiene una implementación satisfactoria de SIEM cubriendo una gran parte de las necesidades más comunes de un SIEM en un despliegue relativamente eficaz y de duración reducida. Además de que, al ser de código abierto, hace uso de tecnologías con licencia libre que ya son conocidas y extensamente documentadas en las comunidades de software libre.

2.1.9 HP ArcSight 6.5c

En la implementación de ArcSight ESM en su versión 6.2 se encontraron diversas problemáticas. Una de las principales limitantes fue el acceso a una licencia de instalación que fue obtenida únicamente bajo el apoyo de un partner. También fue un reto cubrir los requerimientos mínimos del servidor destinado para ArcSight ESM, que no puede ser instalado sin una cierta cantidad de requerimientos mínimos, e inclusive forzando la instalación, el proceso falla si la memoria y el almacenamiento no son los adecuados para la solución.

Para la prueba en laboratorio virtual de ArcSight se implementó una máquina virtual con las siguientes características:

- 4 Núcleos de procesamiento
- 16GB de RAM
- 80Gb de Disco Duro para el sistema de archivos del sistema operativo
- 80Gb de Disco Duro para la Aplicación de ArcSight
- 240Gb de Disco Duro con sistema de archivos XFS para el almacenamiento de logs
- 2 Interfaces de red
- Sistema Operativo Red Hat Enterprise Linux 6.2

Durante el proceso de instalación y durante la configuración el servidor, es necesario apegarse a la documentación de la versión adecuada de ESM, de omitir una serie de pasos puntuales, la instalación o la configuración pueden fallar.

Tras realizar una instalación exitosa del servidor es necesario configurar los sensores y los agentes de ArcSight en los activos a monitorear. Estos agentes, llamados

conectores, están disponibles en 2 formas, Connectors pre compilados listos para instalar en una gran cantidad de dispositivos comerciales, y FlexConnectors que son módulos creados para adaptarse a las necesidades específicas de lo que se desea monitorear, como lectores de archivos planos o basados en expresiones regulares, módulos de recolección de protocolos como SNMP o syslog,

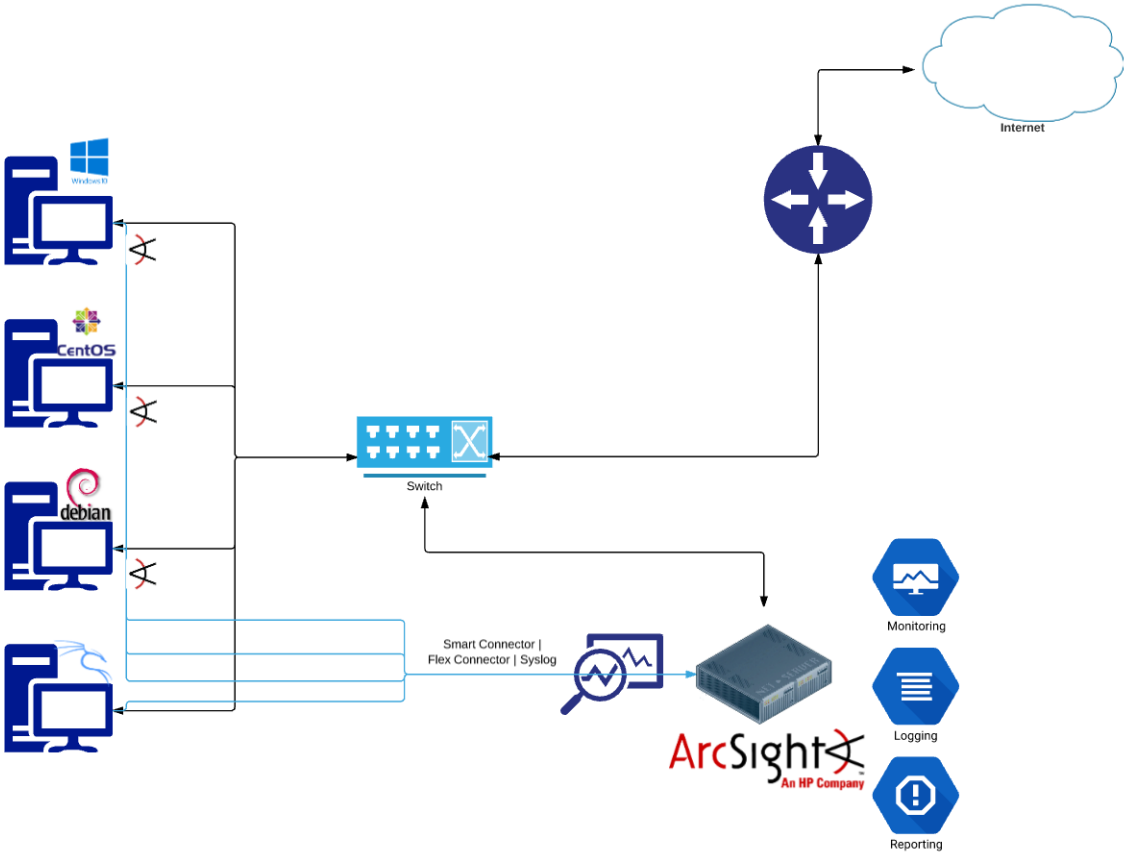

Ilustración 7 – Arquitectura de red del laboratorio de ArcSight

Una vez que se colocan los dispositivos encargados del monitoreo de la red, la solución de ArcSight hace muy eficiente la recolección y el manejo de eventos de seguridad y ofrece consolas de monitoreo y visualización apropiadas para la adecuada respuesta ante cualquier tipo de incidente en los recursos de red.

También cabe mencionar que, aunque no se pudo realizar el ejercicio, el despliegue de aplicaciones masivas de ArcSight es bastante simple, pues consiste únicamente de ligar los Servidores SIEM de ESM a una consola centralizada de correlación de eventos que se encargara de la gestión de eventos para todo el entorno distribuido.

2.1.10 Splunk 6.4

En la instalación de Splunk Enterprise se utilizó una máquina virtual con las siguientes características:

- 2Gb de RAM
- 180Gb de Disco Duro
- Sistema Operativo CentOS 7

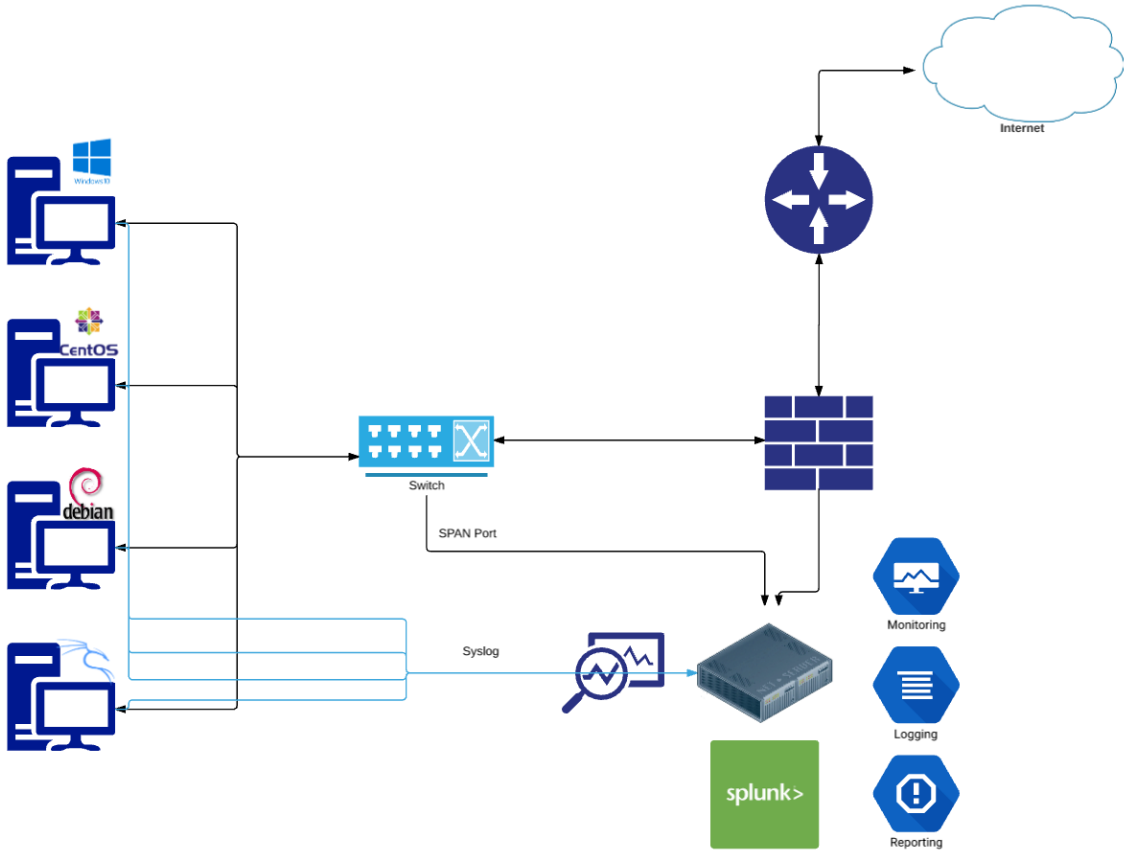

Ilustración 8 – Arquitectura de red del laboratorio de Splunk

La instalación de Splunk a partir de los paquetes pre-compilados es bastante simple, basta con descargar los binarios y seguir las instrucciones durante la instalación para

obtener una consola de Splunk completamente funcional. Con mínimas modificaciones al sistema operativo como agregar reglas permisivas al firewall integrado es suficiente para ponerla en operación.

Para la recolección de logs y eventos de seguridad se configuró un firewall Fortinet quien se ha encargado del reenvió de logs al servidor de Splunk mediante el protocolo de syslog.

Para facilitar el análisis de la información, Splunk integra una aplicación de análisis especialmente diseñada para interactuar con el sistema de registros de Fortinet. Para la instalación de la aplicación únicamente fue necesario contar con una cuenta de Splunk y con solo unos cuantos clicks se instaló la aplicación de análisis para Fortinet. Esto permitió que en cuestión de minutos se tuviera un despliegue funcional para el análisis estadístico de los eventos de seguridad registrados.

Una vez que se importaron datos de otras fuentes como Snort, se analizaron los datos en las múltiples consolas de visualización, verificando el enorme potencial de las herramientas que Splunk ofrece de forma nativa, y el potencial de desarrollar aplicaciones a medida para cubrir los requisitos de análisis de una organización.

Splunk provee de un analizador sintáctico de los registros que implementa una enorme cantidad de beneficios para los analistas de datos. Uno de los rasgos más importantes a destacar, además de la gran potencia intrínseca de su motor de gestión de registros, es la rapidez con la que Splunk puede manipular y hacer búsquedas en grandes volúmenes de información. Esta rapidez está dada en medida del hardware empleado durante la instalación del servidor de Splunk, pero inclusive en entornos pequeños como el que se instaló en el laboratorio de pruebas, fue evidente que las

bondades de su motor de búsqueda y correlación son un factor a destacar para el trabajo diario con herramientas de análisis.

Otro factor crucial a destacar durante el trabajo desarrollado con Splunk, tiene que ver con las interfaces de visualización de los datos. A partir de reglas predefinidas de correlación y aplicaciones de visualización se puede obtener potentes interfaces para el análisis estadístico de los datos registrados, y si se combina con reglas hechas a medida de lo que requiere investigar, Splunk se posiciona como la herramienta preferida a utilizar para el análisis intensivo de grandes cantidades de información.

CAPÍTULO 4 - RESULTADOS

Con base en la investigación realizada durante la elaboración del marco teórico se pudieron identificar las características más importantes que deben implementar las soluciones SIEM disponibles en el mercado, siendo estas las descritas a continuación:

- Capacidad de análisis de la diversidad de logs disponibles en el entorno y su Capacidad de integración para las fuentes que no son soportadas nativamente
- Motor de detección de amenazas en base a los eventos registrados y la correlación de los grupos de eventos de diferentes fuentes
- Herramientas y capacidades de análisis de la información, así como la gestión de registros a largo plazo, en especial durante el análisis forense.
- Capacidad de respuestas automáticas ante posibles incidentes.
- Soporte para el cumplimiento de normativas de seguridad.

A partir de la investigación realizada y respaldando los resultados obtenidos con análisis realizados por la empresa de consultoría Gartner sobre SIEM en los años de 2015 y 2016, se puede apreciar una clara diferencia en las funcionalidades provistas en las soluciones seleccionadas, esto permite enfocar la implementación de los productos al entorno para el cual están siendo implementadas.

En dichos análisis es posible comparar diversas fortalezas y precauciones a considerar en los productos. En los siguientes gráficos se puede apreciar la comparativa ofrecida por Gartner sobre la habilidad de ejecución, y la visión del mercado de los productos seleccionados:

Ilustración 9 – Análisis de Gartner de soluciones SIEM en 2015

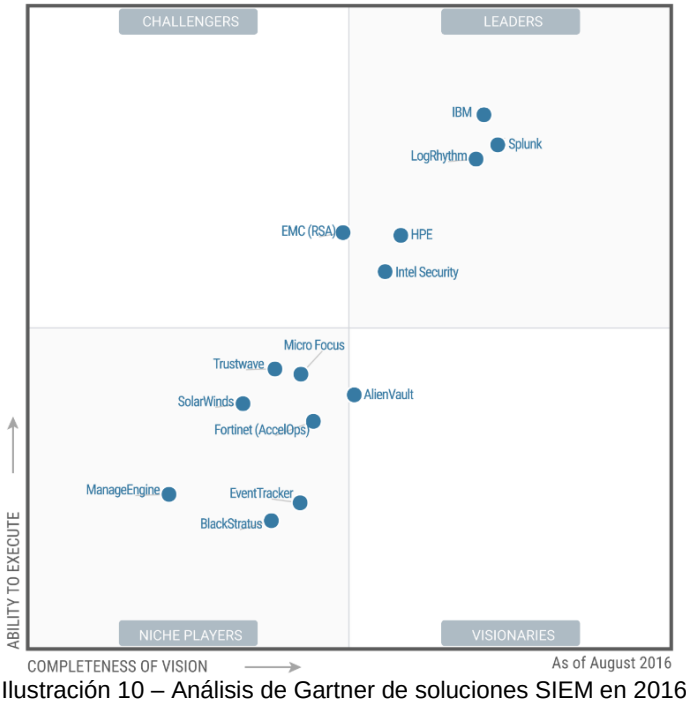

Ilustración 10 – Análisis de Gartner de soluciones SIEM en 2016

Como se puede apreciar en las anteriores imágenes, existe una amplia variedad de soluciones disponibles en el mercado, algunas de ellas se posicionan muy por encima de las soluciones estudiadas en este proyecto, y algunas otras con una amplia brecha de madurez que es necesario ceñir. No obstante, como se ha experimentado en la puesta en marcha de este proyecto, los profesionales de seguridad pueden tomar acciones que sirven para mitigar algunas de las deficiencias que pudieran presentar algunas de las soluciones.

A partir de la investigación realizada y tras la instalación y pruebas de las soluciones SIEM seleccionadas, se obtuvo un conocimiento amplio sobre el estado el arte de las soluciones SIEM en el mercado. Además, fue posible identificar fortalezas y precauciones de estas soluciones específicas durante el despliegue y operación de las mismas.

Cabe recalcar, que ni la solución líder en el mercado será efectiva sin una adecuada planificación e implementación. De la misma forma, soluciones no tan maduras o en un estado emergente, podrían solventar perfectamente las necesidades de su entorno si son desplegadas correctamente. El enfoque modular que ha sido propuesto ayuda en gran medida a complementar las deficiencias y respaldar las fortalezas de esta gama de dispositivos de seguridad.

A continuación, se expone un breve resumen de las principales características identificadas dichas soluciones.

2.1.11 AlienVault

Es una solución que integra una gran cantidad de características avanzadas para la detección de amenazas. Es muy eficiente durante el despliegue, e incluso integra sus propios analizadores sintácticos de logs. Es de fácil acceso y configuración para tenerla funcionando en un tiempo relativamente corto. Su modelo de licenciamiento permite ser instalado en pequeñas y medianas empresas a un costo bajo con posibilidad de crecer o adquirir el licenciamiento comercial sin complicaciones. Inclusive pagando el costo de las licencias sigue siendo una de las mejores opciones para satisfacer cumplimientos como PCI DSS.

Integra gran parte de los requerimientos para el cumplimiento de normativas: SIEM, monitor de integridad de archivos, evaluación y manejo de vulnerabilidades, descubrimiento de activos, y sistemas de detección de intrusiones tanto basados en red como para hosts, recuperación, análisis y almacenamiento de registros.

Su modelo de licenciamiento simplificado permite que esté disponible gratuitamente en su versión de código abierto o comercial con un modelo de licencias basado en la cantidad de dispositivos monitoreados.

Algunas precauciones al considerar las soluciones SIEM de AlienVault son:

El soporte para OSSIM generalmente proviene de terceros (foros), es limitado y gran parte del soporte durante del despliegue se refiere a la documentación de las herramientas en las que está basado.

En entornos con tecnologías que no son ampliamente reconocidas, requiere scripting a medida para las necesidades de la organización.

2.1.12 ArcSight

ArcSight es una solución bastante robusta. Se posiciona como una de las soluciones líderes en el mercado gracias a su nivel de madures y comprensión del manejo de eventos de la seguridad informática. Integra una enorme cantidad de componentes de análisis y correlación de eventos, al mismo tiempo que facilita la integración del despliegue de SIEM a través una enorme cantidad de plugins en los paquetes propietarios de ArcSight, por ejemplo, SOX o PCI, al mismo tiempo que ofrece la posibilidad de que un usuario genere sus propios paquetes de gestión y los exporte e importe en otros sistemas, además de que permite distribuirlos sencillamente a través de sus múltiples interfaces de gestión.

El enorme poderío de ArcSight justifica el coste que pudiera generar su despliegue. Es por esto que esta solución se enfoca a empresas que ya tiene un plan de gestión de su ciberseguridad y buscan escalarlo a nuevos niveles de correlación de eventos.

Sus principales fortalezas residen en su enorme capacidad de detección y de gestión masiva de eventos de seguridad, además de la automatización de ciertos procesos y respuesta ante invidentes identificados.

Las principales precauciones a considerar ArcSight como una plataforma de SIEM tiene que ver con el costo de la solución; no es barata, y de la misma forma que es muy compleja en sus posibilidades de configuración, requiere de una capacitación adecuada por parte del personal que la va a operar para ser aprovechada correctamente.

2.1.13 Splunk

La recolección y análisis de datos son las principales características de Splunk. Sus múltiples interfaces y herramientas de búsqueda destacan de sus competidores debido a que poseen una capacidad superior de investigación y manipulación de los datos indexados que pueden ser utilizados inmediatamente después de desplegar la solución “fuera de la caja”. Además, implementa múltiples aplicaciones que permiten una visualización gráfica de los datos recopilados dónde es posible obtener una visibilidad de los principales tipos y flujos de datos, lo que habilita al personal del SOC o de un NOC para identificar los principales usos que se les da a los sistemas red, permitiendo identificar puntos de mejora o de riesgo en estos sistemas.

Otra característica destacable de Splunk son sus “Apps” disponibles en el marcado de aplicaciones que dan posibilidad de integración con múltiples tecnologías de una forma extraordinariamente simple, permitiendo que el personal se dedique a realizar investigaciones directamente sin perder tanto tiempo realizando scripting a medida para sus dispositivos. Inclusive cuando un dispositivo no es soportado, las funcionalidades y herramientas que ofrece Splunk permiten que la programación de rutinas de normalización sea muy simple y eficiente. Otra funcionalidad destacable integrada en Splunk tiene que ver con la implementación de soporte a cumplimiento de normativas reconocidas como PCI-DSS dónde basta con instalar una App para obtener un status del cumplimiento y señalización sobre qué áreas es necesario mejorar para estar en orden con las normativas.

2.1.14 Resultados generales

Además de los dispositivos y servicios conectados en una red, existe un gran número de tecnologías enfocadas a resguardar la seguridad de las tecnologías de la información, desde simples firewalls statefull, NGFW, IPS, IDS, honeypots, entre otros, todas estas tecnologías presentan funcionalidades que generan registros y bitácoras que pueden ser integrados en el análisis de registros para obtener información relevante de los eventos operativos de una organización.

En el aspecto relevante a la seguridad, el hecho de integrar estas tecnologías y sus registros con técnicas avanzadas de normalización y correlación de datos, resulta en una poderosa fuente de información que ofrece una completa visibilidad de las actividades en una red. Esto ofrece una fuente de información inigualable para los equipos de respuesta a incidentes o de análisis forense para poder investigar cuando se suscite algún incidente, incluso cuando la evidencia original ha sido destruida.

Además de los eventos de seguridad, estos registros pueden obtener una gran inteligencia operativa que puede ser extraída mediante el análisis estadístico o de big data. Por ejemplo, es previsible el momento en que un servicio está alcanzando un punto crítico dónde sus capacidades pueden ser insuficientes y se puede planificar con tiempo el escalado del sistema.

No obstante, el hecho de realizar una adecuada planificación, puede presentar un reto para los profesionales de la seguridad, esto se debe principalmente a que las organizaciones no tienen bien definido cuál es el objetivo por el cual se decide emprender el despliegue de un SIEM, y muchas veces, incluso cuando se tiene bien definido el objetivo, los medios con los cuales se requiere realizar la implementación

no son los adecuados o no estaban debidamente dimensionados para satisfacer las necesidades descritas.

Cualquiera sea el caso, el enfoque modular permite integrar todas estas tecnologías con un impacto disminuido en las responsabilidades del personal encargado de realizar la instalación y el mantenimiento de estos sistemas

Esto se debe a que el enfoque modular permite delegar tareas a personas responsables de cada área de la organización, y una vez que el sistema está debidamente diseñado, la puesta en marcha de los agentes y/o sistemas recolectores de registros se realiza de forma casi transparente para los usuarios y administradores de los sistemas finales. Únicamente quedando como tarea a realizar, el debido afinamiento y mejora de los sistemas de monitoreo y correlación de eventos. Resultando en una rápida y eficaz visibilidad de cualquier evento que ocurra en la organización, permitiendo dirigir la atención a los eventos más relevantes o que resultan de interés para la organización.

Con esto es posible que cualquier comportamiento extraño sea debidamente identificado tan pronto se suscita reduciendo el tiempo de detección y respuesta drásticamente, lo que resulta en una gran mitigación del impacto de cualquier posible brecha en la seguridad de una organización.

2.2 COSTOS OPERATIVOS

La implementación de tecnologías de seguridad puede representar una inversión considerablemente costosa, especialmente en empresas u organizaciones de capital reducido o dónde aún no existe una cultura de protección en el ámbito de la seguridad informática. Bajo estas circunstancias, obtener el presupuesto adecuado para la implementación de estas tecnologías puede representar un reto por sí mismo, en especial si se considera que los resultados de la implementación de un SIEM no podrán ser apreciados inmediatamente.

Toda implementación informática, especialmente aquellas destinadas a ofrecer entornos de seguridad avanzada, tienen un soto económico considerable que deber ser contemplado antes de realizar gestiones de implementación de las tecnologías.

2.2.1 COSTOS DE LAS SOLUCIONES

Se han investigado los costos del licenciamiento para cada una de las soluciones investigadas en este proyecto y se ha tomado en cuenta la labor humana en los procesos de despliegue y manutención de las herramientas. Debido que los fabricantes publican las cotizaciones de sus soluciones en dólares norteamericanos y a la inestabilidad económica mundial, en especial de la modela nacional (MXN), los precios expresados a continuación están expresados en dólares norteamericanos (USD).

AlienVault OSSIM/USM

AlienVault en sus dos presentaciones de licencia libre y licencia de paga, se recomienda para PYMES y empresas medianas que estén dispuestas a usar software libre. O bien compañías que les interesa comenzar a investigar incidentes de

seguridad, pero no desean invertir gran capital en el despliegue de soluciones comerciales.

Debido al tipo de licenciamiento que implementa AlienVault USM, basado en el número de activos a monitorear, empresas grandes con un gran número de activos, pueden ver un incremento significativo en el coste de operación de AlienVault USM, por ello de recomienda considerar usar una solución SIEM cuyo licenciamiento se base en el volumen del tráfico.

En caso de que una organización grande desee implementar AlienVault OSSIM como SIEM (bajo licencia libre), será necesario planificar un manejo de logs externo a esta solución. Esto puede ser contraproducente para el despliegue efectivo del SIEM y es una de las grandes desventajas del licenciamiento libre, en estos casos y cuando existan regulaciones referentes al almacenamiento externo o a largo plazo de los logs, se recomienda usar la versión USM, que ofrece de forma nativa un almacenamiento a largo plazo de los registros y manejo integrado de estos.

En entornos particularmente grandes, únicamente se recomienda usar este tipo de licenciamiento basado en el número de activos a monitorear, cuando la cantidad de tráfico supere en gran medida el número de activos dentro de la organización.

Licencia de código abierto:

- No requiere de expertos certificados en el despliegue de esta solución, sin embargo, si es necesario personal capacitado y con buen conocimiento de la red interna, que invertirá muchas horas en la instalación y despliegue del sistema, además de que para el mantenimiento y operación de la misma también será necesario invertir grandes cantidades de tiempo, en especial en

las primeras fases del despliegue mientras se ajustan los niveles de alertas y alarmas para el entorno destino.

Licenciamiento comercial (por volumen de activos):

- De la misma manera que para el licenciamiento libre, no requiere de personal especializado, pero si será necesario de personal capacitado y suficiente tiempo para el despliegue correcto del sistema, con la principal diferencia que posee soporte de AlienVault durante el proceso de despliegue será de gran ayuda para acelerar la instalación en entornos de tecnologías mixtas.

El licenciamiento de AlienVault se basa en el número de activos finales a monitorear. En la siguiente tabla se presenta los costes de licenciamiento de la solución "AlienVault USM" investigados al momento de la cotización de soluciones:

	Capacidad	Precio (USD)
USM Todo-en-Uno 25A	Monitor para 25 activos únicos	$5,050
USM Todo-en-Uno 75A	Monitor para 75 activos únicos	$9,750
USM Todo-en-Uno 150A	Monitor para 150 activos únicos	$13,250
USM Todo-en-Uno UA	Monitor para 150 activos únicos	$23,100
USM para AWS en la Nube	Ilimitada para entornos en AWS	$1/hora

Ilustración 11 – Licenciamiento para AlienVault 5.2 (AlienVault, Solutions for Every Eviroment!, 2016)

ArcSight Express/ESM

ArcSight es una de las soluciones líderes en el mercado ya que ofrece un enorme potencial de análisis y detección de amenazas, por este motivo, su costo de implementación no es barato, pero reditúa la inversión con inteligencia sobre amenazas que solo los líderes del mercado pueden ofrecer. Aunado a esto, el proceso de despliegue de ArcSight puede ser complicado si no se ha recibido el entrenamiento adecuado. Por esto las organizaciones que consideren ArcSight como una opción a implementar deben estimar un incremento de costos en el proyecto de despliegue del SIEM. Este incremento deberá ser destinado al entrenamiento del personal que va a mantener la solución, o bien como salario del personal certificado en este ámbito. Especialmente dado que el coste del entrenamiento y certificaciones por parte de HP puede encarecer considerablemente el presupuesto estimado del despliegue del SIEM.

El proceso de ventas de ArcSight se realiza con un cierto nivel de hermetismo empresarial, por lo que puede resultar complicado obtener un presupuesto por parte de HPE si no se ha realizado un inventario y planificación del entorno dónde se instalará el sistema. De hecho, incluso cuando se cuenta con toda la planificación, si el personal de ventas considera que el entorno objetivo no puede costear la solución, no ofrecerán una estimación del costo de ArcSight.

Para el producto ESM existen múltiples tipos de licenciamiento, siendo la base para solicitar una cotización los siguientes parámetros:

En la siguiente tabla se presentan los valores base para el licenciamiento de ArcSight ESM:

Modelo de Software	ESM 20 GB/d	ESM 50 GB/d	ESM 100 GB/d	ESM 150 GB/d	ESM 250 GB/d
Gigabytes por día (GB/Day)	20	50	100	150	2500
Eventos Por Segundo (Promedio)	1	2,5	5	7,5	12,5
Dispositivos de red	100	250	500	500	500
Interfaces de usuarios	10	25	25	25	25
Usuarios de las consolas	2	3	3	3	3
Evaluación de Vulnerabilidades	10	10	10	10	10
Actores en las vistas	50	50	50	50	50
Licencias de administración de Connectors.	4	4	4	4	4
Precio estimado[2]	Desde $20,000 USD en entornos pequeños hasta $1,000,000 USD en despliegues grandes con posibilidad de incrementar su precio hasta 10 veces en medida de la cantidad de dispositivos a monitorear.				

Ilustración 12 – Licenciamiento para HP ArcSight Enterprise Security Manager (Hewlett Packard Enterprise, HPE Arcsight Enterprise Security Manager, 2016)

Con base en estos valores, es posible contactar a un vendedor de HPE con objetivo de obtener un presupuesto más acercado a la realidad. Si se desea aumentar algunos de los parámetros especificados, es posible hacerlo con personal de ventas de HPE quienes indicarán cuales serían los costos reales de la solución objetivo.

[2] El precio estimado está basado en publicaciones pasadas sobre licenciamiento de ArcSight, para obtener un precio real es necesario contactar a un vendedor de HPE con el entorno para el cual se está implementando la solución plenamente definido.

Splunk

Splunk se ofrece en dos presentaciones, gratuita y empresarial. La licencia gratuita de Splunk está enfocada a un uso personal y está limitada un máximo de 500Mb por día. Las licencias empresariales y de la nube existe en dos tipos, anual, o licencia perpetua, ambas ofrecen las mismas capacidades añadidas a la versión gratuita con múltiples roles de usuarios, entornos distribuidos con soporte para *clustering,* aplicaciones premium para la manipulación de los datos recopilados y soporte para el análisis de un tráfico de datos mucho más amplio.

El licenciamiento de Splunk está basado en el volumen máximo de tráfico por día de datos sin compresión que es indexado, expresado en Gigabytes por día, y no hay límite de búsquedas, alertas, interfaces o reportes en cualquiera de los 2 modelos de compra, licencia anual, y licencia perpetua. Cabe mencionar que el costo de la licencia perpetua no incluye el costo de mantenimiento y soporte por parte de Splunk, estos servicios deben ser contratados al menos durante el primer año de implementación. El modelo de licencias de Splunk brinda flexibilidad en el precio de los costos operativos ya que se adapta en gran medida al volumen de datos a analizar. Esto es especialmente útil cuando se analizan volúmenes de tráfico especialmente extensos; ya que el precio de la licencia disminuye en medida que aumenta el tráfico analizado (Splunk, Pricing, 2016).

En las siguientes figuras se presentan los precios base publicados por el fabricante para el licenciamiento de Splunk Enterprise:

	Licencia Perpetua		Licencia Anual		
Volumen de datos indexados por día	**Precio del plan**	**Precio por GB**	**Precio del plan**	**Precio por GB**	**Precio mensual por GB**
1 GB/día	$4,500	$4,500	$1,800	$1,800	$150
10 GB/día	$25,000	$2,500	$10,000	$1,000	$833
50 GB/día	$95,000	$1,900	$38,000	$760	$3,166
100 GB/día	$150,000	$1,500	$60,000	$600	$5,000
>100 GB/día	Contactar vendedores de Splunk		Contactar vendedores de Splunk		

Ilustración 13 – Licenciamiento para Splunk Enterprise (Splunk, Pricing, 2016)

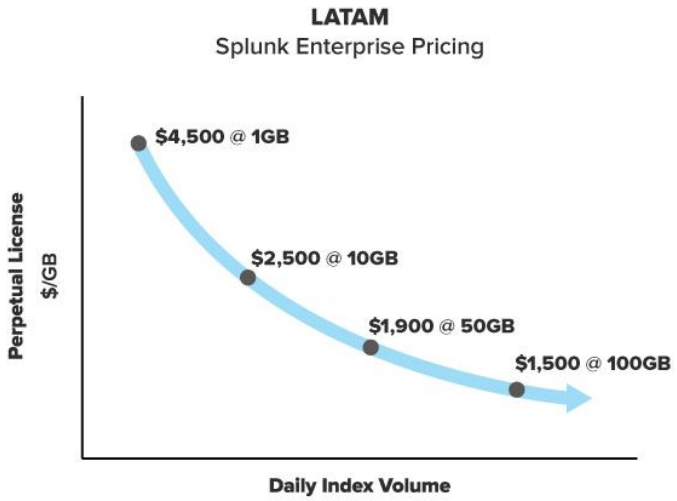

Ilustración 14 – Costos del licenciamiento para Splunk Enterprise (Splunk, Pricing, 2016)

En base a estas premisas, es evidente que la oferta de análisis de datos de Splunk está orientada a organizaciones medianas y grandes, u organizaciones que registran gran volumen de datos y que requieren un análisis en profundidad de ellos. Para organizaciones que implementan Big Data también existe una solución llamada Hunk, que es una instancia de análisis de Splunk para Hadoop. Los precios de Hunk se basan en el número de nodos TaskTracker (nodos de computación en YARN) en los clústeres de Hadoop. El precio de una licencia de un año de Hunk comienza en

$3,000 por nodo TaskTracker de Hadoop o nodo de cómputo con un mínimo de diez nodos TaskTracker o nodos de cómputo (Splunk, Pricing, 2016).

En caso de que una organización no se adapte a los modelos de licencia anteriormente descritos, Splunk ofrece una solución para entornos más pequeños de TI que automatiza la búsqueda y análisis de logs en un producto denominado “Splunk Light” que al igual que la versión Enterprise, basa su licenciamiento en el volumen de datos indexado por día.

En la siguiente tabla se presentan los valores base para el licenciamiento de Splunk light

	Licencia Perpetua		**Licencia Anual**		
Volumen de datos indexados por día	**Precio del plan**	**Precio por GB**	**Precio del plan**	**Precio por GB**	**Precio mensual por GB**
1 GB/día	$1,800	$1,800	$900	$900	$75
2 GB/día	$3,300	$1,650	$1,650	$825	$69
5 GB/día	$7,500	$1,500	$3,750	$750	$63
10 GB/día	$13,500	$1,350	$6.75	$675	$56
15 GB/día	$18,900	$1,260	$9,450	$630	$53
20 GB/día	$24,000	$1,200	$12,000	$600	$50

En general, los costos de implementación y de mantenimiento de Splunk pueden ser fácilmente adecuados a un presupuesto, pero existe la posibilidad de que incidentes particulares (como ser víctima de ataques DDoS) incrementen el volumen de datos de manera significativa, lo que podría repercutir en la cantidad de datos que se podrían indexar, y por tanto en el precio final de la implementación.

En cuanto al personal que deberá desplegar, usar y dar mantenimiento entre otras actividades, no requiere de personal certificado, pero si es necesario que posea un buen nivel de conocimientos técnicos en materia de redes y de scripting. Esto es esencial en entornos dónde exista una amplia variedad de tecnologías de diversos fabricantes. En medida del volumen de datos también será necesario incrementar el número de personal que atienda la solución, esto a razón de que la fortaleza de Splunk se basa en la inteligencia operativa que provee.

Simulación de costos

Debido a que el tipo de licenciamiento de las diferentes soluciones es medido de forma diferente, es complicado ofrecer un punto de comparativa entre el licenciamiento basado en el número de activos, contra el licenciamiento basado en la cantidad de tráfico analizado por día. Para ejemplificar una comparativa de los costes de implementación de las diferentes soluciones, se presentan 10 empresas ficticias cuyo número de activos y volúmenes de datos por día se establecen de forma proporcional como lo muestra la siguiente tabla:

	NÚMERO DE ACTIVOS	TRÁFICO ANALIZADO AL DÍA (EN GB)	ALIENVAULT USM ALL-IN-ONE	SPLUNK ANUAL	SPLUNK PERPETUO	COSTO ARCSIGHT
			(Costo aproximado estimado en USD)			
EMPRESA 1	5	1	5595	1800	5400	6000
EMPRESA 2	10	2	5595	3000	9000	10000
EMPRESA 3	25	5	5595	6000	18000	20000
EMPRESA 4	75	10	10800	10000	30000	30000
EMPRESA 5	150	15	14500	15000	45000	50000
EMPRESA 6	250	25	30000	22500	67500	70000
EMPRESA 7	500	50	*	38000	114000	120000
EMPRESA 8	1000	100	*	60000	180000	190000
EMPRESA 9	2500	250	*	*	*	*

EMPRESA 10	5000	500	*	*	*	*

Ilustración 15 – Tabla comparativa de costos aproximados de licenciamiento (Splunk, Pricing, 2016) (Alienvault, 2016) (Hewlett Packard Enterprise, HPE Arcsight Enterprise Security Manager, 2016)

Esta tabla muestra el costo aproximado del costo de las licencias requeridas de acuerdo al caso hipotético de cada una de estas empresas, con base en su número de activos y el tráfico por día que es necesario analizar. Gráficamente se puede apreciar de la siguiente forma:

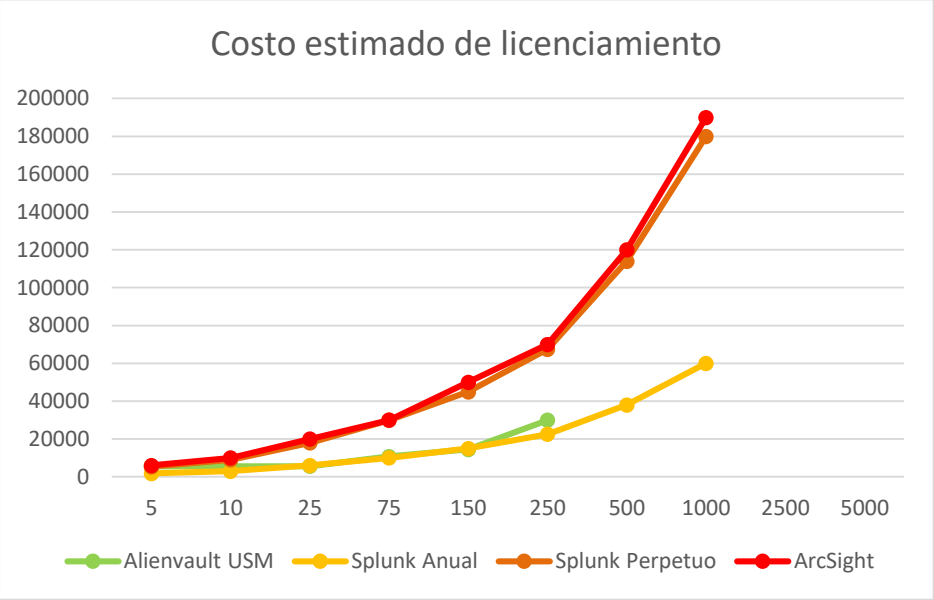

Ilustración 16 – Gráfica comparativa de costos aproximados de licenciamiento (Splunk, Pricing, 2016) (Alienvault, 2016) (Hewlett Packard Enterprise, HPE Arcsight Enterprise Security Manager, 2016)

CAPÍTULO 5 - CONCLUSIONES

Después del trabajo realizado, se ha obtenido un buen conocimiento sobre las herramientas SIEM en el mercado con énfasis en las soluciones seleccionadas, y se puede concluir que, para hacer un análisis de registros eficiente, es necesario planificarlo adecuadamente, siempre intentado apegarse a las normativas aplicables y a las necesidades de la organización.

Un aspecto clave a definir en las diferentes soluciones SIEM líderes del mercado tiene que ver con la arquitectura en la cual basan sus operaciones. La arquitectura modular que fue investigada ofrece una correlación escrupulosa y centralizada de los eventos de seguridad, desglosando y correlacionando cada evento en particular Se recomienda ampliamente orientar la arquitectura del SIEM a este enfoque modular debido a las facilidades y mejoras identificadas. Este enfoque permite realizar un análisis más efectivo de la información que otras arquitecturas centralizadas en un único núcleo, permitiendo segmentar y delimitar una manera precisa cuales son las áreas críticas en las que se quiere basar en análisis de la información. Otra ventaja del enfoque modular es que estas tecnologías permiten ayudar a detectar amenazas que de otra forma hubieran logrado mantenerse ocultas puesto que analizan la información en diversos niveles de aplicación, la coordinación de la correlación de los eventos registrados en los diferentes niveles de abstracción de los datos hace más efectivo su nivel de detección.

Es necesario mencionar, que existen muchas otras herramientas de SIEM tan valiosas como las opciones seleccionadas, y cada una aporta un producto diferente de los demás, cada uno enfocado a un tipo de funcionalidades específicas.

En general, para cualquier despliegue de los diversos fabricantes disponibles, si existe un procedimiento adecuado de planeación y de implementación, se puede

obtener un sistema funcional de administración, análisis, correlación y almacenamiento de registros a un costo asequible.

Para lograr esto, las organizaciones con interés en implementar un SIEM deben de definir sus necesidades antes de buscar soluciones y cuando encuentren algún producto que se adapte a sus necesidades, deben definir las metas que se buscan cumplir con el despliegue del mismo, de esta manera, podrán decantarse por una solución que cumpla con los requisitos que fueron planteados durante la definición de sus necesidades.

Algunas de las bondades de implementar un SIEM tiene que ver con la facilidad que ofrece para cumplir normativas como PCI DSS, además de aliviar la carga del personal de seguridad durante la respuesta incidentes, y ya que un SIEM puede proveer de mucha información que mejora la inteligencia operativa, que ayuda a detectar puntos de mejora en los sistemas.

Se puede concluir que las herramientas de SIEM se convertirán en una pieza clave dentro de la vida diaria de un SOC, y en base a las herramientas de detección y análisis que posean, la efectividad de respuesta a incidentes crecerá de manera acorde, sin embargo, para lograr esto, es necesario realizar una buena planificación y proyección de lo que se desea obtener al desplegar una solución SIEM. De lo contrario, el costo de la solución puede crecer considerablemente y puede suscitarse el caso que no cumpla con los objetivos para los cuales estaba pensada.

2.3 TRABAJO FUTURO

El mundo de la seguridad informática es un entorno dinámico que siempre se encuentra en un estado cambiante, según las predicciones de Kaspersky y Symantec

las amenazas a la seguridad van a seguir incrementándose cada vez más y para estar preparado antes las posibles brechas en la seguridad, será necesario contar con una apropiada respuesta a incidentes, lo cual solo podrá ser logrado efectivamente a través de este tipo de herramientas SIEM.

Por esto, se busca seguir explorando más soluciones SIEM y al igual que en el presente proyecto, investigar sus funcionalidades más importantes. Así como probar sus capacidades de detección de amenazas usando técnicas sofisticadas de evasión de sistemas de detección de intrusos.

Actualmente se está trabajando en la investigación de más herramientas de correlación como LogRhythm que continúa destacando en los reportes anuales de Gartner como un SIEM de alta madures y capacidad (Gartner, Kavanagh, & Rochford, Magic Quadrant for Security Information and Event Management, 2016), y cuyo SIEM no ha podido ser evaluado durante la realización de este proyecto debido a que los costos de licenciamiento o de asociación con la compañía, al momento de la realización de este proyecto eran incosteables. Sin embargo, en fechas recientes se ha logrado obtener demos y training por parte del fabricante con lo que se ha logrado identificar muchas de las fortalezas más grandes de esta solución, destacando ampliamente su motor de inteligencia artificial que le permite obtener una correlación de eventos mucho más avanzada que la competencia que basa su análisis en simples reglas de operaciones.

De igual manera se busca realizar la evaluación de otras soluciones líderes como IBM Security, EMC por RSA, o Intel Security.

En el campo de la detección de ciberamenazas existen tecnologías emergentes que presentan nuevos desafíos y las adecuadas respuestas en el ámbito de la

ciberseguridad, a medida que se detectan técnicas de ofuscación y ocultación cada vez más avanzadas, los profesionales de la seguridad deben prepararse para combatirlas y además deben poseer herramientas que les permitan responder acorde al nivel adecuado de riesgo aceptable en pro de su organización, no obstante, el hecho de que las amenazas avanzadas sea cada vez más difíciles de detectar, orilla a que se desarrollen nuevas técnicas de análisis y detección de amenazas como por ejemplo software de detección de amenazas basado en técnicas de inteligencia artificial (MIT, 2016), y en aprendizaje de máquinas.

La industria privada sigue liderando el ámbito de la investigación de amenazas, y así lo confirman recientes inversiones que se comparan con las inversiones que fueron destinadas en su momento a la creación de empresas como SourceFire y FireEye (Gregg, 2016). De la misma forma que impulsan los campos de la ciberseguridad, también puede ser contraproducente dado que las mejores técnicas de detección y respuesta son reservadas para el sector privado, y organizaciones que no poseen los recursos para comprar los servicios privados, tienen que limitar sus capacidades de respuesta a las herramientas de código abierto que a menudo quedan rezagadas en funcionalidades comparados respecto a sus contrapartes privadas.

Otro aspecto innovador a explorar tiene que ver con una nueva tecnología de TrapX que busca inducir respuesta a incidentes basada en la “decepción” de los atacantes, que integra innovadoras trampas virtuales que resultan en una avanzada especie de “*honeypots*” basados en aplicaciones virtuales o híbridas que no requieren realizar cambios sustanciales en la infraestructura de red. Se espera que esta tecnología se encuentre disponible a mitad del año 2017 (TrapX Security, s.f.).

Una propuesta teórica de evaluación y mejora de las herramientas de SIEM consiste en la implementación de estas tecnologías en ambientes de alta actividad maliciosa,

por ejemplo, eventos de tipo *Capture The Flag* (CTF) dónde constantemente se realizan intentos de intrusión y explotación de vulnerabilidades en laboratorios controlados de pruebas. Este escenario plantea una interesante oportunidad de investigación en el futuro del desarrollo de herramientas de detección y mitigación de incidentes de seguridad.

3 GLOSARIO

ACL.- (*Access List*). Lista de Control de Acceso. Lista de Control de Acceso

Amenaza.- Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Antispam.- Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus.- Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Ataque dirigido.- Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas. No son ataques masivos, porque su objetivo no es alcanzar al mayor número posible de ordenadores. Su peligro estriba precisamente en que son ataques personalizados, diseñados especialmente para engañar a las potenciales víctimas

Ataques Web.- Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Back Door.- Puerta trasera. Es una secuencia especial dentro del funcionamiento de un sistema, mediante la cual se pueden evitar los sistemas de seguridad (autentificación) para acceder al sistema, que pueden ser utilizadas para fines maliciosos y de espionaje.

Backup.- Copia de seguridad. Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Base de datos.- Es un conjunto de ficheros que contienen datos y los programas que gestionan la estructura y la forma en la que éstos se almacenan, así como la forma en la que deben relacionarse entre sí. Algunos ejemplos de sistemas de bases de datos, son: Access, Oracle, SQL, Parados, dBase, etc.

BIOS.- (*Basic Input / Output System*). Sistema básico de entrada y salida. Estándar de facto que define la interfaz de firmware para computadoras IBM PC compatibles

Blacklist.- Lista Negra. La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos

Bot.- Robot. Un bot es una computadora individual infectada con malware, la cual puede formar parte de una red de bots (bot net).

Botnet.- Red de robots. Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

C&C.- (*Control and command*). Canal de control y comando. Un canal de mando y control es el medio por el cual un atacante se comunica y controla los equipos infectados con malware, lo que conforma un botnet.

CPU.- (*Central processing unit*). Unidad central de procesamiento. Hardware dentro de un ordenador u otros dispositivos programables, que interpreta las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema

DMZ.- (*Demilitarized zone*). Zona desmilitarizada o Red perimetral. Zona segura que se ubica entre la red interna de una organización y una red externa, generalmente en

Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna

DoS.- (*Denial of service*). Denegación de servicio. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima

Encriptación.- La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

Exploits.- son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

Filtración de datos.- Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados

Firewall.- Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

GUI.- (*Graphical User Interface*). Interfaz Gráfica de Usuario. Programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.

IDS.- (*Intrussion Detection System*). Sistema de detección de intrusos. Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

IPS.- (*Intrussion Prevention System*). Sistema de prevención de intrusos. Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

IRC.- (*Internet Relay Chat*). . Protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior.

LAN.- (*Local Area Network*). . es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

Log.- Registro o Bitácora. Registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática un log es usado para registrar datos o información sobre quien, que, cuando, donde y por qué un evento ocurre para un dispositivo en particular o aplicación.

Malware.- El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos

extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

Payload.- El payload en informática son los datos transmitidos en una comunicación. Concretamente, es la parte de la transmisión la cuál era el propósito fundamental de la comunicación, es decir, el payload no incluye información enviada como cabeceras o metadatos. En seguridad computacional, el payload se refiere a la parte del malware que realiza la acción maliciosa. En el análisis de software malicioso como gusanos, virus o Troyanos, se refiere a los resultados del ataque del software. Ejemplos de payloads podrían ser destrucción de datos, mensajes ofensivos o correo electrónico basura enviado a una gran cantidad de personas (spam).

PCI DSS.- (*Payment Card Industry Data Security Standard*). Estándar de seguridad de Datos de la Industria de Tarjetas de Pago.

Phishing.- es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito otra información bancaria).

Rootkits.- Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final. Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano

o incluso simplemente al navegar en un sitio Web malicioso. Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

SEM.- (*Security Event Management*). . Consola de administración de seguridad que basa su funcionalidad en el monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de las consolas de análisis.

SIEM.- (*Security Information and Event Management*). Administración de eventos e información de seguridad. En el campo de la seguridad informática productos y servicios de SIEM proveen análisis en tiempo real de eventos de seguridad, generan alertas y permiten la gestión de los incidentes.

SIM.- (*Security Information Management*). Consola de administración de seguridad que basa su funcionalidad en el almacenamiento a largo plazo, así como el análisis y presentación de datos de registro.

SNMP.- (*Simple Network Management Protocol*). . es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SOC.- (*Security Operation Center*). Centro de Operaciones de Seguridad. El SOC es una facilidad dónde los activos informáticos de una organización (sitios web, aplicaciones, bases de datos, data centers, servidores, redes, estaciones de trabajo y otros endpoints) son monitoreados, evaluados, y defendidos.

SPAM.- También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar

direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

SSL.- (*Secure Sockets Layer*). capa de puertos seguros. Protocolo criptográfico que proporcionan comunicaciones seguras por una red. Usa criptografía asimétrica para autentificar a la contraparte con quien se está comunicando, y para intercambiar una llave simétrica. Esta sesión es luego usada para cifrar el flujo de datos entre las partes. Esto permite la confidencialidad del dato/mensaje, y códigos de autenticación de mensajes para integridad y como un producto lateral, autenticación del mensaje. Es el antecesor de TLS.

Syslog.- es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

TCP.- (*Transmission Control Protocol*). . Es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. El fin de TCP es proveer un flujo de datos confiable de extremo a extremo sobre una red que es susceptible a fallos.

TI.- Tecnologías de la información. es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.

TLS.- (*Transport Layer Security*). seguridad de la capa de transporte. Protocolo criptográfico que proporcionan comunicaciones seguras por una red. Usa criptografía asimétrica para autentificar a la contraparte con quien se está comunicando, y para intercambiar una llave simétrica. Esta sesión es luego usada para cifrar el flujo de datos entre las partes. Esto permite la confidencialidad del dato/mensaje, y códigos de autenticación de mensajes para integridad y como un producto lateral, autenticación del mensaje. Es el sucesor de SSL.

Troyano.- (*Trojan*). Caballo de Troya. Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es

que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

UDP.- (*User datagram protocol*). . Es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción

VPN.- (*Virtual Private Network*). Red Privada Virtual. Es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Vulnerabilidad.- Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas

Whitelisting.- Lista blanca. La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

Worm.- Gusano. Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

Virus.- Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios: Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa. Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Vector de ataque.- Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

4 BIBLIOGRAFÍA

AlienVault. (2016, 06 12). *AlienVault Unified Security Management™: Better Threat Detection for Effective Response*. Retrieved from AlienVault: https://www.alienvault.com/products

AlienVault. (2016, 06 12). *Solutions for Every Eviroment!* Retrieved from AluenVault: https://www.alienvault.com/products/pricing

Alienvault. (2016, 12 01). *USM Appliance Pricing*. Retrieved from Alienvault: https://www.alienvault.com/products/usm-appliance/pricing

Anderson, J. P. (1980). *Computer Security Threat Monitoring and Surveillance.* Washington.

Barraco, L. (2014, 03 15). *Top 5 Problems with Traditional SIEM (Infographic).* Retrieved from AlienVault: https://www.alienvault.com/blogs/security-essentials/top-5-problems-with-traditional-siem-infographic

Chuvakin, A. A., Schmidt, K. J., & Phillips, C. (2013). *Logging and Log Management.* Waltham, MA, USA: Syngress.

Davis, A. (2015, 03 06). *A History of Hacking*. Retrieved from The Institute: http://theinstitute.ieee.org/technology-focus/technology-history/a-history-of-hacking

Gartner, Kavanagh, K. M., & Rochford, O. (2015, 07 20). *Magic Quadrant for Security Information and Event Management*. Retrieved from Gartner: https://www.gartner.com/doc/reprints?id=1-2JNR3RU&ct=150720&st=sb

Gartner, Kavanagh, K. M., & Rochford, O. (2016, 08 10). *Magic Quadrant for Security Information and Event Management*. Retrieved from Gartner: https://www.gartner.com/doc/reprints?id=1-2Q17LAL&ct=151019&st=sb

Gregg, A. (2016, 08 23). *The Washington Post.* Retrieved from The Washington Post: https://www.washingtonpost.com/business/capitalbusiness/new-enterprise-associates-ups-its-investment-in-cyber-threat-detection/2016/08/22/10863296-68a0-11e6-8225-fbb8a6fc65bc_story.html

Hewlett Packard Enterprise. (2016, 06 12). *HPE Arcsight Enterprise Security Manager*. Retrieved from HP: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA4-3483ENW.pdf

Hewlett Packard Enterprise. (2016, 06 12). *HPE ArcSight SIEM solution*. Retrieved from HP: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA6-4463ENW.pdf

Hewlett Packard Enterprise. (2016, 06 12). *HPE Security ArcSight ESM Express All-in-one SIEM appliance.* Retrieved from HP: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA4-1163ENW.pdf

Holland, T. (2004, 2 23). Undestanding IPS and IDS. *Using IDS and IPS together for Defense in Depth*, p. 12.

HP Enterprise. (2016, 06 12). *ArcSight Express Technical Specifications*. Retrieved from HP: http://www8.hp.com/us/en/software-solutions/arcsight-express-siem-appliance/tech-specs.html

http://cert.org/about/. (2015, 03 09). *"About Us: The CERT Division".* Retrieved from Software Engineering Institute. Carnegie Mellon University.: http://cert.org/about/

Jackson, D. D. (2005, 08 23). *SANS*. Retrieved from GIAC Security Essentials Certification: https://www.giac.org/paper/gsec/3209/cliff-notes-guide-history-information-security-past-present-future/105327

Kemmerer , R. A., & Vigna, G. (2002). *Intrusion Detection: A Brief History and Overview.* Santa Barbara: University of California Santa Barbara.

Maynor, D. (2011). Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research. In D. Maynor, *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research* (p. 350). Elsevier: Syngress.

MIT. (2016, 04 18). *Massachusetts Institute of Technology.* Retrieved from MIT News: http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

Price, D. (2008, 06 30). *Blind Whistling Phreaks and the FBI's Historical Reliance on Phone Tap Criminality*. Retrieved from Counter Punch: http://www.counterpunch.org/2008/06/30/blind-whistling-phreaks-and-the-fbi-s-historical-reliance-on-phone-tap-criminality/

Scarforne, K., & Mell, P. (2001). Guide to Intrussion Detection and prevention Systems (IDPS). *National institute of atendards an Technology*, 127.

Schwab, P. (2015, 9 9). *The History of Intrusion Detection Systems (IDS) - Part 1*. Retrieved from Threath Stack: http://blog.threatstack.com/the-history-of-intrusion-detection-systems-ids-part-1

SourceFire, I. (2012, 01). *Snort::Home page*. Retrieved from Snort.

Splunk. (2016, 08 23). *Pricing.* Retrieved from Splunk: http://www.splunk.com/en_us/products/pricing.html

Splunk. (2016, 06 12). *Splunk Enterprise and Splunk Cloud.* Retrieved from Splunk: http://www.splunk.com/en_us/products/splunk-enterprise/features.html

The New York Times. (1981, 07 26). Retrieved from CASE OF THE PURLOINED PASSWORD: http://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html

TrapX Security. (n.d.). *TrapX*. Retrieved from https://deceive.trapx.com/rs/929-JEW-675/images/White_Paper_TrapX_DeceptioninDepth.pdf

Visa Europe. (2012, 12 21). *Planning for and implementing security logging.* Retrieved from Visa Europe: https://www.visaeurope.com/media/images/security_logging_factsheet-73-18417.pdf

Wilcox, J. E. (2001). *Solving the Enigma: History of the Cryptanalytic Bombe, a NSA phamphle.* Center for Cryptologic History, National Security Agency.
Winterbotham, F. W. (1974). *The Ultra secret: the inside story of Operation Ultra, Bletchley Park and Enigma.* London: Orion Books .