Implementación de una arquitectura de correlación de eventos para la mitigación de riesgos informáticos de una infraestructura de servidores virtuales del laboratorio de redes convergentes del ITM

Diana Milena Camacho Echavarría

Leidy Johana Moreno López

Ingeniería de Sistemas

Director:

Miguel Ángel Roldán Álvarez

INSTITUTO TECNOLÓGICO METROPOLITANO

2018

RESUMEN

Debido al auge que ha tomado en la actualidad la ola de la información, grandes y pequeñas empresas se ven a diario expuestas a amenazas en sus redes de comunicación al exponer servicios virtuales que dan acceso a un sin número de personas diariamente, haciendo que la vulnerabilidad sea mucho mayor y obligando así a protegerse y buscar medidas de prevención, para evitar posibles ataques que atenten contra la integridad, confiabilidad y disponibilidad de sus sistemas.

Por tal motivo este proyecto tiene como objetivo implementar un correlacionador de eventos de seguridad en el laboratorio de redes convergentes del bloque O del ITM sede fraternidad, específicamente en los servidores virtuales, los cuales se identificaron como los más vulnerables a ataques debido a su exposición en la red. Para la adecuada implementación del proyecto se selecciona la herramienta OSSIM, por ser un open source que proporciona todas las características de seguridad de un SIEM necesarias para gestionar eventos que suceden en la red, permitiendo recopilar logs, normalizar, correlacionar y alertar sobre posibles vulnerabilidades.

Para garantizar el adecuado funcionamiento se realizan finalmente una serie de pruebas, evaluando las respuestas y comportamiento del SIEM implementado, se analiza los resultados arrojados por la herramienta y se demuestra su utilidad en la detección de posibles amenazas en una red, como accesos indebidos, ataques a la información, entre otros.

Palabras claves: Correlación de eventos, SIEM, prevención y mitigación de amenazas, vulnerabilidades.

RECONOCIMIENTOS

Especial agradecimiento al laboratorio de redes convergentes del bloque O del ITM y al monitor Christian Gaviria por facilitarnos acceso y el ambiente adecuado para llevar a cabo este proyecto.

Agradecimiento muy especial a nuestros asesores Javier Mauricio Duran y Miguel Ángel Roldan, ya que su orientación y ayuda fue fundamental en la realización del proyecto.

A la Institución universitaria ITM y todo el grupo de profesores que brindan sus conocimientos para enriquecer sus alumnos y ayudarnos a crecer profesional y personalmente.

A nuestra familia que incondicionalmente nos brindan su apoyo y compresión en cualquier circunstancia presente.

ACRÓNIMOS

SIEM Security Information and Event Management

HIDS Sistema de detección de intrusos de Host

OSSIM Open Source Security Information Management ó Gestión de información de seguridad de código abierto

LOG Registro de eventos y acciones sucedidas

SSH Secure Shell, protocolo de administración remota que permite a los usuarios modificar sus servidores remotos a través de internet.

SQL Structured Query Language ó Lenguaje de consulta estructurada

CFG Archivo de configuración genérica

BASH Bourne-Again Shell, programa informático, cuya función consiste en interpretar órdenes y un lenguaje de consola

SYSLOG Sistema para procesamiento de registro

RSYSLOG Sistema de cohete rápido para el procesamiento de registro

TCP Transmission Control Protocol o Protocolo de Control de Transmisión

UDP User Data Protocol o Protocolo de datos de usuario

PLUGIN Aplicación que en un programa informático, añade una funcionalidad adicional o una nueva característica al software

IPS Intrusion Prevention system ó sistema de prevención de intrusos

HUB dispositivo para compartir una red de datos o de puertos USB de una computadora

IPV4 Internet Protocol version 4, cuarta versión del protocolo de internet (IP)

IPV6 Internet Protocol version 6

HFC Hibrid fiber coaxial

HOST Computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella.

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

1. INTRODUCCIÓN

1.1. GENERALIDADES

1.1.1. Pertinencia

La adecuada gestión de eventos en diferentes dispositivos de red, presenta una evidente pertinencia a la hora de brindar seguridad en las redes para las empresas que manejan datos y dispositivos con diferentes servicios expuestos, en este sentido, los eventos vistos de forma correlacionada generan alertas de vulnerabilidades que se presenten en la red y permite analizarlos de una forma adecuada, esto ayuda a tomar medidas de prevención.

1.1.2. Justificación

En la actualidad grandes, medianas y pequeñas empresas tienen su información y recursos expuestos en la red a través de servicios web, bases de datos o simplemente al dejar algún puerto abierto, dando lugar a que la información que por ellas circula sean mucho más accesibles a personas mal intencionadas que pueden atentar contra la disponibilidad e integridad de los servicios ofrecidos, por lo cual se hace importante tener una adecuada gestión de la seguridad en las redes que permita estar alerta ante cualquier posible amenaza.

A diario en cada dispositivo de red se genera gran cantidad eventos, los cuales es imposible poder revisar uno a uno en cada dispositivo, esto hace que ocurran eventos críticos que no sean detectados y de la forma contraria que se dé importancia a eventos que no son relevantes, haciendo que los dispositivos y servicios de la red estén expuestos a amenazas que no se puedan controlar o detectar con anticipación.

La correlación de eventos ofrece una solución bastante amplia para gestionar los eventos generados en cada dispositivo, al hacerlo de forma relacionada ayuda a priorizar los eventos más

críticos que se presenten en la red y generar alertas que ayuden a tomar medida para mitigar posibles amenazas. Esto hace que implementar un correlacionador de eventos sea un plus para mantener la seguridad de la misma.

1.1.3. Problema abordado

La seguridad en las redes informáticas es un tema que ha tomado alta relevancia en todos los escenarios actuales de tecnología, debido a que continuamente las empresas se ven expuestas o vulnerables a ataques maliciosos que atentan contra la integridad, autenticidad, disponibilidad, confidencialidad y no repudio de la información y sistemas en general.

Se evidencia en diferentes reportes de seguridad, índices de crecimiento continuo en los incidentes informáticos presentados en las empresas.

En el último reporte de seguridad realizado en Latinoamérica por ESET (ESET security report 2017), se evidencia que solamente en el año 2016 el 49% de los incidentes presentados en las empresas latinoamericanas corresponde a infecciones por Malware, presentando un preocupante crecimiento con respecto a años anteriores, seguido por incidentes por ransomware con un 16% y phishing con un 15%.

Ilustración 1. Incidentes de seguridad en empresas de Latinoamérica (Eset , 2017).

Estas cifras muestran el alto índice de inseguridad informática que se presenta en las empresas y hacen cuestionar acerca de ¿qué mecanismos se pueden implementar que puedan ayudar a mitigar estas vulnerabilidades y prevenir futuros ataques? Aunque es claro que en gran parte la seguridad depende del cuidado humano, también existen herramientas y métodos que apoyan la gestión de la seguridad en las empresas.

Así como en muchas empresas de Latinoamérica, el laboratorio de redes convergentes del ITM, también se encuentra expuesto a amenazas tales como accesos indebidos a la red, alteración o robo de la información contenida en los servidores, interrupción de los servicios prestados, entre otros, ya que no cuenta con herramientas suficientes para analizar y monitorear el flujo de eventos que ocurren frecuentemente, por lo que pueden ocurrir algún incidente de los mencionados anteriormente y de los cuales no se tenga aviso alguno y pueden causar grandes daños en la red y exponer su información.

Hasta ahora el laboratorio de redes convergentes no cuenta con ninguna herramienta de correlación de eventos, por lo cual la revisión de logs se debe realizar desde cada dispositivo de forma independiente, sin embargo al ser demasiados los logs que se generan a diario en cada uno de ellos, muchos de estos eventos se pierden y no son analizados ni tenidos en cuenta para tomar medidas de prevención.

De acuerdo con lo anterior, este proyecto se implementa una herramienta SIEM que permite relacionar diferentes eventos de los servidores más críticos del laboratorio de redes convergentes y a partir de unas reglas de correlación definidas y configuradas previamente, se puede identificar alertas de posibles amenazas en dichos dispositivos, todo esto debidamente documentado ayuda a tomar medidas preventivas y por ende a mitigar dichas amenazas.

1.2. OBJETIVOS

1.2.1. General

Implementar una arquitectura de correlación de eventos para mitigar riesgos informáticos en la infraestructura de servidores virtuales en el laboratorio de redes convergentes del ITM.

1.2.2. Específicos

- Identificar los dispositivos de red del laboratorio de redes convergentes del ITM que se deben monitorear para la correcta gestión de eventos de seguridad.

- Configurar los mecanismos para la gestión de logs en los dispositivos que reportarán eventos de seguridad que permitirán promover la prevención y mitigación de posibles amenazas.

- Implementar la tecnología, topología, reglas y arquitectura de SIEM open source más apropiada a las necesidades de correlación de eventos en los dispositivos identificados en el laboratorio.

- Realizar pruebas sobre la implementación SIEM seleccionada en el laboratorio de redes a partir de la definición de un conjunto de reglas según las amenazas que se pretenden prevenir y mitigar.

1.3. ORGANIZACIÓN DE LA TESIS

El desarrollo del trabajo de grado está compuesto por 4 capítulos, el primero es el marco teórico en el cual se sustentan y analizan teorías e investigaciones referidas a la implementación de Correlación de eventos SIEM, se detalla su funcionalidad, sus inicios, los aportes en la industria, se comparan diferentes herramientas SIEM open source y diversas metodologías para el desarrollo de la implementación.

El segundo capítulo es la Metodología donde se desarrolla paso a paso las técnicas seleccionada para el cumplimiento de los objetivos, se divide en cuatro etapas:

- **Fase de reconocimiento:** donde se identifican y tipifican los dispositivos del laboratorio, determinando los dispositivos que se deben monitorear, tales como servidores que contienen información sensible.
- **Fase de Diseño:** en esta fase se realiza el diseño de la arquitectura y se definen las herramientas y configuraciones requeridas para la gestión adecuada de logs.
- **Fase de implementación:** donde se realiza el despliegue y configuración de la herramienta SIEM, así como la implementación de reglas de correlación y configuraciones de los parámetros requeridos en los dispositivos a monitorear.
- **Fase de Pruebas:** donde se realiza pruebas de funcionamiento del software implementado.

Seguidamente en el capítulo de resultados y discusión, se analizan los diferentes resultados obtenidos después de la implementación de la herramienta de correlación de eventos y su aporte en la mitigación y prevención de amenazas de seguridad en la red del laboratorio.

Finalmente en el último capítulo de conclusiones, recomendaciones y trabajo Futuro, se concluye el trabajo realizado desde diferentes frentes como infraestructura, herramientas y configuraciones de los dispositivos, se dan las recomendaciones de acuerdo al desarrollo del

trabajo y se plantean posibles trabajos futuros que ayuden a potencializar la herramienta instalada en pro de beneficiar la seguridad en la red del laboratorio.

2. MARCO TEÓRICO

Evento es todo aquello que sucede (en una red, en un sistema, entre otros) y la correlación de eventos o SIEM (Security Information and Event Management) es interrelacionar varios eventos que puedan dar señales de un comportamiento anormal y generar alertas, que de otra forma sería muy difícil detectar. “Mediante la recopilación de eventos de login, acceso a BBDD, logs de firewall, proxy, IPS, logs de aplicaciones, etc, un SIEM es capaz de monitorizar y predecir el comportamiento futuro de la plataforma TIC de tal manera que ante una conducta inusual de la plataforma puede generar una alerta y/o realizar una acción determinada” (SeguridadX, 2013).

Según (Sekharan & Kamalanathan Kandasamy, 2018) actualmente las organizaciones generan grandes cantidades de información y manejarla es fundamental para la operación de sus actividades. Por lo tanto, requieren herramientas de alto perfil que les ayude a gestionar la información y los eventos de seguridad. Security Information and Event Management (SIEM, por sus siglas en inglés) es una herramienta de gestión de eventos de seguridad que se encarga de dar una visión general del estado de la seguridad despertando gran interés en las empresas.

El término SIEM no es más que una combinación de las categorías de productos SIM (Security Information Management) o gestión de la seguridad de la información, el cual acumula datos en un repositorio central para análisis y brinda informes automatizados y centralizados y SEM (Security Event Manager) o gestión de eventos de seguridad, que centraliza la administración de almacenamiento, correlaciona los archivos de registro y permite funciones de monitoreo casi en tiempo real en un sistema de gestión de seguridad (Sekharan & Kamalanathan Kandasamy, 2018).

Los dispositivos de una red generan una gran variedad de logs de eventos que contienen información valiosa, una de las funciones de los sistemas SIEM es recolectar, relacionar y monitorear esta información para lograr mitigar posibles amenazas. También se busca por medio de los sistemas SIEM a través de reglas de correlación de eventos, verificar posibles ataques en diferentes dispositivos y con el histórico de la información, verificar la veracidad de dichos

ataques o crear reglas en caso de sospecha de alguna amenaza nueva. Los SIEM cuentan con análisis automatizado de eventos correlacionados y generan alertas para notificar a los usuarios de los problemas, estas alertas se generan por medio de un tablero de mando o a través de canales como correo electrónico.

Las plataformas SIEM son herramientas dedicadas a recopilar, almacenar, filtrar, correlacionar y mostrar los distintos eventos de seguridad en una organización. Tienen al menos las siguientes funciones y capacidades (SeguridadX, 2013):

Tabla 1. Características de herramientas SIEM. (Elaboración propia)

Funciones y Capacidades	Aportes
Agregación de datos	(administración de logs) Un SIEM tiene la capacidad de administrar de forma estandarizada los logs.
Agrupación	Se relacionan eventos con similitud en uno solo, para que su visualización sea más simple.
Correlación	Se agrupan eventos que presentan relación con una misma actividad o comportamiento sospechoso.
Priorización	Para visualizar los eventos más importantes de manera clara.
Alerta	Se analizan los eventos correlacionados para la producción de alertas, notificando a los destinatarios de los problemas inmediatamente.
Panel de control	Herramientas que permite convertir los datos del evento en tablas informativas.
Cumplimiento	Las aplicaciones SIEM se pueden utilizar para la recopilación de datos automática y elaboración de informes.

Retención	Se puede realizar almacenamiento de datos a largo plazo que facilitan la correlación con el tiempo.

La siguiente imagen ilustra la utilidad de utilizar una herramienta de correlación de eventos:

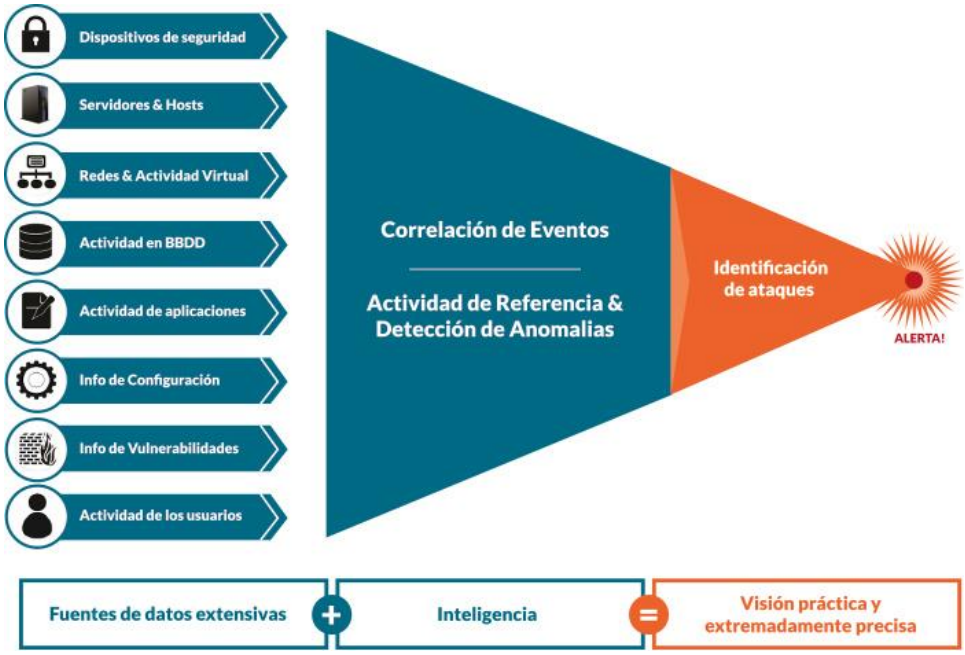


Ilustración 2. Utilidad herramientas SIEM (Sofistic, s.f.).

En la actualidad se pueden encontrar varias herramientas que permiten realizar procesos de correlación de eventos, entre las cuales se pueden destacar:

- **XpoLog**: es una solución de análisis de logs, análisis de eventos, correlación de eventos, análisis de logs de seguridad y aplicaciones, todo en una sola solución que se ofrece para instalación en infraestructura del Cliente o bajo un modelo SaaS hosteado en servidores de Xailna. (Xailna, s.f.)

- **SolarWinds:** Es una herramienta SIEM que facilita el uso de registros para seguridad, cumplimiento, detección y solución de problemas.

- **Logrhythm:** Es adecuado para las organizaciones que requieren capacidades avanzadas de monitoreo de amenazas en combinación con SIEM.

- **Ossim:** Software de AlienVault de código abierto, rico en funciones de recopilación, normalización y correlación. Ofrece una variedad de capacidades de seguridad integradas, incluyendo SIEM, monitoreo de integridad de archivos, evaluación de vulnerabilidades, descubrimiento de activos y sistemas de detección de intrusos basados en host y basados en la red.

- **Ossec:** Combina todos los aspectos de HIDS (detección de intrusión basada en host), monitoreo de registros y administración de incidentes de seguridad (SIM) / información de seguridad y administración de eventos (SIEM) juntos en una solución simple, poderosa y de código abierto.

El mercado de SIEM es definido por la necesidad del cliente para la detección temprana de ataques específicos e informar sobre los registros para dar respuesta oportuna a incidentes, esta necesidad impulsa a la expansión de proveedores de SIEM nuevos y existentes en el Mercado dando respuesta a los usuarios que buscan características avanzadas de análisis y respuestas.

El Cuadrante Mágico para la Información de Seguridad y Gestión de Eventos de Gartner (Kelly M. Kavanagh, 2016) se divide en las siguientes partes:

- Líderes: Se compone de proveedores que han sido los más exitosos en la construcción de una base instalada y una fuente de ingresos dentro del Mercado.

- Visionarios: Proporcionan productos que son una combinación funcional fuerte con los requisitos generales del mercado de SIEM, pero que tienen una capacidad de ejecución más baja que los líderes.
- Desafiantes: Proveedores qué carecen del historial de éxito competitivo con sus tecnologías SIEM.
- Jugadores de Nicho: Se compone de proveedores que son un buen partido para el uso específico o un subconjunto de requisitos funcionales de SIEM.

Ilustración 3. Cuadrante mágico para la información de seguridad. Fuente: A partir de Kavanagh (2016).

Tabla 2.Comparativo de herramientas de correlación de eventos SIEM. (Elaboración propia)

Herramienta	Autor	Aporte
OSSEC	Third Brigade, Inc.	Es un sistema de detección de intrusiones basado en host de fuente abierta (HIDS). Realiza análisis de registros, comprobación de integridad, supervisión del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuestas activas.
Graylog	GrayLog, Inc.	Es una plataforma de administración de syslog de código abierto que le ayuda a recopilar, indexar y analizar syslog en una ubicación centralizada. Estructurados de cualquier fuente.
EventLog Analyzer	ManageEngine	Es una herramienta que ayuda a automatizar el proceso completo de gestionar logs generados por computadora recolectando, analizando, correlacionando, buscando, generando informes y almacenando logs desde una ubicación central. Este software para el análisis de logs de eventos le ayuda a monitorear la integridad de los archivos, llevar a cabo análisis forenses de logs, monitorear usuarios privilegiados y cumplir con diferentes entidades regulatorias al analizar inteligentemente sus logs y generar instantáneamente una variedad de informes como de actividad de usuarios, tendencias históricas y más.
SIEMonster	SIEMonster	SIEMonster es una herramienta SIEM de código abierto, construida sobre componentes escalables, sin licencia, completamente documentada.
Logalyze	ZURIEL Kft.	LOGalyze es un software de monitoreo de redes y gestión de registros centralizado de fuente abierta. Si desea manejar todos sus datos de registro en un solo lugar, LOGalyze es la elección correcta. Es compatible con servidores Linux / Unix, dispositivos de red, hosts de Windows. Proporciona detección de eventos en tiempo real y amplias capacidades de búsqueda. (Logalyze, 2018)
Pandora FMS	Sancho Lerena	Es un software de monitorización para gestión de infraestructura TI. Esto incluye equipamiento de red, servidores Windows y Unix, infraestructura virtualizada y todo tipo de aplicaciones.
OSSIM	AlienVault	Es un sistema de administración de eventos y de información de seguridad de código abierto, que integra una selección de herramientas diseñadas para ayudar a los administradores de redes en seguridad informática, detección de intrusiones y prevención. (ALIEN VAULT, 2018)
Syslog		Es un sistema de logs que se encarga principalmente de la administración de logs, los cuales son generados por eventos del sistema.

Mecanismos de gestión de logs

La recolección de logs se realiza a través de protocolos de red y cada uno de estos tiene sus propios mecanismos y formas definidas de enviar los logs, a continuación se presenta algunos de los utilizados para estos envíos:

Tabla 3. *Mecanismos para la gestión de logs. (Elaboración propia)*

Mecanismo	Características
Syslog	Es el más común de los mecanismos para recolección de logs, es un protocolo cliente/servidor. Los mensajes de syslog se suelen enviar vía UDP, por el puerto 514 en formato de texto plano. Aunque ya hay versiones que utilizan TCP para que los datos viajen cifrados mediante SSL/TLS4 para el envío de los registros de datos, la herramienta syslog toma los registros de datos del Visor de Eventos (Windows) o de las notificaciones que llegan al sistema operativo (Unix), para transmitirlos al servidor del SIEM. (Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015)
SNMP	Protocolo Simpe de Administración de Red (por sus siglas en ingles Simple Network Management Protocol) Es un protocolo para la transmisión de logs de diversos tipos de datos generalmente utilizado para dispositivos de red. Se dispone mediante un dispositivo que administra los equipos de la red y recibe las notificaciones de los dispositivos administrados para reenviarlas al servidor centralizado de logs. (Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015)
Windows Event Log	Es un protocolo propietario de Microsoft para la recolección y transmisión. (Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015)
Bases de datos	Es una manera estructurada para el almacenamiento y recolección de logs. Donde se especifican los usuarios y privilegios que tendrán sobre los registros de logs, esta base de datos es recomendable que no se configure en el mismo tablespace de la base de datos de los registros, para evitar vulnerabilidades de seguridad que se puedan presentar. Adicional se debe instalar un programa para la lectura de los datos almacenados. (Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015)
Rsyslog	Es una versión mejorada del mecanismo syslog que ofrece alto rendimiento, excelentes características de seguridad y un diseño modular. Comenzó como un syslogd regular, pero se ha convertido en un excelente mecanismo para la gestión de registros, pudiendo aceptar entradas de una amplia variedad de fuentes, transformarlas y generar resultados para diversos destinos. A diferencia de syslog puede utilizar también protocolos TCP para el envío de eventos.

Metodologías de gestión de logs

Para la realización de este proyecto se evalúan diferentes metodologías que abordan el tema tratado, las cuales son descritas brevemente en la siguiente tabla:

Tabla 4. *Metodologías de Gestión de Logs. (Elaboración propia)*

Metodología	Autor	Aporte
Metodología para la detección de vulnerabilidades en redes de datos (Franco, Perea, & Puello, 2012)	David A. Franco, Jorge L. Perea y Plinio Puello	En esta metodología se realizan tres etapas: 1. Reconocimiento, donde se busca obtener la mayor información posible de la red objetivo, en esta se debe realizar una lista con todos los dispositivos que tiene conexión a internet. 2. Escaneo de puertos y enumeración de servicios en esta fase se evalúan los equipos obtenidos para determinar los puertos y servicios que están activos en cada uno de ellos, para determinar cuáles de estos son críticos dentro de la red. 3. Escaneo de vulnerabilidades.
Best Practices. Event Log Management for security and Compliance Initiatives (Ipswitch, s.f.)	Ipswitch	Este documento relaciona los requisitos necesarios para las herramientas ELM (Gestión de Registro de Eventos) y las mejores prácticas para disminuir el potencial de violaciones de seguridad y reducir la posibilidad de problemas legales o de cumplimiento en las organizaciones
Log Management Best Practices. The Benefits of Automated Log Management (Alertlogic, s.f.)	Alertlogic	En el documento se recomienda recoger, consolidar y procesar cualquier dato o registro generado en la organización, para ayuda de investigaciones y trazabilidad de eventos.
Succesful SIEM and Log Management Strategies for Audit and Compliance. (Swift, 2010)	Swift	Este documento plantea una guía, definiendo y separando los eventos de interés, documentando el alcance de cada uno y el proceso a realizar
Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM (Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015)	Avella Coronado, Julián David Calderón Barrios, Leonardo Fabio Mateus Díaz, Cristian Andrés	En este trabajo se ofrece una guía para la gestión de logs donde se debe conocer primero las tecnologías, procedimientos y políticas para el registro de logs, generación de logs, almacenamiento, análisis y seguridad de estos, así como la herramienta a implementar que para la guía se seleccionó OSSIM.
Gestión de Logs (Alonso-Alegre Díez, 2016)	Alonso-Alegre Díez, Mª Begoña	Se presenta una metodología y forma de actuar, cuyo objetivo es ayudar a la recopilación y clasificación de los ficheros logs, así como el procedimiento para una detección de vulnerabilidades y fallos de software.

Guía metodológica para la gestión centralizada de registros de eventos de seguridad en PYMES (NIÑO MEJIA & SIERRA MUNERA, 2007)	Diana Carolina Niño, Alejandro Sierra	En este documento de un trabajo de grado se propone una completa guía metodológica para gestionar de forma centralizada eventos de seguridad, en esta propone un paso a paso que comprende desde las configuraciones iniciales de los dispositivos hasta la evidencia digital de los logs.

Luego de investigar y analizar diferentes guías metodológicas enfocadas en la gestión de logs, se selecciona la Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM (Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015), esta herramienta ha sido caso de éxito en empresas como, el Bank of Marin el cuál gana una visibilidad detallada en su red gracias a OSSIM Y Celopay la cual protege su entorno AWS con OSSIM. La metodología fue seleccionada porque se adapta a las necesidades del problema a solucionar y las herramientas usadas son de fácil alcance.

La guía se divide en varias actividades para lograr que la gestión de logs se encuentre dentro de un marco fundamental para la seguridad de la información de la organización, en la Ilustración 5 se muestran dichas actividades:

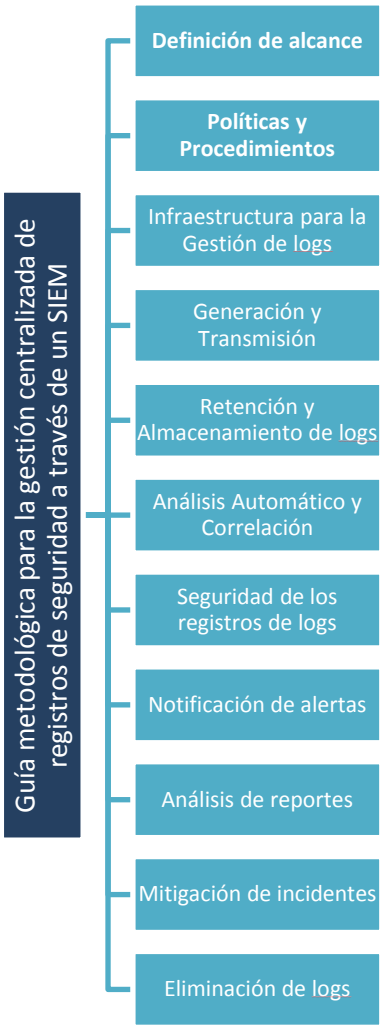


Ilustración 4. Diagrama de la metodología. Fuente: a partir de *(Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015)*

1. **Definición de alcance:** Definir que plataformas y tipos de logs harán parte del proceso de gestión.
    - Dispositivos de hardware o software. Identificar los activos ya sea software o hardware que tengan más criticidad para el negocio,
    - Responsables. Definir las responsabilidades dentro del proceso de gestión de logs.
    - Tipos de logs. Los sistemas de información generan varios tipos de registros de datos (logs), algunos son eventos no relevantes, por lo tanto es necesario realizar un filtro de los logs que generan más impacto para cada uno de los sistemas de información.

- Infraestructura para la gestión logs. En el alcance se debe definir con que infraestructura se va a contar para implementar la gestión de registros de datos (logs), Se debe realizar una caracterización en el diseño y la implementación de la infraestructura para la gestión de logs de acuerdo al alcance.

2. **Políticas y Procedimientos:** Generación de Políticas y Procedimientos que puedan formalizar e implementar el proceso de gestión de logs. Siguiendo las siguientes recomendaciones:
    - Se deben establecer los requerimientos en caso de que aplique a la organización referente a:
        - Generación de logs.
        - Transmisión de logs.
        - Almacenamiento de logs.
        - Disposición de los logs.
        - Análisis de logs.
        - Seguridad de los logs.
    - Establecer políticas que se puedan cumplir. Que no amenacen con la interrupción o disponibilidad de los procesos estratégicos o de negocio de una organización.
    - La política debe ser revisada periódicamente. Cada vez que hayan cambios en la infraestructura de tecnología.
    - Especificar los eventos más significativos para su tratamiento y análisis.
    - Hacer referencia a normas y regulaciones. Que se encuentren relacionadas dentro de la gestión de logs y deban ser aplicadas de acuerdo al negocio de la organización.

3. **Infraestructura para la Gestión de logs:** La guía sugiere el uso de una herramienta SIEM de uso libre como dispositivo central para la gestión de logs. Las siguientes

consideraciones deben ser tomadas para el diseño, implementación y adecuación de la infraestructura:

- El SIEM debe ser una plataforma centralizada, todos los logs de todas las fuentes definidas en el alcance deben ser transmitidos a la plataforma.
- La arquitectura en una infraestructura de gestión de logs, está compuesta por las siguientes partes:
    - Los activos que generan logs llamados fuentes o generadores de logs de datos.
    - Servidores de logs, donde se efectúa el análisis y el almacenamiento.
    - Servidor de monitoreo, donde se encuentran las consolas para el monitoreo de logs y reportes estadísticos e históricos.
- Utilizar medidas de control como cifrado de los logs que pasan a través de esta infraestructura, el motivo es evitar o reducir la propagación de amenazas de red.
- Características funcionales de la infraestructura de la gestión de logs:
    - Almacenar o tratar los logs de mayor interés filtrando aquellos que no supongan una información útil o relevante.
    - La infraestructura debe ser capaz de consolidar logs que tengan los mismos datos y convertirlo en uno solo.
    - Archivado de logs, debe tener capacidad de retener y preservar los archivos de registros por un periodo de tiempo establecido.

4. **Generación y Transmisión:** Asegurar que los registros de logs de las plataformas definidas en el alcance sean generados y transmitidos a la plataforma de gestión de logs.
    - Habilitar en los activos a analizar la generación de logs y su almacenamiento, además de su transmisión.
    - Revisión de documentación de fabricantes, desarrolladores y organizaciones de investigación sobre los tipos de logs que genera las fuentes de datos.

- Filtrar los eventos de acuerdo a la experiencia obtenida en la administración del activo.
- Habilitar un protocolo para recolección y transmisión de datos que se adapte a las capacidades y diseño en los elementos de arquitectura implementados para la gestión de logs.
- Que el formato generado por los protocolos para recolección y transmisión
- sean soportados por la arquitectura de la gestión de logs, es recomendado utilizar protocolos como syslog o bases de datos.

5. **Retención y Almacenamiento de logs:** En la gestión de logs es clave definir la retención y almacenamiento de los logs, estos requerimientos se deben especificar mediante políticas, donde se define el tipo de almacenamiento, tamaño, costo, velocidad de recuperación, archivado y destrucción de los logs.

6. **Análisis Automático y Correlación:** En el desarrollo de la guía y en la implementación de una herramienta SIEM, se hace necesario el análisis automático de los registros. En este proceso, se puede definir como el paso más importante, la correlación de los eventos.

7. **Seguridad de los registros de logs**: Implementar mecanismos de seguridad para protección de logs en las actividades de recolección, transmisión, almacenamiento y retención.

   Aunque las herramientas SIEM, están diseñadas para prevenir e identificar incidencias de seguridad que afecten a los activos de una organización, estas no están exentas de ser atacadas o vulneradas, durante los procesos en los que están involucrados.

8. **Notificación de alertas:** Establecer y configurar medios de notificación de alertas.

   De acuerdo a la política y los procedimientos que se crearon anteriormente, teniendo en cuenta los pasos descritos en la presente guía, se deben desarrollar y parametrizar las

reglas de análisis de eventos y las notificaciones de alertas a los eventos que no cumplan con los parámetros establecidos.

Es por esto que uno de los pasos principales indicados en la guía es el desarrollo y planteamiento de la política de seguridad dado que lo que incumpla con la misma es de obligatoria notificación.

9. **Análisis de reportes:** Configurar y ajustar reportes estadísticos e históricos para validación de comportamientos de la infraestructura tecnológica.

   Establecer tareas operativas para realizar análisis correcto y efectivo de los reportes de registros:

   En la presente guía se sugiere que se realicen tareas con diferentes periodicidades:

   - Diarias: para identificar posibles cambios en estructuras de los registros en los últimos días, tomar acciones en un menor tiempo.
   - Semanal: Se sugieren realizar revisiones semanales para evaluar posibles cambios y revisar variaciones en los sistemas.
   - Quincenales: Evaluar resultados de investigaciones realizadas.
   - Mensuales: Se recomiendan para evaluar procedimientos y estructuras de registros.
   - Anuales. Se sugieren para evaluar la efectividad y ajustes de la política de seguridad.

10. **Mitigación de incidentes:** Durante el análisis de los registros de logs, es posible identificar eventos de importancia como incidentes o problemas operacionales que requieran de una respuesta. Cada organización define el procedimiento para tratar estos eventos, desarrollando políticas o aplicando estándares como ITIL.

    Dentro de las mejores prácticas se recomienda construir una base de conocimientos de incidentes de seguridad, con información de vulnerabilidades conocidas, el significado de

los mensajes de registro y datos que ayuden a identificar los incidentes que se estén generando.

11. **Eliminación de logs:** Aplicar procedimientos y políticas para la eliminación apropiada de logs.

Con base en la anterior guía metodológica de define en el siguiente diagrama la metodología a seguida para la adecuada implementación del proyecto:

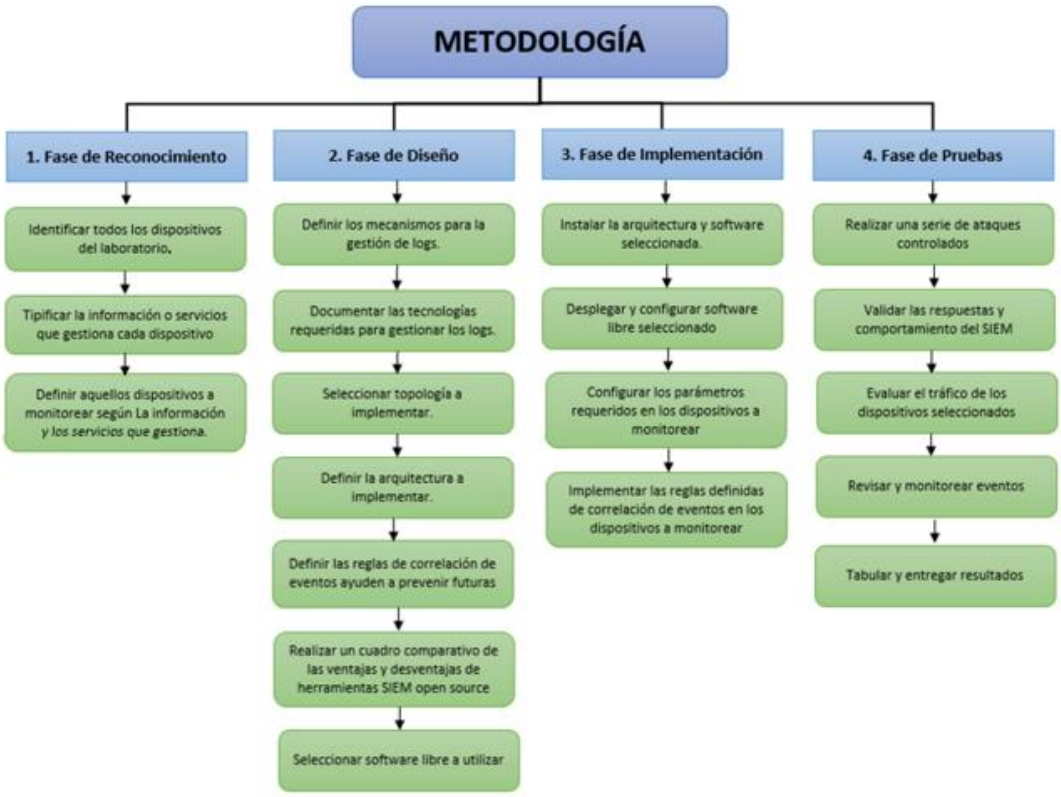


Ilustración 5. Metodología definida. Fuente: elaboración propia a partir de *(Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015)*)

3. METODOLOGÍA

3.1. Fase de reconocimiento

Laboratorio de redes convergentes Bloque O

El laboratorio de redes convergentes del ITM, se encuentra en el bloque O de la universidad y está compuesto por una red de servidores físicos y virtuales que exponen diferentes servicios.

A dicha red se puede ingresar públicamente a través de VPNs y Dst-NATs directamente al clúster, igualmente se puede ingresar locamente dentro de la red del semillero de forma cableada en cada laboratorio o de forma inalámbrica. La salida a internet desde el clúster, se realiza por medio del router de borde, para lo cual se debe pasar por diferentes routers antes de llegar a internet:

Ilustración 6. Ingreso a la red del semillero del bloque O. (Elaboración propia)

En el siguiente esquema se puede ver claramente el diseño de entrada y salida de la red del Bloque O:

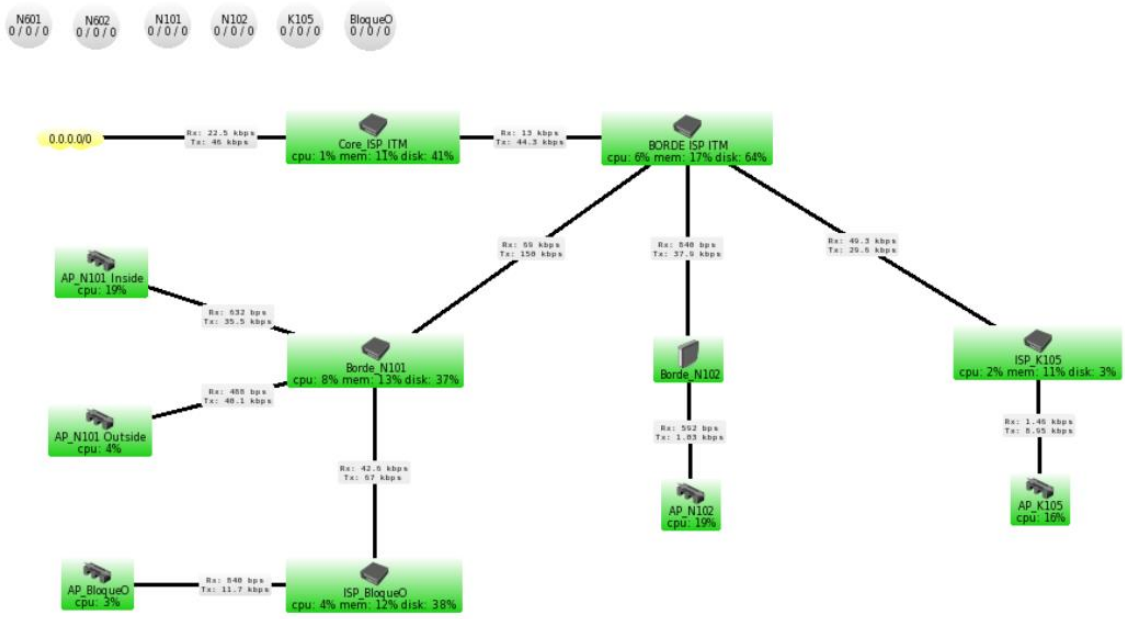


Ilustración 7. Diseño de entrada y salida de la red del Bloque O (Elaboración propia).

A continuación, se presenta un esquema de la red del laboratorio del Bloque O:

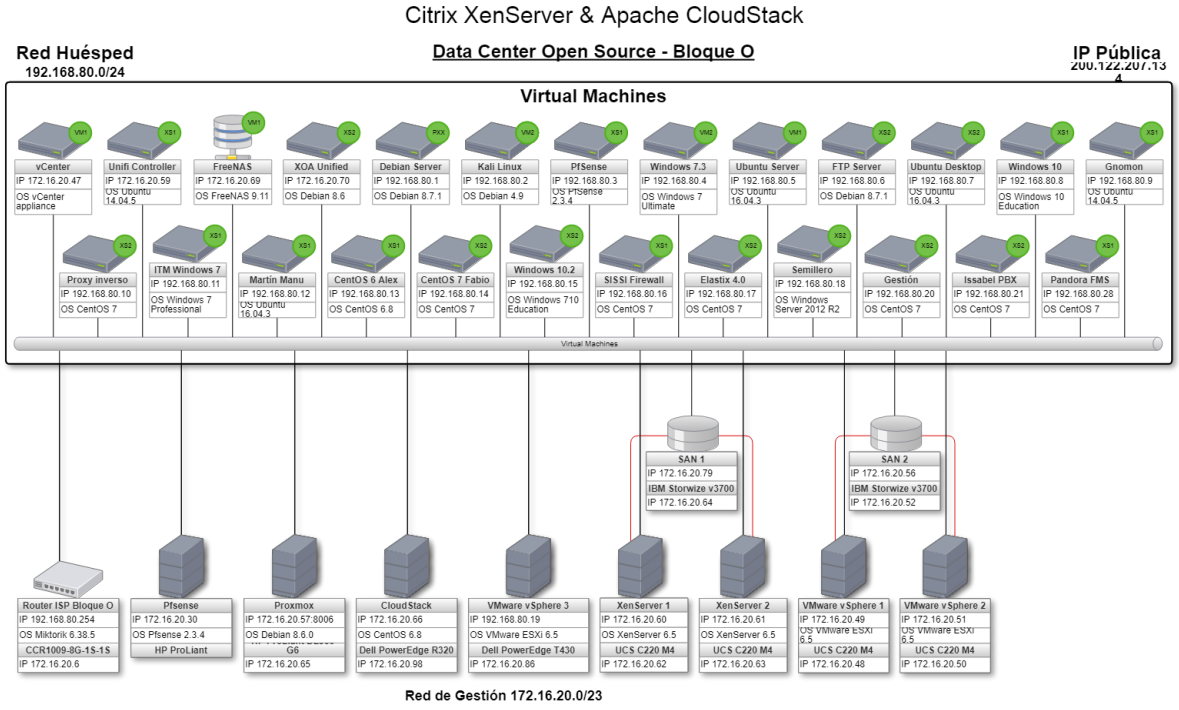


Ilustración 8. DataCenter servidores Laboratorio de Redes Convergentes Bloque O (Elaboración propia).

Topología del laboratorio de redes convergentes

El diseño de la red del laboratorio de redes convergentes corresponde a una topología tipo Estrella. En este tipo de topologías todas las máquinas están conectadas a un concentrador o hub desde el cual se re-direccionan los datos al computador adecuado.

Si las funciones de hub las realiza un dispositivo con muchos puertos, corresponde a una topología *estrella pasiva*, por el contrario si la función del hub la realiza una computadora que regenera la señal y la envíe a su destino es una topología *estrella activa* en la cual muchas veces estas computadoras cumplen funciones como servidores y realizan labores estadísticas.

Para el caso del laboratorio de redes convergentes se concluye que la topología es estrella pasiva ya que las funciones de hub son realizadas por el Router de borde ISP Bloque O el cual tiene como dirección IP 192.168.80.254 y sistema operativo Mikrotik 6.41.1.

Ventajas topología estrella

- Tiene los medios para prevenir problemas
- Si una máquina se desconecta o se daña el cable solo queda fuera de la red esa máquina.
- Fácil de agregar y reconfigurar la arquitectura de las máquinas.
- Fácil de prevenir daños o conflictos.
- Permite que todos los nodos se comuniquen entre sí de una manera conveniente.
- El mantenimiento resulta más económico y fácil que otros tipos de topología.

Desventajas topología estrella

- Si el nodo central falla, toda la red se desconecta.
- Es costosa, ya que requiere más cable que las topologías bus o anillo.
- El cable viaja por separado del hub a cada computadora.

Cobertura

La cobertura del laboratorio de redes convergentes corresponde a una red LAN que tiene cobertura en el bloque O de la sede Fraternidad del ITM.

Arquitectura

El laboratorio de redes convergentes esta tiene una arquitectura definida por las siguientes características:

- Red guiada bajo el estándar 802.3 ethernet con tecnología HFC (hibrid fiber Coaxial), cada tarjeta de red con capacidades de ancho de banda de 10, 100 y 1000 Mbps.
- Protocolos IPV4 – IPV6.
- Cableado RJ45 categoría 5E el cual permite un ancho de banda de 1GB.

Identificación de los dispositivos del laboratorio y servicios que gestionan

En este sentido se detalla cada uno de los servidores con su dirección IP, nombre y breve descripción de los servicios que contienen:

Tabla 5. *Servidores del Laboratorio de Redes Convergentes Bloque O. (Elaboración propia)*

Nombre Servidor	IP Servidor	Descripción del Servidor
FTP Server	192.168.80.6	Es un servidor Linux FTP, tiene el puerto 22 abierto (Gestión), adicionalmente tiene un servicio FTP dejando abiertos dos puertos el puerto 21 que es el puerto de control y el 20 que es el puerto de datos (Este abre cuando se está recibiendo información, si el servicio FTP es activo. Si el servicio está configurado como pasivo se debe conocer el rango de puertos dinámicos, debido a que cuando se realiza la conexión con el servidor se define aleatoriamente un puerto para datos). Se utiliza el protocolo FTP, acrónimo de "File Transfer Protocol", es un protocolo de transferencia de archivos a través de la red entre sistemas conectados a través de conexiones TCP. Este protocolo se basa en una arquitectura cliente-servidor, donde el cliente solicita acceso al servidor y, una vez garantizado, le permite descargar o subir archivos a él.

Gnomon	192.168.80.9	Es un servidor Linux que almacena una página web, tiene el puerto 22 abierto (Gestión), también se encuentra un servidor web por el puerto 80 que contiene la página grupo de investigación de Matemáticas (GNOMON); el puerto 161 se encuentra abierto ya que desde allí se monitorea el estado del servidor, los demás están cerrados debido a que no tienen servicios asociados.
Proxy Inverso	192.168.80.10	Es un servidor Linux que almacena una página web, tiene el puerto 22 abierto (Gestión). El comportamiento del servidor es redirigir el trafico http según las reglas que tengan configura.
ITM Windows	192.168.80.11	Es un servidor Windows orientado a las VPN, tiene abiertos los puertos 3389 (Escritorio Remoto), el 161 por ser puerto de monitoreo del servidor, el 500 porque es un servicio de VPN remota y 4500 debido a que es un servicio VPN.
Martin UdeA	192.168.80.12	Es un servidor Linux que almacena una página web, tiene el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página Manuela Castrillón.
Centos6	192.168.80.13	Es un servidor Linux que almacena una página web, tiene el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de Apache 2 Test Page.
Centos7	192.168.80.14	Es un servidor Linux que almacena una página web, tiene el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de HTTP Web Example.
Elastix 2.5	192.168.80.16	Es un servidor Linux orientado a telefonía, tiene el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de HTTP y el puerto 443 contiene la página de HTTPS, el puerto 5060 por donde funciona los teléfonos, el puerto 123 es para la sincronización de reloj entre los teléfonos y el servidor y el puerto 69 para descargar versiones a los teléfonos debido a que el servidor es un servidor de telefonía.
Elastix 4	192.168.80.17	Es un servidor Linux orientado a telefonía, tiene el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de HTTP y el puerto 443 contiene la página de HTTPS, el puerto 68 para asignaciones de direcciones IP dinámicas, el puerto 69 para descargar versiones a los teléfonos y el puerto 5060 por donde funciona los teléfonos.
Semillero	192.168.80.18	Es un servidor Windows, tiene el puerto 3389 abierto (Escritorio Remoto), tiene un servidor que es un controlador de dominio.
Hyper-V Server	192.168.80.19 hypervserver.ingeitm.local	Es un servidor Windows utilizando como hipervisor tiene el puerto 3389 abierto (Escritorio Remoto).
Daniel Jimenez	192.168.80.20	Es un servidor Linux, tiene abierto el puerto 22 abierto (Gestión).
Windows 7	192.168.80.21	Es un servidor Windows de VPN, tiene abiertos el puerto 3389 (Escritorio Remoto), el puerto 500 y 161 de monitoreo.
Windows 7,2	192.168.80.111	Es un servidor Windows, tiene abierto los puertos 3389 (Escritorio Remoto), el puerto 135 y 445 de carpetas compartidas.

Load Balancer	192.168.80.23	Es un servidor Linux, tiene el puerto 22 abierto (Gestión)
UCS C220 M4	172.16.20.48	Es un servidor de directorios, tiene abierto los puertos 389, el puerto 443 por protocolo HTTPS y 161 por monitoreo.
UCS C220 M4	172.16.20.50	Es un servidor de directorios tiene abiertos los puertos 389, el puerto 443 por protocolo HTTPS y 161 por monitoreo.
SAN 2	172.16.20.56	Es un servidor de almacenamiento
Proxmox	172.16.20.57	Es un servidor hipervisor, tiene abierto por defecto el puerto que usa Proxmox es el 8006.
UCS C220 M4	172.16.20.62	Es un servidor de directorios, tiene abiertos los puertos 389, el puerto 443 por protocolo HTTPS y 161 por monitoreo.
UCS C220 M4	172.16.20.63	Es un servidor de directorios, tiene abiertos los puertos 389, el puerto 443 por protocolo HTTPS y 161 por monitoreo.
HP ProLiant DL360 G6	172.16.20.65	Es un servidor físico, y no se sabe su contenido por lo tanto se deja abierto el puerto de monitoreo
CloudStack web	172.16.20.66	Encargada de coordinar de manera centralizada el aprovisionamiento automático de capacidades de cómputos y sus dependencias (almacenamiento, redes y sistemas operativos).
SAN 2	172.16.20.79	Es un sistema de almacenamiento tiene el puerto 161 abierto de monitoreo.
Dell PowerEdge R320	172.16.20.98	Es un sistema de almacenamiento tiene abierto el puerto 161 de monitoreo.
VMware vCenter Server Appliance	172.16.20.47	VM para administrar el hipervisor Vmware vSphere
Web Server	172.16.20.59	VM donde se alojan libros para los estudiantes
FreeNAS	172.16.20.69	VM para alojamiento de ISOs y demás archivos, es un sistema de almacenamiento.
Xen Orchestra Web	172.16.20.70	VM para administrar el hipervisor XenServer.
(LAN) Pfsense-Pfsense 2.3.4	192.168.80.3	VM de trabajo de grado de Firewall.
Windows 7.3 - Windows 7 Ultimate	192.168.80.4	VM de pruebas.
Ubuntu Desktop 16.04.3	192.168.80.7	Ubuntu Desktop para administración.
Windows 10.2-Windows 10 Education	192.168.80.15	VM de pruebas para el firewall PfSense.
Pandora FMS - CentOS 7	192.168.80.28	VM para monitoreo de toda la infraestructura.
SAN1 XenServer-	172.16.20.64	Almacenamiento de todas las máquinas virtuales en la red, tiene el puerto 161 abierto de monitoreo.

IBM Storwize v3700		
SAN2 Vmware- IBM Storwize v3700	172.16.20.52	Almacenamiento de todas las máquinas virtuales en la red, tiene el puerto 161 abierto de monitoreo.
Router Mikrotik	192.168.80.254	Router de borde de la red del bloque O (el que da acceso a Internet)
Proxmox VE- Ubuntu 16.04	172.16.20.57:8006	Servidor físico donde se encuentra instalado Proxmox VE
HyperV- HyperV Server 2012 R2	192.168.80.19	Hypervisor Windows
XenServer 1- Citrix XenServer	172.16.20.60	Servidor físico donde se encuentra instalado XenServer
XenServer 1- Citrix XenServer	172.16.20.61	Servidor físico donde se encuentra instalado XenServer
VMware vSphere 1- VMware ESXi 6.5	172.16.20.49	Servidor físico donde se encuentra instalado Vmware vSphere
VMware vSphere 2- VMware ESXi 6.5	172.16.20.51	Servidor físico donde se encuentra instalado Vmware vSphere

Dispositivos del laboratorio de redes convergentes a monitorear

En la tabla anterior se identifican detalladamente los dispositivos de red del laboratorio, más sin embargo, los servidores web y el router de borde del bloque O por sus características y servicios que se exponen en la web los hace más vulnerable a ataques maliciosos, por tal motivo estos son considerados como dispositivos de red a monitorear para este proyectos como tal. A continuación, se detallan estos dispositivos:

Tabla 6. *Servidores críticos a monitorear. (Elaboración propia)*

Nombre Servidor	IP Servidor	Sistema Operativo	Descripción del Servidor	Impacto
VMware vCenter Server Appliance	172.16.20.47	vCenter appliance	VM para administrar el hipervisor Vmware vSphere	Estas máquinas virtuales exponen servicios a internet, por lo tanto, se encuentran expuestas a alto tráfico y por ende son más vulnerables a

FreeNAS	172.16.20.69	FreeNAS 9.11	VM para alojamiento de ISOs y demás archivos, es un sistema de almacenamiento.	posibles ataques maliciosos. Al realizar correlación de eventos en estas máquinas se puede identificar aquellos puntos vulnerables y tomar medidas de mitigación que garanticen una mayor protección de estas.
Xen Orchestra Web	172.16.20.70	Debian 8.6	VM para administrar el hipervisor XenServer	
(LAN) Pfsense-Pfsense 2.3.4	192.168.80.3	PfSense 2.4.1	VM de trabajo de grado de Firewall	
Windows 7.3 - Windows 7 Ultimate	192.168.80.4	Centos 7	VM de pruebas	
Gnomon	192.168.80.9	Ubuntu 14.04.5	Servidor Linux que almacena una página web, así como un servidor web por el puerto 80 que contiene la página grupo de investigación de Matemáticas (GNOMON)	
Martin UdeA	192.168.80.12	Ubuntu 16.04.3	Servidor Linux que almacena una página web, así como un servidor web por el puerto 80 que contiene la página Manuela Castrillón.	
Windows 10.2-Windows 10 Education	192.168.80.15	Centos 7	VM de pruebas para el firewall PfSense	
GitLab	192.168.80.25	Centos 7		
Ubuntu IPv6	192.168.80.26	Ubuntu 16.04.3		
Windows server 2012	192.168.80.18	Windows 2012		
Router ISP	192.168.80.254	Mikrotik 6.41.1	Router de borde de la red del bloque O (el que da acceso a Internet)	

3.2. Fase de diseño

Mecanismos para la gestión de logs

De los mecanismos vistos en el marco teórico se elige Rsyslog como el mecanismo para transmitir los logs a Ossim, debido a sus múltiples características para gestionar logs y la practicidad en su implementación, por lo cual a continuación se detalla sus características y funcionalidades principales:

Rsyslog

Rsyslog Es un sistema para el procesamiento de registros syslog, recibe entradas de una amplia variedad de fuentes, las transforma y genera resultados para diversos destinos. Puede entregar más de un millón de mensajes por segundo a destinos locales cuando se aplica un procesamiento limitado. Incluso con destinos remotos y un procesamiento más elaborado.

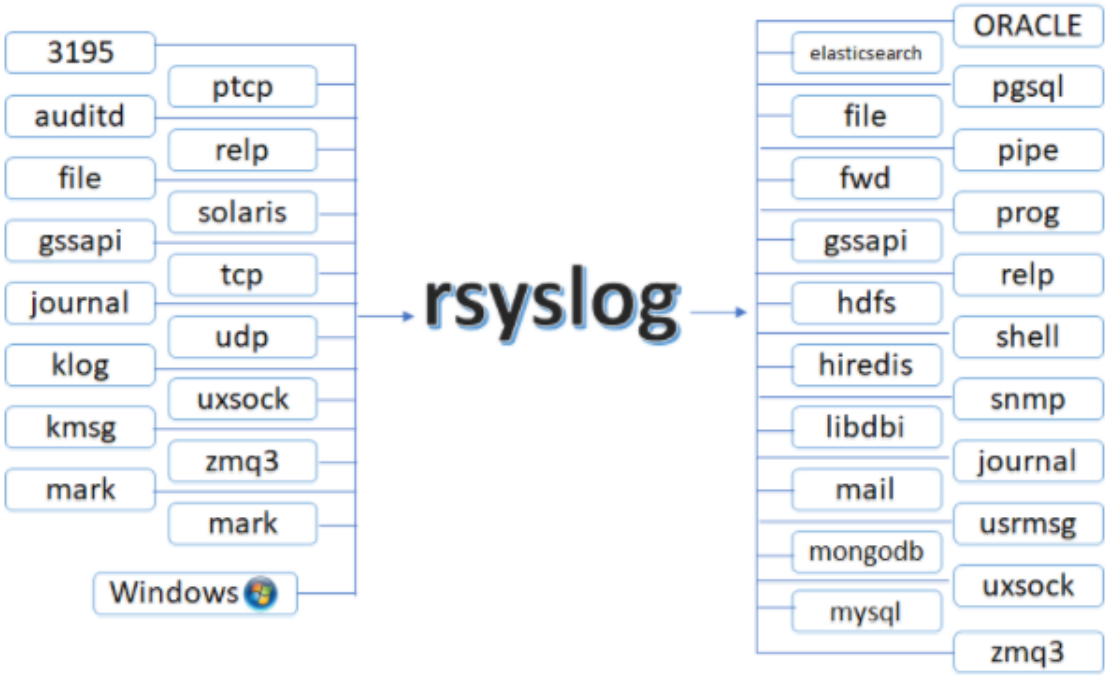


Ilustración 9. Entradas y salidas de Rsyslog *(RSYSLOG, 2018)*

Rsyslog se ha convertido en estándar de la mayoría de distribuciones Linux. Uno de sus objetivos es admitir una gran cantidad de mensajes por segundo.

¿Qué es Syslog?

Syslog es un protocolo en el que los dispositivos de red envían mensajes de eventos a un servidor de registro, generalmente conocido como servidor Syslog. El protocolo Syslog es compatible con una amplia gama de dispositivos y se puede utilizar para registrar diferentes tipos de eventos. Syslog es una excelente forma de consolidar registros de múltiples fuentes en una única ubicación.

Los mensajes de Syslog generalmente incluyen información para ayudar a identificar información básica sobre dónde, cuándo y por qué se envió el registro: dirección IP, marca de tiempo y el mensaje de registro real.

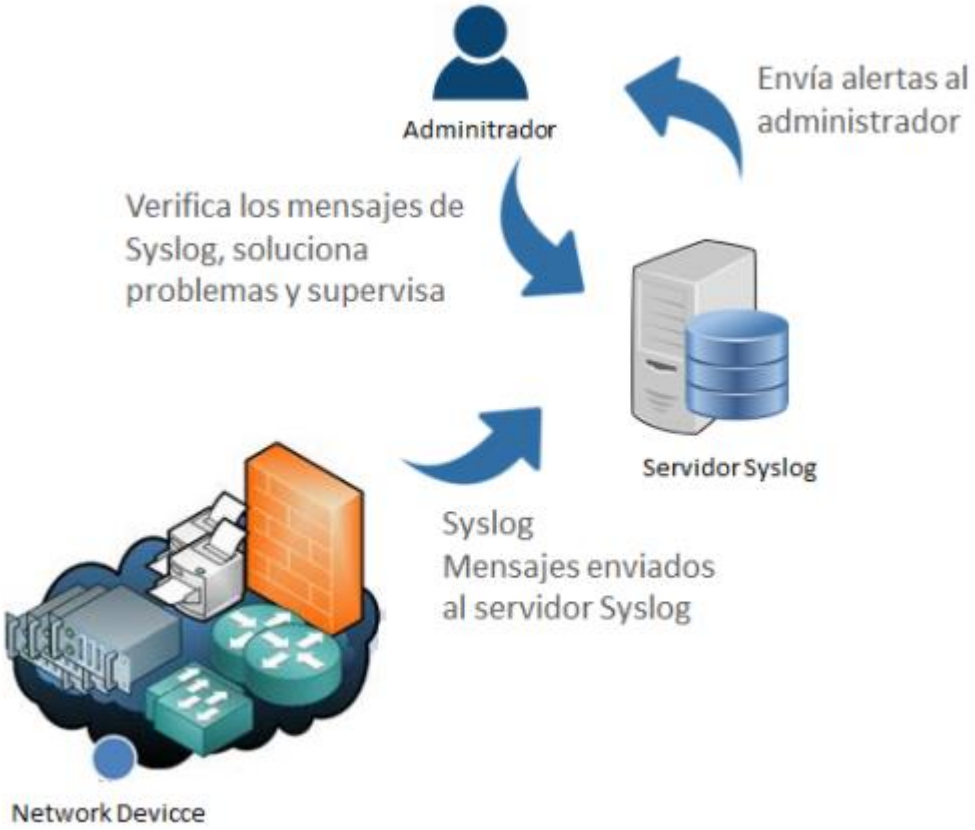


Ilustración 10. Funcionamiento de SYSLOG *(Network Management Software, 2018)*

Rsyslog y OSSIM

OSSIM utiliza rsyslog ya que es una implementación de syslog en la herramienta que se encuentra predeterminada para la recolección de logs desde dispositivos externos. Una apropiada configuración de syslog en OSSIM es concluyente para la recopilación de logs porque los pluggins detectores de OSSIM esperan que los logs de dispositivos externos estén en ubicaciones predestinadas para recopilar los datos de las máquinas correctamente.

Comparativo Herramientas de correlación de eventos SIEM

A continuación, se muestra un cuadro comparativo con diferentes herramientas SIEM open Source donde se exponen varias características y sistemas operativos soportados comparando el comportamiento de cada herramienta en estas variables:

Tabla 7. *Herramientas de correlación de eventos SIEM open source. (Elaboración propia basado en (Avella Colorado, Calderón Barrios, & Mateus Díaz, 2015))*

Tipo	Característica	OSSEC	OSSIM	GRAYLOG	LOGALYZE	SIEMONSTER
Características	Descubrimiento de Activos		X			
	Gestión Centralizada	X	X	X	X	X
	Recolección de logs y eventos de seguridad	X	X	X	X	X
	Correlación de Eventos	X	X		X	X
	Análisis de Logs	X	X	X	X	X
	Clasificación y Prioridad de eventos	X	X		X	X
	Monitoreo en tiempo Real	X	X	X	X	X
	Normalización	X	X	X	X	X
	Reportes	X	X	X	X	X
	Interfaz Gráfica de administración	X	X	X	X	X
	Modo de recolección de Eventos	Agente/Sin agente	Agente/Sin agente	Agente	Agente/Sin agente	Agente/Sin agente
Sistema Operativo Soportado	LINUX/UNIX	X	X	X	X	X
	MAC	X	X			

	BSD	X	X			
	WINDOWS	X	X		X	X

Herramienta de correlación de eventos OSSIM

Luego de evaluar diferentes herramientas de soluciones SIEM, se llegó a la conclusión de trabajar con OSSIM de Alienvalult la cual trabaja con licencia open source y es la más completa en componentes que se pueden aprovechar para las necesidades del Laboratorio de Redes Convergentes del Bloque O.

OSSIM, Son las siglas de Open Source Security Information Management en inglés, es un SIEM creado por la empresa Española AlienVault. Es una herramienta muy completa para recopilación, normalización y correlación de eventos de seguridad. Su principal objetivo es proporcionar una herramienta SIEM de uso libre, debido a la falta de productos de código abierto disponibles en el mercado.

Alienvault ha adicionado una infraestructura robusta de colección, motor de correlación, evaluación de riesgos, reportes y herramientas de administración que son muy impresionantes. El resultado es una plataforma cohesiva que ofrece abstracción de datos y permite monitorear eventos.

Arquitectura OSSIM

En la siguiente gráfica se detalla la arquitectura de OSSIM y sus componentes principales:

Ilustración 11. Arquitectura de OSSIM *(ALIEN VAULT, 2018)*

A continuación, se explica la Arquitectura de OSSIM

Interfaz de Usuario: medio con que el usuario puede comunicarse con la máquina

Administrador: Usuario encargado de monitorear la herramienta

Modo de Correlación

- **Agregación**: soluciones para administración de logs desde muchas fuentes.
- **Correlación:** busca los atributos comunes, y relaciona eventos en paquetes o incidentes.
- **Priorización:** Priorización de eventos de acuerdo a las necesidades de mitigación de riesgo.

Colector de Eventos: Recolecta los eventos de seguridad de las máquinas.

OSSIM proporciona una plataforma unificada con muchas de las capacidades de seguridad esenciales, como:

- Descubrimiento de activos
- Evaluación de vulnerabilidad
- Detección de intrusos
- Control del comportamiento
- SIEM
- Panel de Control
- Gestión de Eventos
- Reglas de Seguridad

Topología OSSIM

La topología seleccionada es una topología Estrella activa donde OSSIM cumple las veces de concentrador o hub recibiendo los logs de todos los dispositivos habilitados para enviar sus logs a la plataforma para ser analizados y relacionados.

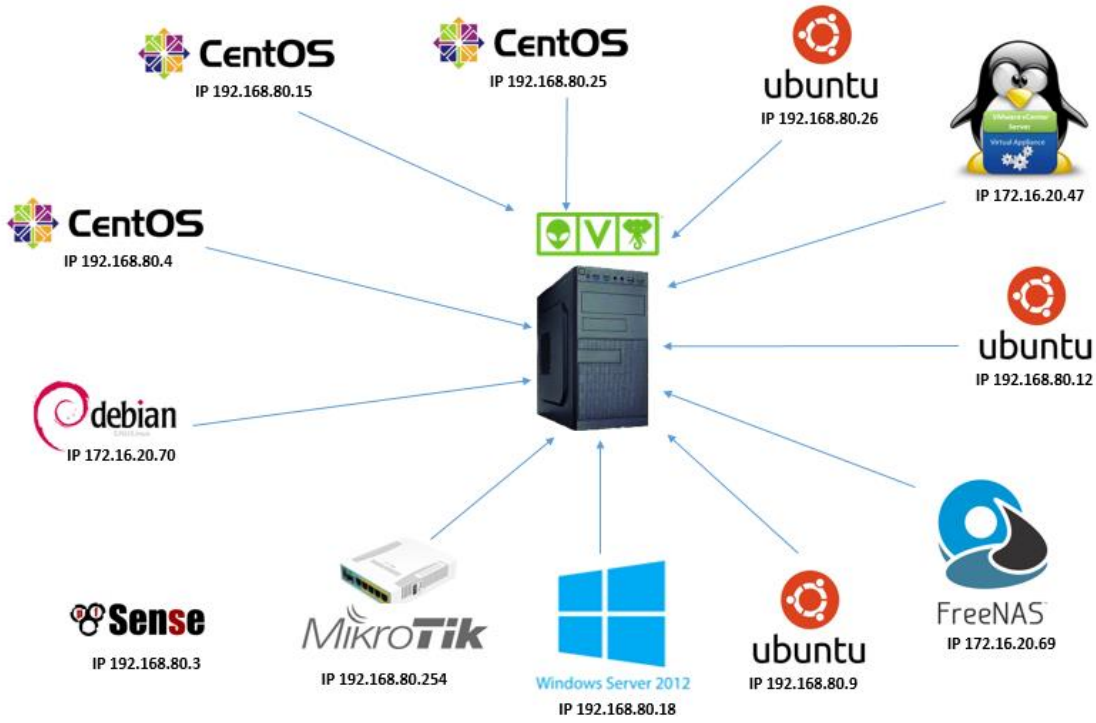


Ilustración 12. Topología implementación OSSIM (Elaboración propia).

Reglas de correlación de eventos en los dispositivos a monitorear

OSSIM tiene la funcionalidad de crear reglas de correlación para filtrar eventos, activar notificaciones que ayuden a mejorar el rendimiento de OSSIM y convertir políticas de seguridad en prácticas de seguridad en la red. Lo anterior da gran capacidad de realizar análisis a aquellos eventos que son más críticos en la red sin tener que revisar cada evento.

Para el desarrollo de este proyecto se implementaron dos políticas de seguridad que buscan detectar cuando suceden eventos que requieren de más atención.

1. **Intento de acceso fallido a PfSense:** según el monitoreo de evento y la correlación de OSSIM, el pfsense del laboratorio es uno de los servidores que más eventos recibe, esta regla proporciona información a los administradores de posibles ataques por intrusos a pfsense.

2. **Escaneo de puertos:** con esta política se busca que OSSIM pueda mostrar un ticket cada vez que se realiza un escaneo de puertos a algún dispositivo de la red. En el APENDICE C se puede ver la configuración de una política.

3.3. Fase de implementación

Instalación y configuración de herramienta SIEM AlientVault OSSIM

El software utilizado y que se eligió previamente se puede descargar desde la página web https://www.alienvault.com/products/ossim

Se preparó una máquina virtual con las siguientes especificaciones requeridas para el correcto funcionamiento:
200GB de DD,
8GB de memoria RAM.

Instalación de OSSIM

Se realizó la instalación de la herramienta SIEM seleccionada para la correlación de eventos la cual es OSSIM, esta herramienta se instaló en una máquina virtual y se accede desde la plataforma web, ver Apéndice A para más detalle de la instalación.

Configuración de OSSIM

Después de ser instalado en la máquina virtual y realizar las configuraciones necesarias, se debe acceder a la plataforma web a través de la IP configurada en la instalación https://192.168.80.29 y realizar las configuraciones iniciales necesarias, donde se indica un usuario y password para

acceder a la plataforma web así como el nombre, correo electrónico y compañía, finalmente se puede acceder a todas las características que ofrece OSSIM.

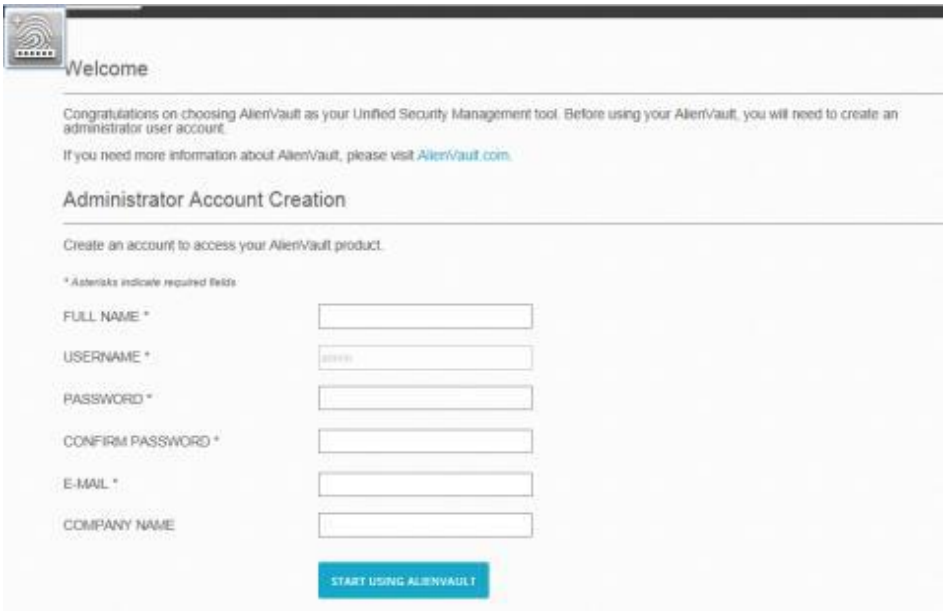


Ilustración 13. Despliegue de OSSIM desde plataforma web (Elaboración propia).

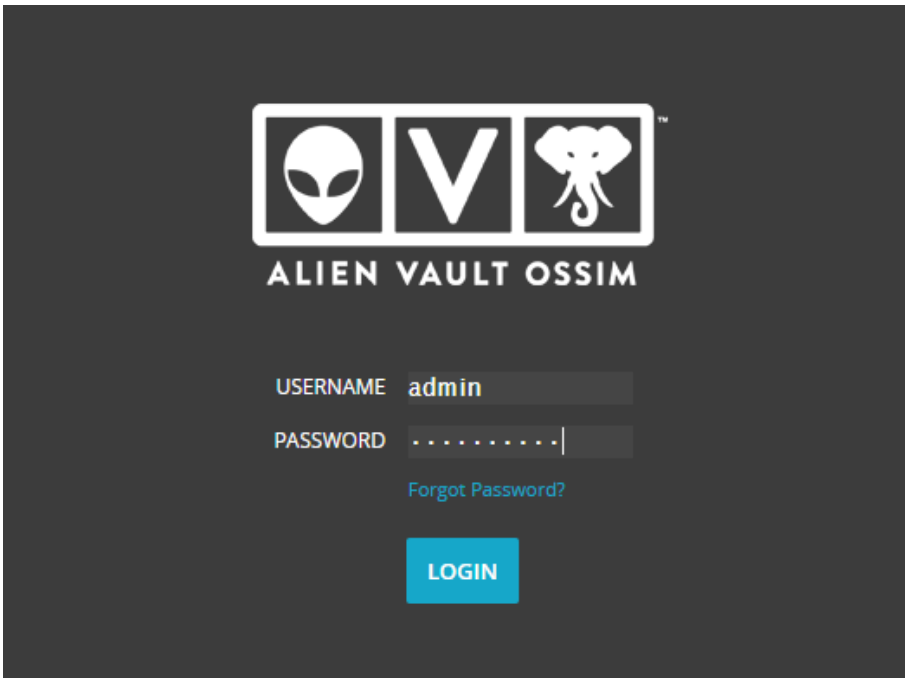


Ilustración 14. Acceso a plataforma web de OSSIM (Elaboración propia).

Configuración de parámetros en dispositivos a monitorear

Habilitar rsyslog en los dispositivos a monitorear para el envío de logs hacia AlienVault OSSIM. Este procedimiento requiere revisar la configuración de Rsyslog en cada servidor ya que esta varía según la configuración del fabricante. En el Apéndice B se encuentra Configuración de los parámetros requeridos en los dispositivos a monitorear.

Implementar de reglas de correlación de eventos en los dispositivos a monitorear

Para el desarrollo de este proyecto se implementan dos políticas de seguridad que buscan detectar cuando suceden eventos que requieren de más atención.

- **Intento de acceso fallido a PfSense:** En el Apéndice C se puede ver la configuración de la política.

- **Escaneo de puertos:** En el Apéndice C se puede ver la configuración de la política.

4. RESULTADOS Y DISCUSIÓN

4.1. ATAQUES CONTROLADOS

Para evaluar el comportamiento y resultado de la herramienta implementada, se generan un par de ataques controlados dentro de la red, a continuación se detalla el comportamiento en cada uno de ellos:

4.1.1. Escaneo de puertos

Se realizó escaneo de puertos con Nmap a PFSENSE con dirección IP 192.168.80.3, desde una maquina Centos 7 la cual tiene dirección IP 192.168.80.16

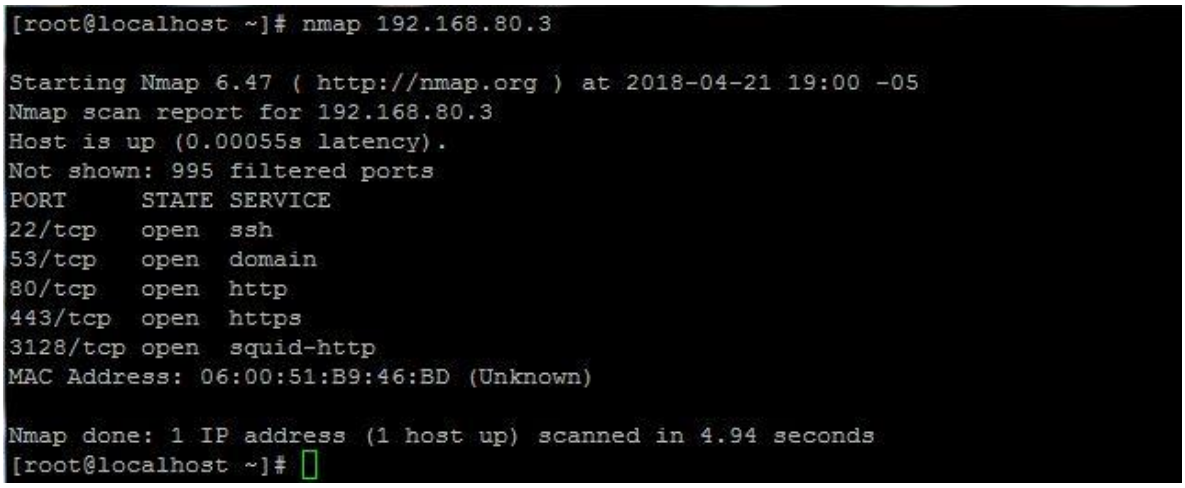


Ilustración 15. Escaneo de puertos (Elaboración propia).

Como respuesta se puede ver que OSSIM reconoce este escaneo de puertos en su almacenamiento de logs, como se puede ver en las siguientes imágenes:

En la imagen 16 podemos ver la respuesta de Ossim desde la plataforma web, mientras que en la imagen 17 se puede ver el registro del log generado por este escaneo de puertos desde la consola bash de Ossim.

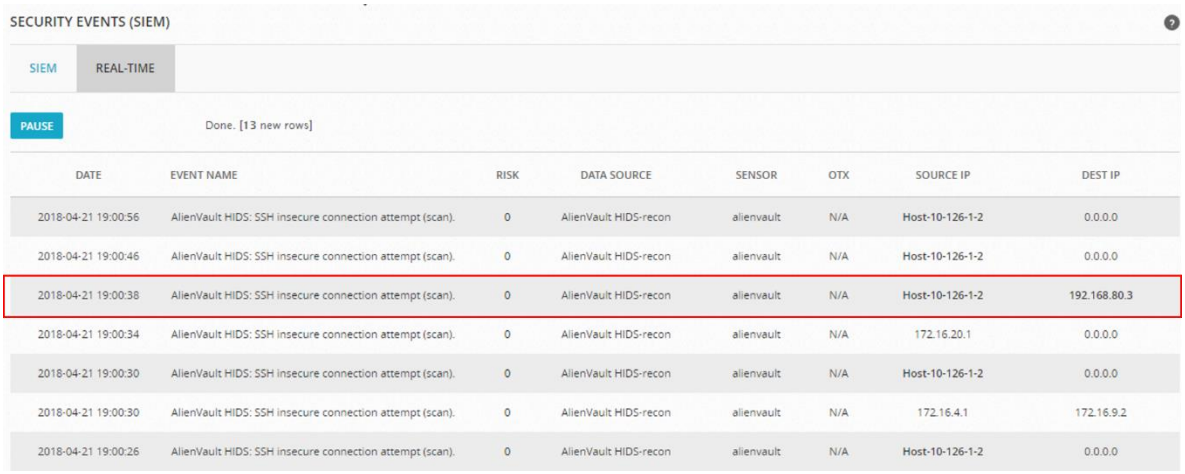


Ilustración 16. Respuesta en Ossim de escaneo de puertos (Elaboración propia).

```
alienvault:~# tcpdump -i eth0 udp port 514
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:00:25.778081 IP 172.16.9.2.syslog > alienvault.alienvault.syslog: SYSLOG loca
l0.info, length: 125
19:00:28.312839 IP 172.16.9.2.syslog > alienvault.alienvault.syslog: SYSLOG loca
l7.info, length: 94
19:00:28.403309 IP 172.16.9.2.syslog > alienvault.alienvault.syslog: SYSLOG auth
.info, length: 86
19:00:28.584930 IP 192.168.80.3.syslog > alienvault.alienvault.syslog: SYSLOG lo
cal5.info, length: 123
```

Ilustración 17. Respuesta desde consola Ossim a escaneo de puertos (Elaboración propia).

4.1.2. Autenticación fallida

Se realizaron intentos fallidos de ingreso a la plataforma web de PfSense la cual tiene dirección IP 192.168.80.3

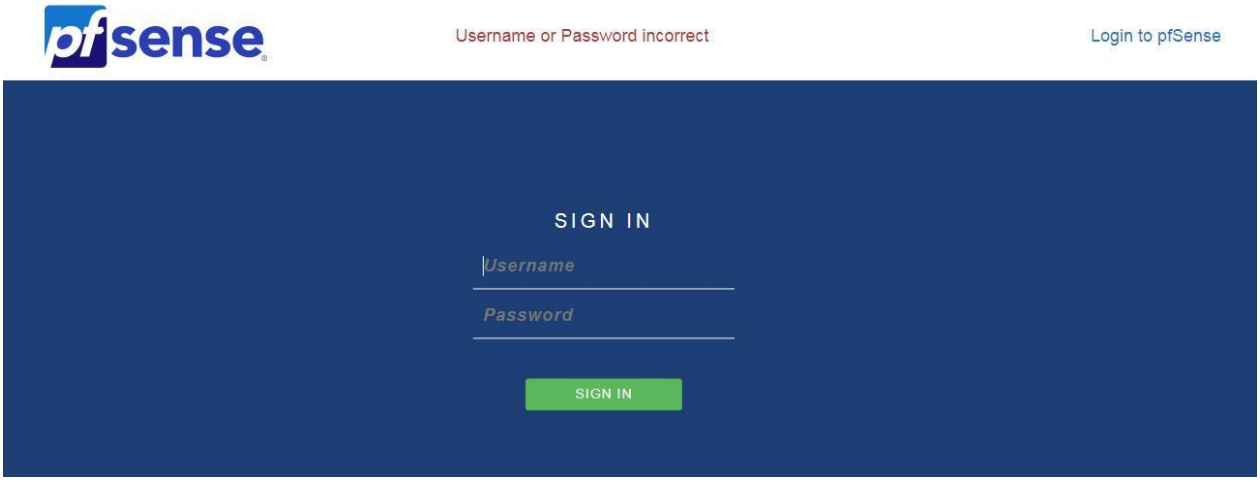
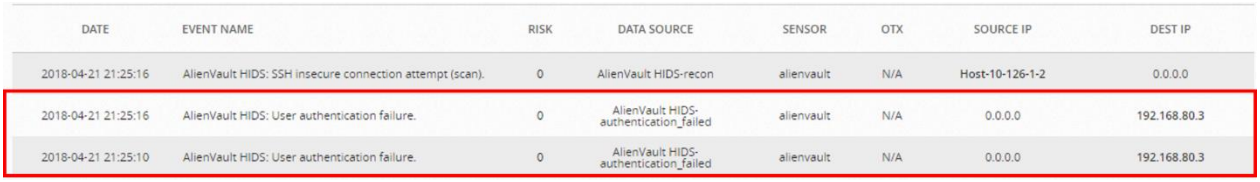


Ilustración 18. Intento de acceso fallido a PfSense (Elaboración propia).

Se logra identificar desde la plataforma web OSSIM reconoce estos intentos fallidos al PfSense, como se muestra en la siguiente imagen:



DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	OTX	SOURCE IP	DEST IP
2018-04-21 21:25:16	AlienVault HIDS: SSH insecure connection attempt (scan).	0	AlienVault HIDS-recon	alienvault	N/A	Host-10-126-1-2	0.0.0.0
2018-04-21 21:25:16	AlienVault HIDS: User authentication failure.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	0.0.0.0	192.168.80.3
2018-04-21 21:25:10	AlienVault HIDS: User authentication failure.	0	AlienVault HIDS-authentication_failed	alienvault	N/A	0.0.0.0	192.168.80.3

Ilustración 19. Log de intento fallido a PfSense en Ossim (Elaboración propia).

4.2. Correlación de eventos

Como resultado a las reglas creadas anteriormente se evidencia que al realizar un intento fallido al pfSense, automáticamente se genera un ticket reportando este evento:

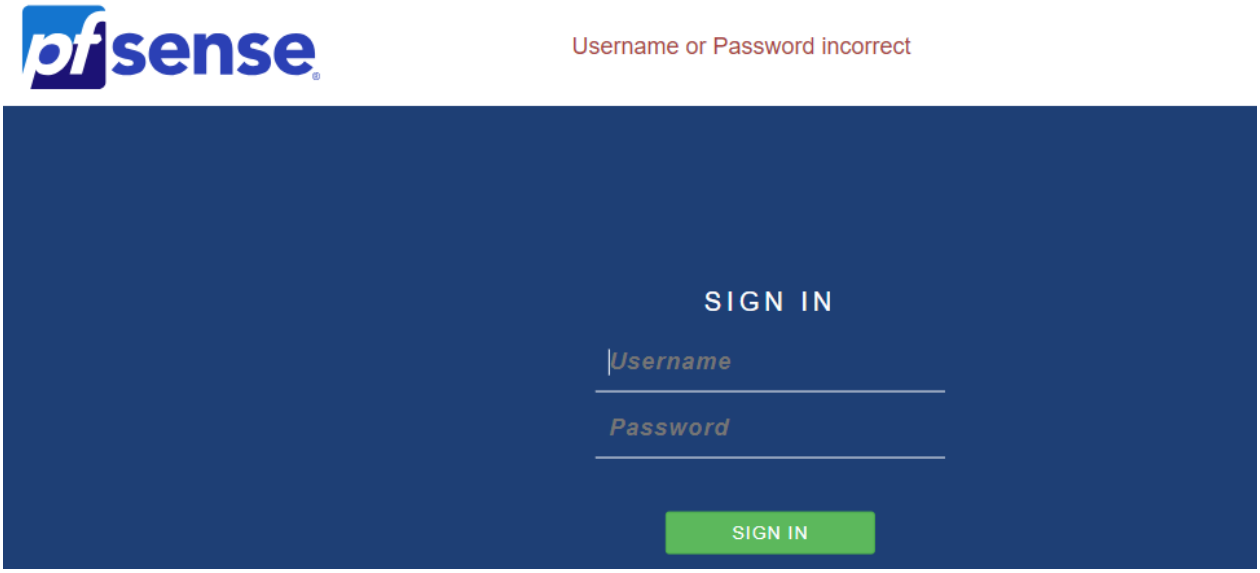


Ilustración 20. Acceso fallido a PfSense (Elaboración propia).

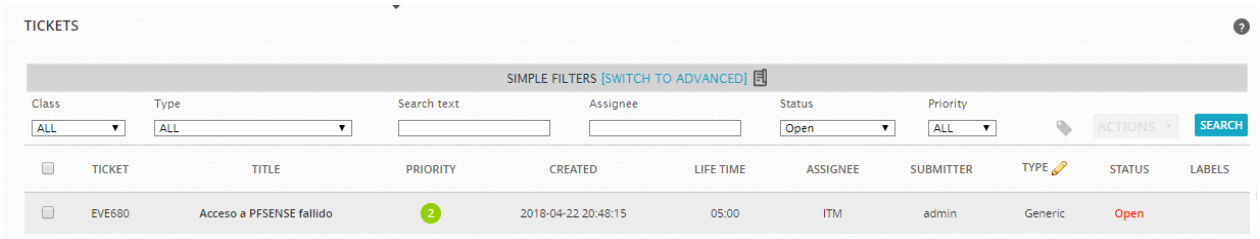


Ilustración 21. Ticket en Ossim de intento acceso fallido a PfSense (Elaboración propia).

En el mismo sentido cuando se realizó un escaneo de puertos desde la máquina IP 192.168.80.16 a la máquina Centos 192.168.80.15 se generó inmediatamente un ticket reportando este evento:

```
[root@localhost ~]# nmap -sS 192.168.80.15

Starting Nmap 6.47 ( http://nmap.org ) at 2018-04-22 20:53 -05
Nmap scan report for 192.168.80.15
Host is up (0.00012s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql
8089/tcp open  unknown
MAC Address: D2:53:E7:C4:D4:42 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Ilustración 22. Escaneo de puertos (Elaboración propia).

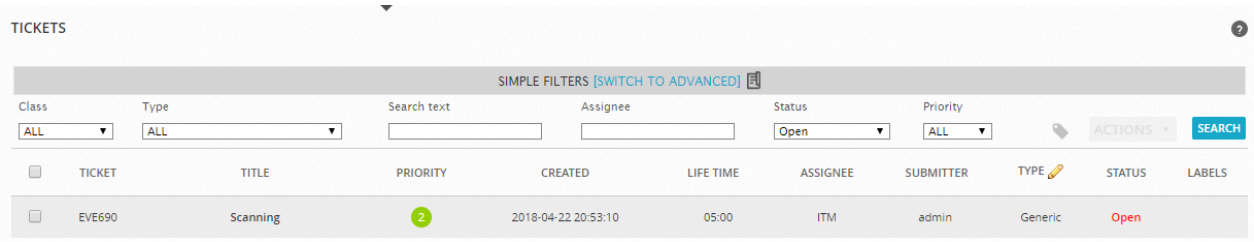


Ilustración 23. Ticket en Ossim de escaneo de puertos (Elaboración propia).

Ossim tipifica los tickets según el motivo de ocurrencia y genera estadísticas con esta información, a continuación se puede evidenciar que el 99% de los tickets generados son de tipo Genérico y el 1% que corresponde a 1 evento es un ticket de tipo Anomalías:

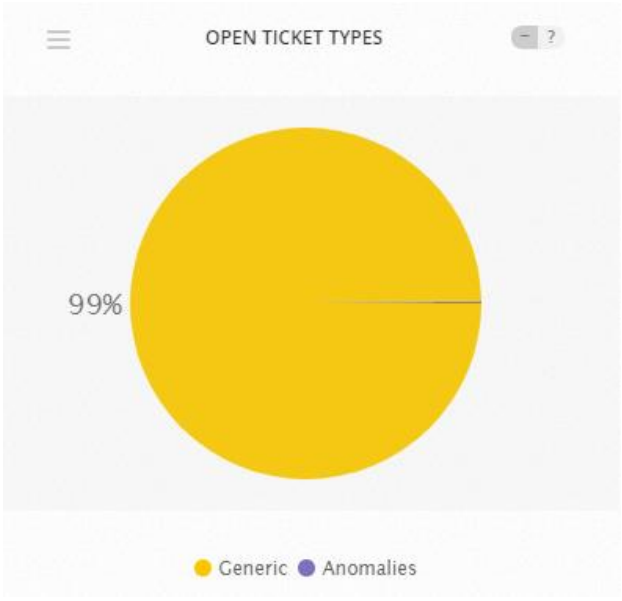


Ilustración 24. Tickets por tipo en Ossim (Elaboración propia).

4.3. Captura de tráfico

En la siguiente imagen se puede evidenciar el flujo de tráfico del día Abril 22 de 2018 en todos los protocolos, donde se observó que las horas de mayor tráfico son aproximadamente desde las 10am a las 18pm

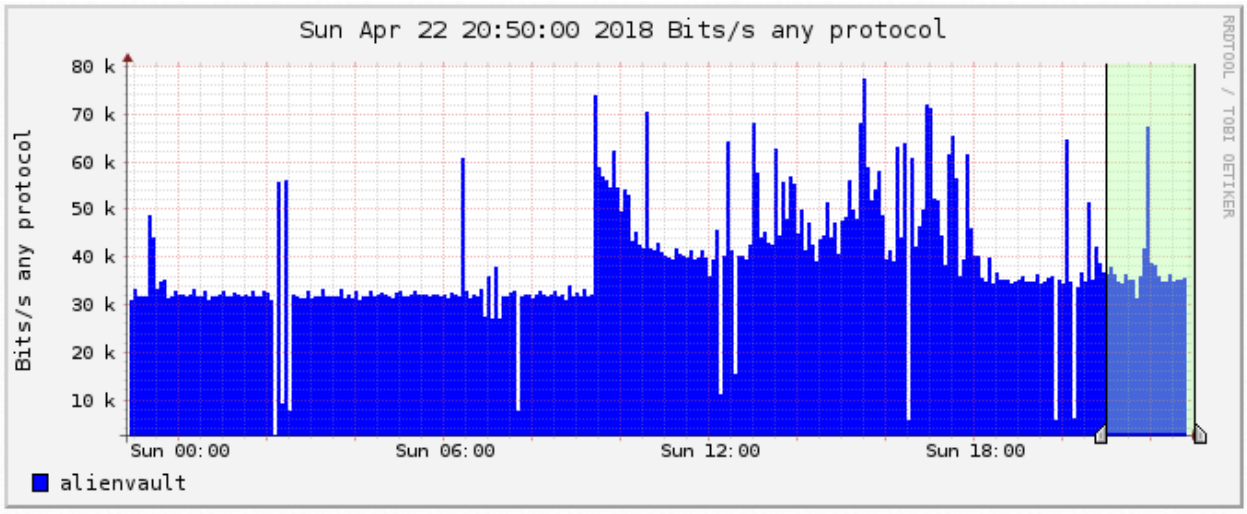
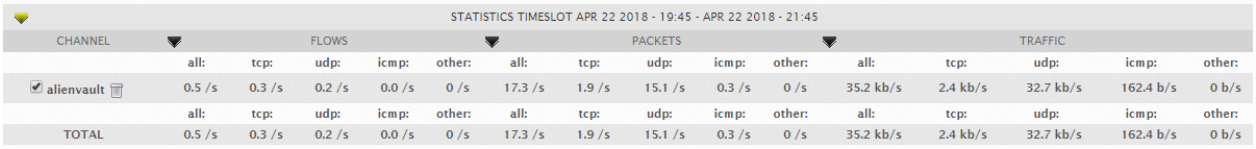


Ilustración 25. Tráfico en Ossim de todos los protocolos (Elaboración propia).

En la siguiente imagen tomada de la plataforma web de Ossim se muestra el tráfico por protocolo, en esta se puede evidenciar que el protocolo ICMP presenta el mayor tráfico en la red con 157,8 b/s, seguido de protocolo UDP con 33.8 b/s.



STATISTICS TIMESLOT APR 22 2018 - 19:45 - APR 22 2018 - 21:45

CHANNEL	FLOWS					PACKETS					TRAFFIC				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
alienvault	0.5 /s	0.3 /s	0.2 /s	0.0 /s	0 /s	17.3 /s	1.9 /s	15.1 /s	0.3 /s	0 /s	35.2 kb/s	2.4 kb/s	32.7 kb/s	162.4 b/s	0 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	0.5 /s	0.3 /s	0.2 /s	0.0 /s	0 /s	17.3 /s	1.9 /s	15.1 /s	0.3 /s	0 /s	35.2 kb/s	2.4 kb/s	32.7 kb/s	162.4 b/s	0 b/s

Ilustración 26. Tráfico en Ossim por protocolo (Elaboración propia).

4.4. Revisión y monitoreo de eventos

Se revisaron los eventos durante un periodo de un mes utilizando la consola de administración de OSSIM y los reportes de correlación de eventos SIEM, esto ayudó para definir reglas de correlación y alertas. Luego de la correlación se puede observar un resumen de diversos aspectos de seguridad y otros estados, actividades y eventos que ocurren en la red. A continuación, se muestran los resultados.

En el siguiente grafico se muestra el top 10 de categorías de evento que más se presentaron en los servidores web del laboratorio, el 57% son eventos de reconocimiento, el 41 % son de autenticación y un porcentaje menor son alertas.

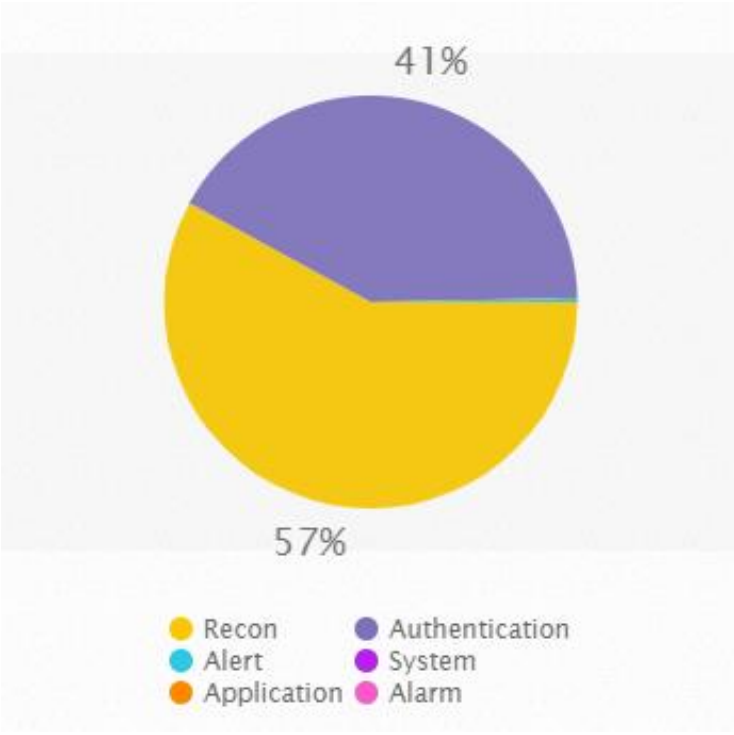


Ilustración 27. Gráfico Top 10 categorías de eventos (Elaboración propia).

En el siguiente gráfico se pueden ver los eventos por sensor u origen de datos, el sensor que más eventos detectó fue Alienvault HIDS.

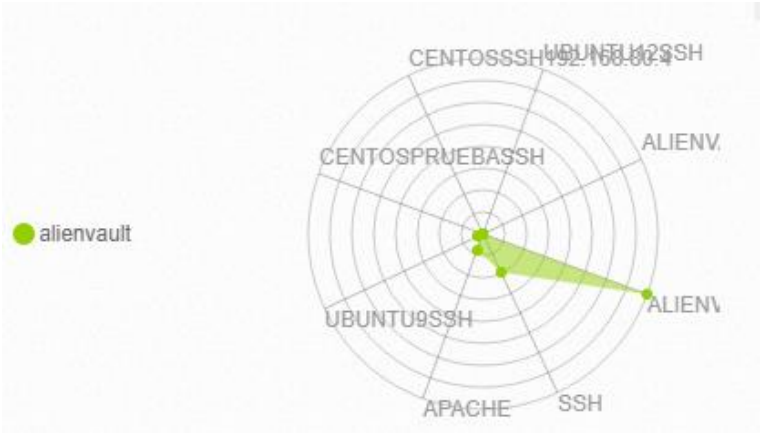


Ilustración 28. Eventos por sensor u origen de datos (Elaboración propia).

El siguiente gráfico muestra el top 5 de los eventos qué más se presentan en la red

AlienVault HIDS: SSH insecure connection attempt (scan): 64809

SSHd: Did not receive identification string

AlienVault HIDS: Login session opened. 27.506

AlienVault HIDS: Loin session closed. (27.191)

Apache: Moved Temporarily. 11.363

Los ataques que más se presentan en los servidores web del laboratorio son de intento de conexión inseguro por medio de SSH e inicio y cierre de sesión.

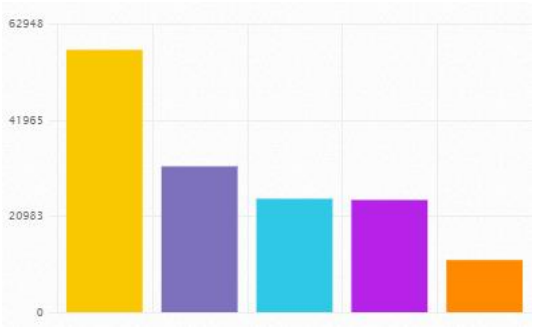


Ilustración 29. Eventos por tipo de protocolo (Elaboración propia).

En el siguiente gráfico se hace un comparativo de los inicios de sesión exitosos y fallidos, en el resultado se puede ver que en el 99% de los casos los inicios de sesión son exitosos

Ilustración 30. Eventos por Login exitoso vs Login fallido (Elaboración propia).

Top 10 host atacante, aquí se muestran los 10 host que más envían solicitudes para acceder a los servidores web del laboratorio.

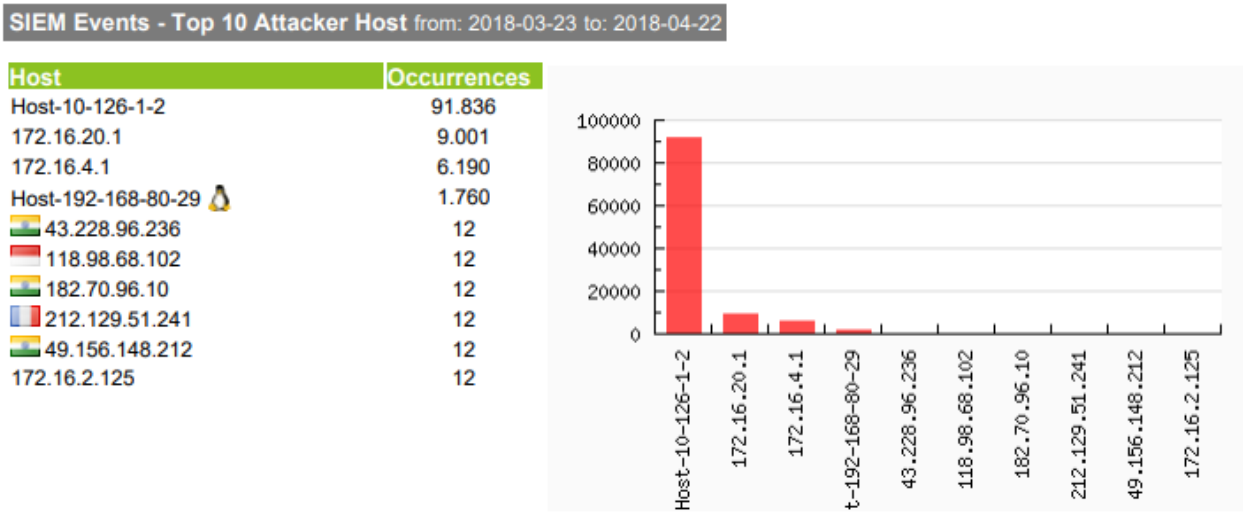


Ilustración 31. Top 10 host atacante (Elaboración propia).

Top 10 de host atacados, aquí se muestra el top 10 de los servidores web del laboratorio que son más atacados desde el exterior, donde se evidencia una gran cantidad de ocurrencias al PfSense con dirección IP 192.168.80.3

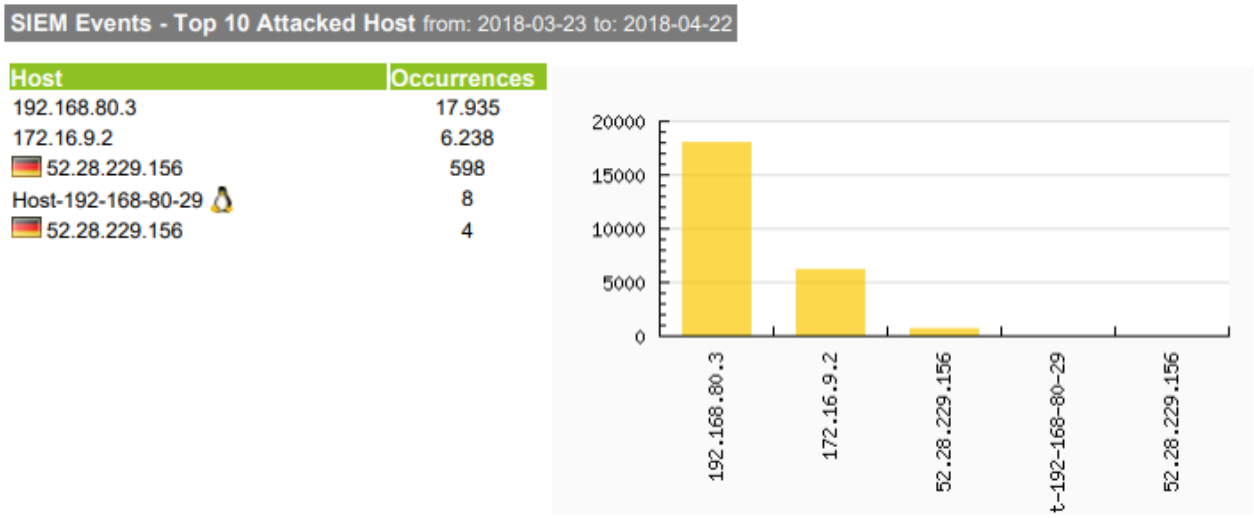


Ilustración 32. Top 10 de host atacados (Elaboración propia).

Top 10 puertos usados, aquí se muestran los puertos más usados en los servidores web del laboratorio y estos son el 22 ssh, el 80 http y el 443 https.

SIEM Events - Top 10 Used Ports from: 2018-03-23 to: 2018-04-22

Port	Service	Occurrences
22	ssh	32.799
80	http	602
443	https	4

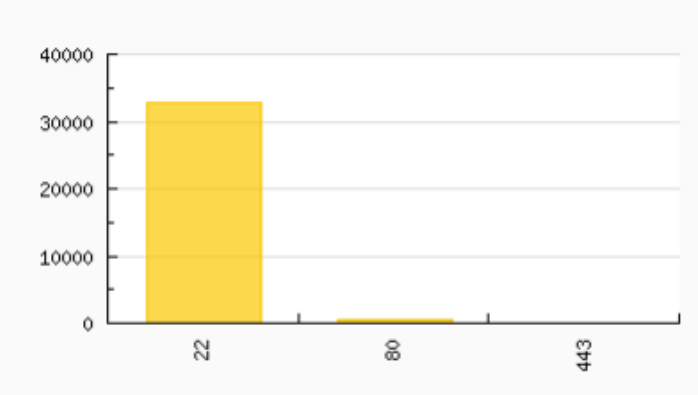


Ilustración 33. Top 10 puertos usados (Elaboración propia).

Top 15 de eventos de último mes, se evidencia que los eventos de mayor ocurrencia son los de Ssh-scan con un 39 %, seguido de sesión abierta con un 16,8% y en un tercer lugar en ocurrencia se encuentra los eventos de cierre de sesión con un 16,6%

SIEM Events - Top 15 Events from: 2018-03-23 to: 2018-04-22

Event	Occurrences
AlienVault HIDS: SSH insecure connection attempt (scan).	65.055
AlienVault HIDS: Login session opened.	27.543
AlienVault HIDS: Login session closed.	27.229
SSHd: Did not receive identification string	26.167
Apache: Moved Temporarily	11.363
SSHd: Did not receive identification string	3.176
SSHd: Did not receive identification string	864
SSHd: Did not receive identification string	795
SSHd: Did not receive identification string	794
AlienVault NIDS: "ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management"	598
SSHd: Connection closed	529
AlienVault HIDS: Successful sudo to ROOT executed	319
SSHd: Failed password	144
SSHd: Received disconnect	136
AlienVault HIDS: User successfully changed UID.	105

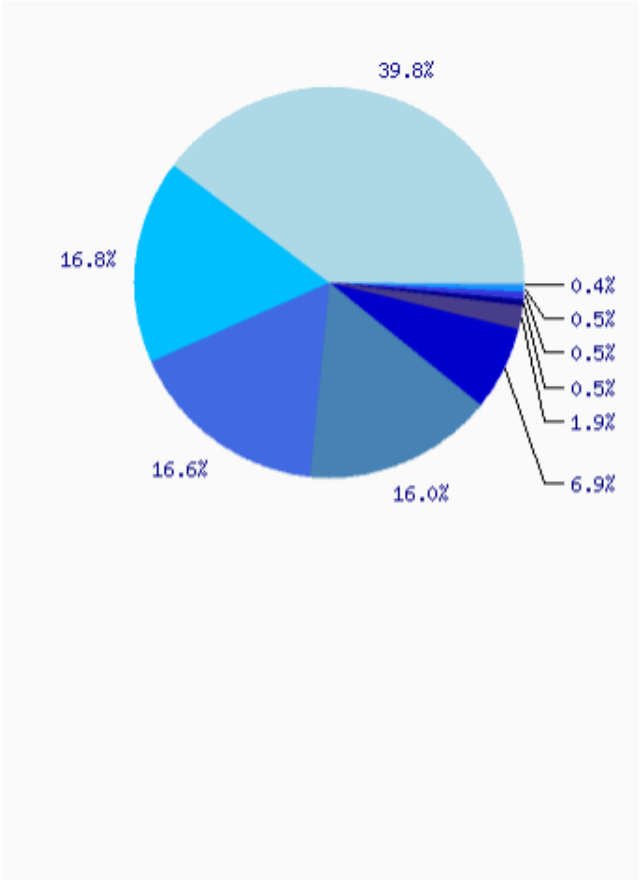


Ilustración 34. Top 15 eventos (Elaboración propia).

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

5.1. CONCLUSIONES

Pequeñas, medianas y grandes empresas en la actualidad que gestionan redes de información, necesitan tener sus datos y dispositivos seguros en la medida de lo posible, lo que hace necesario implementar herramientas que ayuden a detectar donde puede estar en riesgo la red y así poder tomar medidas que ayuden a prevenir y mitigar posibles riesgos.

Es así como desde la revisión teórica y análisis de diferentes herramientas de gestión, se identificó que la implementación de un correlacionador de eventos es una medida que beneficia a las empresas al ayudar a gestionar los eventos de seguridad que a diario se generan en los dispositivos y que no es posible revisar detallada e independientemente.

Se puede pensar que con herramientas de seguridad como antivirus y firewalls se encuentra la integridad y la información de la red totalmente segura, pero estas solo contienen información de los sucesos que han detectado, no hay un antes y después del evento. Los correlacionadores de eventos SIEM suelen ser de vital importancia para una detección verdadera a tiempo y poder implementar acciones que mantengan la red totalmente segura.

SIEM es una capa de gestión por encima de los controles de seguridad. Conecta y unifica la información contenida en los servidores existentes, lo que permite analizar los eventos desde una sola interfaz. Se puede proteger la información de la red, el sistema y su comportamiento ya que el SIEM tiene un práctico sistema que ayuda a realizar detecciones efectivas, análisis y respuestas en las operaciones de seguridad

En este sentido se cumple con los objetivos planteados al implementar una herramienta SIEM en el laboratorio de redes convergentes del ITM, donde se logró demostrar su efectividad en la correlación de eventos de seguridad.

El uso de una herramienta SIEM hace parte fundamental en una arquitectura de gestión de eventos, proporcionando información valiosa de una forma sencilla para analizar y diagnosticar, esto ofrece un valor de seguridad de la información por su rapidez y practicidad en la automatización de eventos logrando identificar fácilmente los impactos en la infraestructura.

5.2. RECOMENDACIONES

Se recomienda un amplio conocimiento del funcionamiento, conectividad, arquitectura y topología del lugar donde se desee implementar un correlacionador de eventos, lo cual es fundamental para obtener los resultados que se esperan de una herramienta SIEM.

5.3. TRABAJOS FUTUROS

A partir del trabajo realizado donde no se logró implementar una gran cantidad de reglas de correlación se sugiere un trabajo futuro donde se realice un detallado análisis de las vulnerabilidades presentadas en el laboratorio de redes convergentes del ITM y se implementen reglas de correlación de acuerdo a las necesidades presentadas, realizando seguimiento periódico a los resultados arrojados por el SIEM.

Un futuro trabajo es implementar un correlacionador de eventos con base en la metodología propuesta en el presente trabajo en un ambiente industrial, con una mayor cantidad de dispositivos a monitorear, evaluando la respuesta de la herramienta OSSIM en cuanto a capacidad y funcionalidad.

REFERENCIAS

Alertlogic. (s.f.). *Alertlogic*. Obtenido de Alertlogic: https://www.alertlogic.com/assets/log-manager/Log-Management-Best-Practices.pdf

ALIEN VAULT. (2018). Obtenido de https://www.alienvault.com/products/ossim

Alonso-Alegre Díez, M. B. (2016). *Gestión de Logs.*

Avella Colorado, J. D., Calderón Barrios, L. F., & Mateus Díaz, C. A. (2015). *Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM.*

Franco, D. A., Perea, J., & Puello, P. (2012). Metodología para la detección de vulnerabilidades en redes de datos. *Información Tecnologica*.

Ipswitch. (s.f.). *ipswitch*. Obtenido de ipswitch: https://www.ipswitch.com/resources/best-practices/log-management-compliance-for-the-healthcare-industry

Kelly M. Kavanagh, O. R. (10 de Agosto de 2016). *Gartner*. Obtenido de McCafee: https://www.gartner.com/doc/reprints?id=1-3C43L7Q&ct=160721&st=sb

Logalyze. (04 de 2018). *Logalyze*. Obtenido de Logalyze: http://www.logalyze.com/

Network Management Software. (2018). Obtenido de Network Management Software: https://www.networkmanagementsoftware.com/what-is-syslog/

NIÑO MEJIA, D. C., & SIERRA MUNERA, A. (2007). *METODOLÓGICA PARA LA GESTIÓN CENTRALIZADA DE REGISTRO DE EVENTOS DE SEGURIDAD EN PYMES.*

Polanco, M. (2010). Arquitectura de eventos de seguridad. *Magazcitum*.

RSYSLOG. (2018). Obtenido de RSYSLOG: https://www.rsyslog.com/

SeguridadX. (Enero de 2013). Obtenido de https://www.seguridadx.com/que-es-un-siem-que-es-prelude-siem/

Sekharan, S. S., & Kamalanathan Kandasamy. (2018). Profiling SIEM tools and correlation engines for security analytics. *IEEE*, (pág. 5). Chennai, India.

Sofistic. (s.f.). Obtenido de https://www.sofistic.com/productos/security-information-and-event-management-siem/

Swift, D. (2010). *Successful SIEM and log management strategies for audit and compliance. SANS Institute InfoSec Reading Room.*

Xailna. (s.f.). Obtenido de http://www.xailna.com/index.php/log-analysis?_sm_au_=iVVsVS7WfHZqT1tq

APÉNDICE

Apéndice A: Instalación de OSSIM

1. Seleccionar la opción de instalación “Install Alient Vault USM”

Ilustración 35 Instalación de OSSIM (Elaboración propia).

2. Seleccionar el lenguaje, localización y parámetros regionales

Ilustración 36 Instalación OSSIM – Lenguaje (Elaboración propia).

Ilustración 37. Instalación Ossim – Ubicación (Elaboración propia).

Ilustración 38 Instalación OSSIM – Ubicación (Elaboración propia).

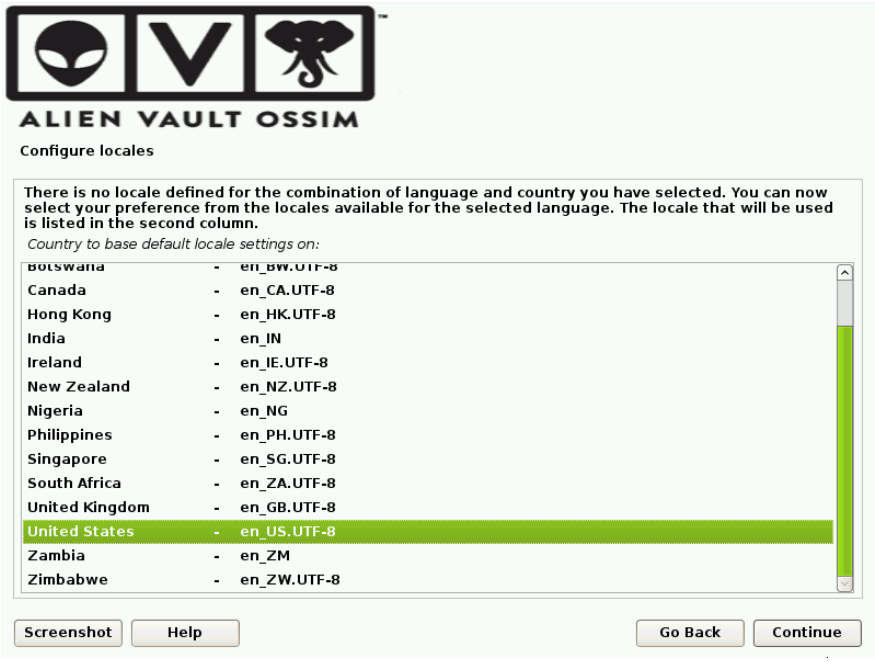


Ilustración 39. Instalación OSSIM - Parámetros regionales (Elaboración propia).

3. Seleccionar el tipo de teclado

Ilustración 40. Instalación OSSIM - Tipo teclado (Elaboración propia).

4. Configurar los valores de dirección IP, Máscara de red y Gateway

Ilustración 41. Instalación OSSIM - Dirección IP (Elaboración propia).

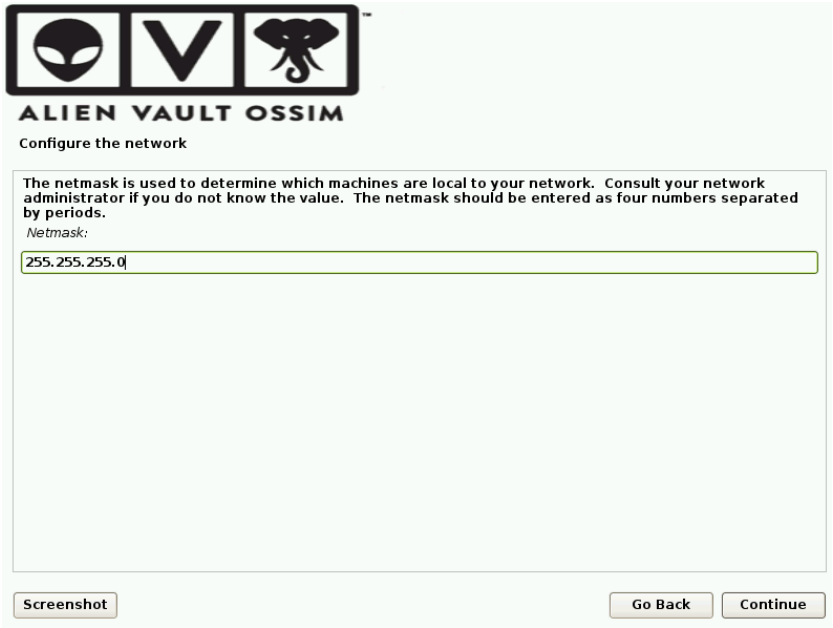


Ilustración 42. Instalación OSSIM - Configuración mascara de red (Elaboración propia).

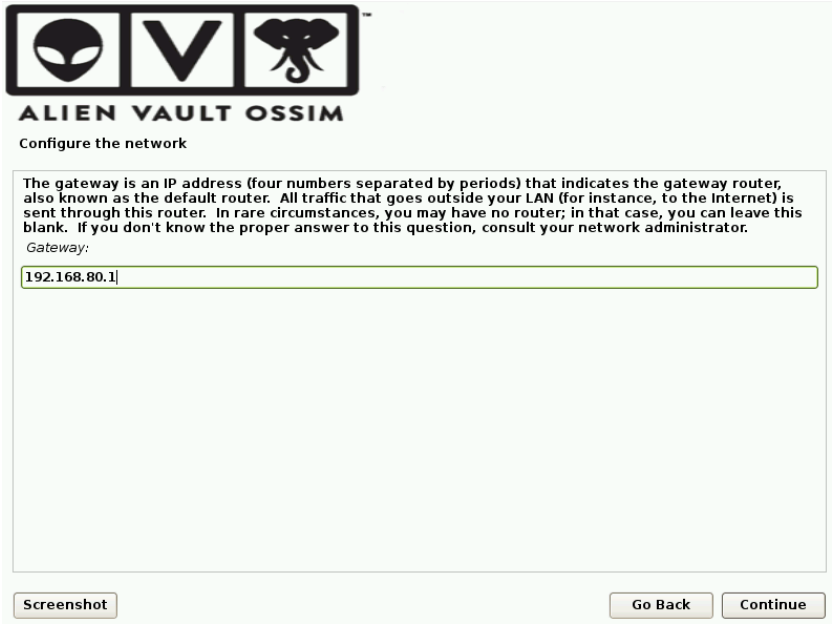


Ilustración. Instalación OSSIM - Configuración Gateway (Elaboración propia).

5. Establecer la contraseña para el usuario Root

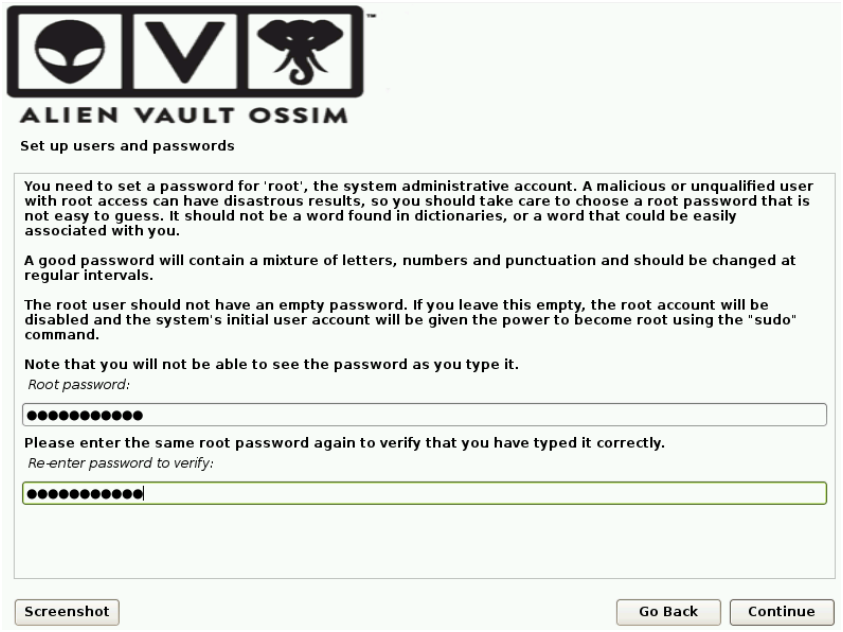


Ilustración 43. Instalación OSSIM – Contraseña (Elaboración propia).

6. Inicio de la instalación

Ilustración 44. Instalación de OSSIM – Configuraciones (Elaboración propia).

7. Luego de finalizada la instalación, se ingresa por consola y se configuran los parámetros:

   - Definir servidor para relay de correos, para las notificaciones de SIEM

   - Configuración del sensor IDS y plugins de origen de datos

   - Definir los CIDRs de redes

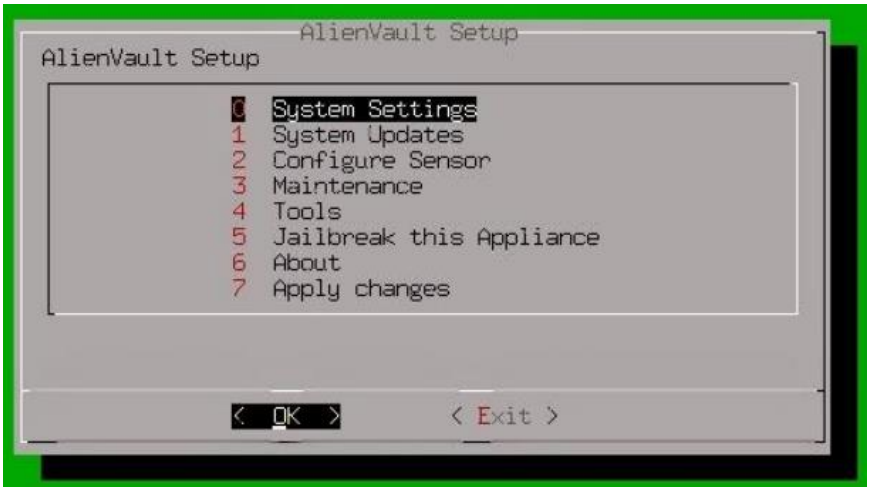


Ilustración 45. Configuración Alient Vault (Elaboración propia).

Apéndice B: Configuración de rsyslog para el envió de logs

Configuración en Linux

1. El daemon de Rsyslog se instala automáticamente en la mayoría de las distribuciones de Linux. Sin embargo, si Rsyslog no está instalado en su sistema, puede emitir uno de los siguientes comandos para instalar el servicio, necesitará privilegios de administrador para ejecutar los comandos.
   - En las distribuciones basadas en Debian:

     Sudo apt- get install rsyslog

   - En las distribuciones basadas en RHEL como CentOS:
     Sudo yum install rsyslog

2. Para verificar si el daemon Rsyslog se inicia en un sistema, ejecute los siguientes comandos, según su versión de distribución.

   - En las distribuciones de Linux más nuevas con systemd:
     systemctl status rsyslog.service

   - En versiones anteriores de Linux con init:
     service rsyslog start o /etc/init.d/rsyslog start

3. Para iniciar el demonio rsyslog, emita el siguiente comando.

   - En versiones anteriores de Linux con init:
     service rsyslog start o /etc/init.d/rsyslog start
   - En las últimas distribuciones de Linux:
     systemctl start rsyslog.service

4. Luego de tener RSYSLOG instalado crear un archivo llamado alienvault.conf en la ruta /etc/rsyslog.d

```
[root@localhost ~]# cd /etc/rsyslog.d
[root@localhost rsyslog.d]# nano alienvault.conf
```

Ilustración 46. Configuración RSYSLOG (Elaboración propia).

5. Poner en el archivo el siguiente texto en el archivo que creamos: *.* @192.168.80.29

```
 GNU nano 2.3.1            File: alienvault.conf

*.* @192.168.80.29
```

Ilustración 47. Configuración de IP de OSSIM en RSYSLOG (Elaboración propia).

6. Finalmente se reinicia Rsyslog, para aplicar los cambios realizados al archivo de configuración, a continuación, se encuentran las instrucciones que aplican según el tipo de versión de Linux

   sudo service rsyslog restart o sudo systemctl restart rsyslog

Configuración en Windows server 2012

Se requiere instalar un agente que envíe los logs hasta Alienvault OSSIM, se puede utilizar diferentes opciones como por ejemplo Datagram SyslogAgent, Correlog Windows Agent o Snare Epilog for Windows. En la realización de este proyecto se utiliza el Correlog Windwos Agent el cual se puede descargar de la página web https://correlog.com/distributed-security-solutions/correlog-agent-windows/

Seguidamente se pide un registro con los datos básicos

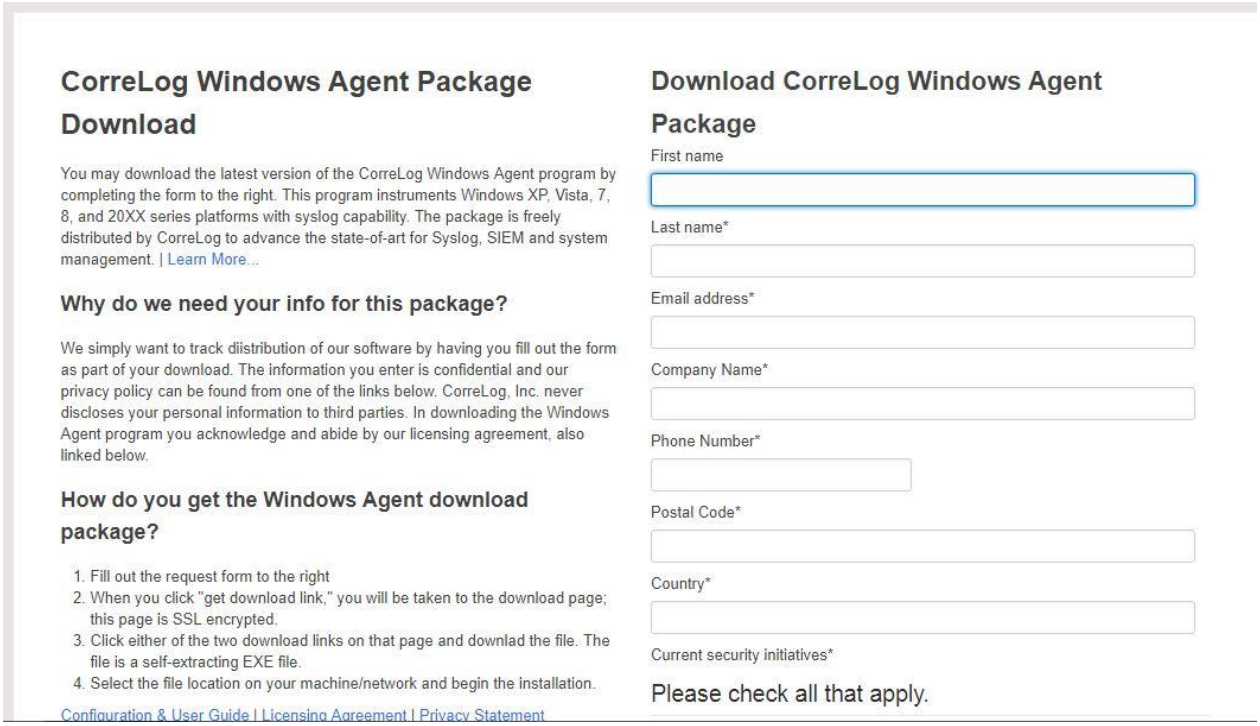


Ilustración 48. Configuración de cuenta Correlog (Elaboración propia).

Se inicia la instalación

Ilustración 49. Inicio instalación Correlog (Elaboración propia).

Y en la instalación se configura el servidor al cual se desean enviar los logs

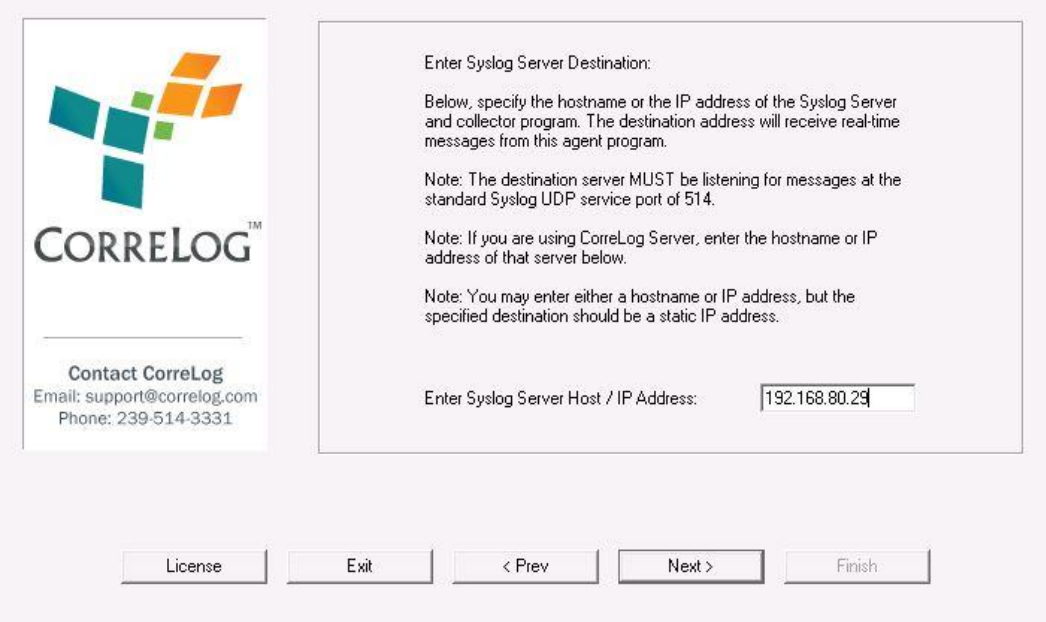


Ilustración 50. Configuración servidor Ossim en Correlog (Elaboración propia).

Apéndice C: Creación de reglas de correlación

1. Se crea una acción para la política que se creará posteriormente, en esta se define el nombre de la acción, una descripción y que tipo de acción generará, lo cual puede ser abrir un ticket, enviar un mensaje por email o ejecutar un programa externo:

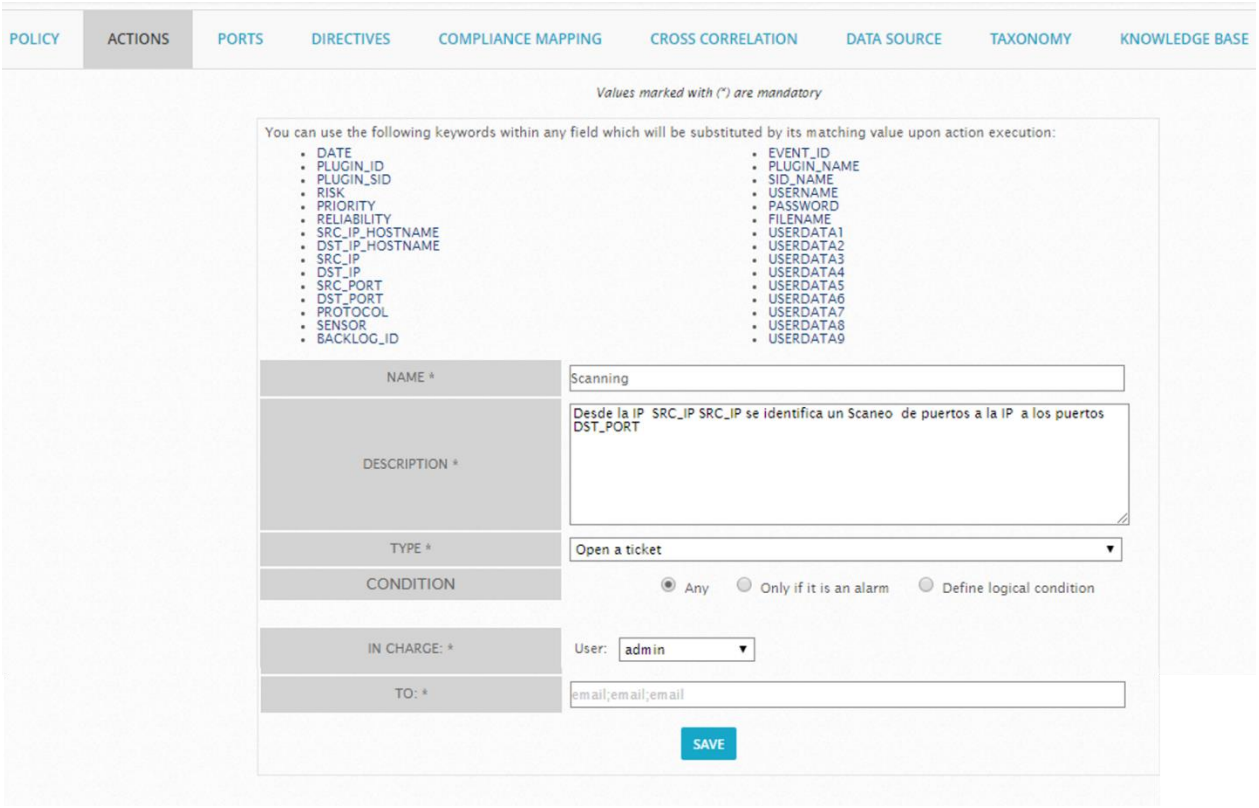


Ilustración 51. Creación de Acción en OSSIM (Elaboración propia).

2. Se ingresa a la opción Inteligencia de amenazas y en la opción de Politicas, se da selecciona Nueva:

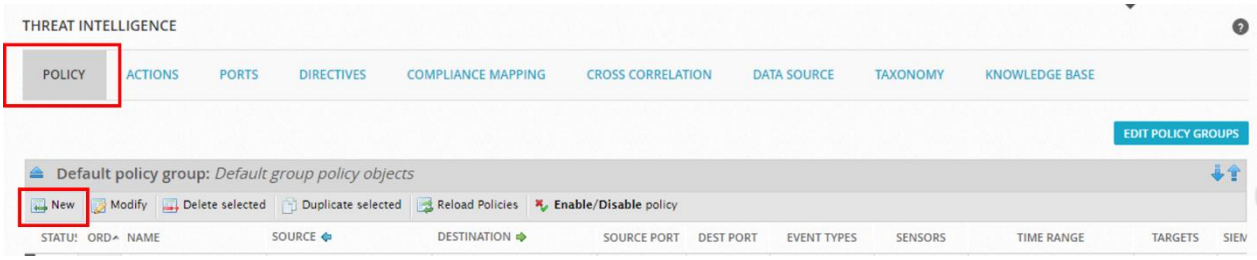


Ilustración 52. Nueva política en OSSIM (Elaboración propia).

3. Se debe definir un nombre para la política a crear y seguidamente ingresar las condiciones de la política donde se debe definir IP fuente, IP destino, puertos fuente y destino y tipo de evento, por último se define la consecuencia de la política que será la acción creada en el primer paso.

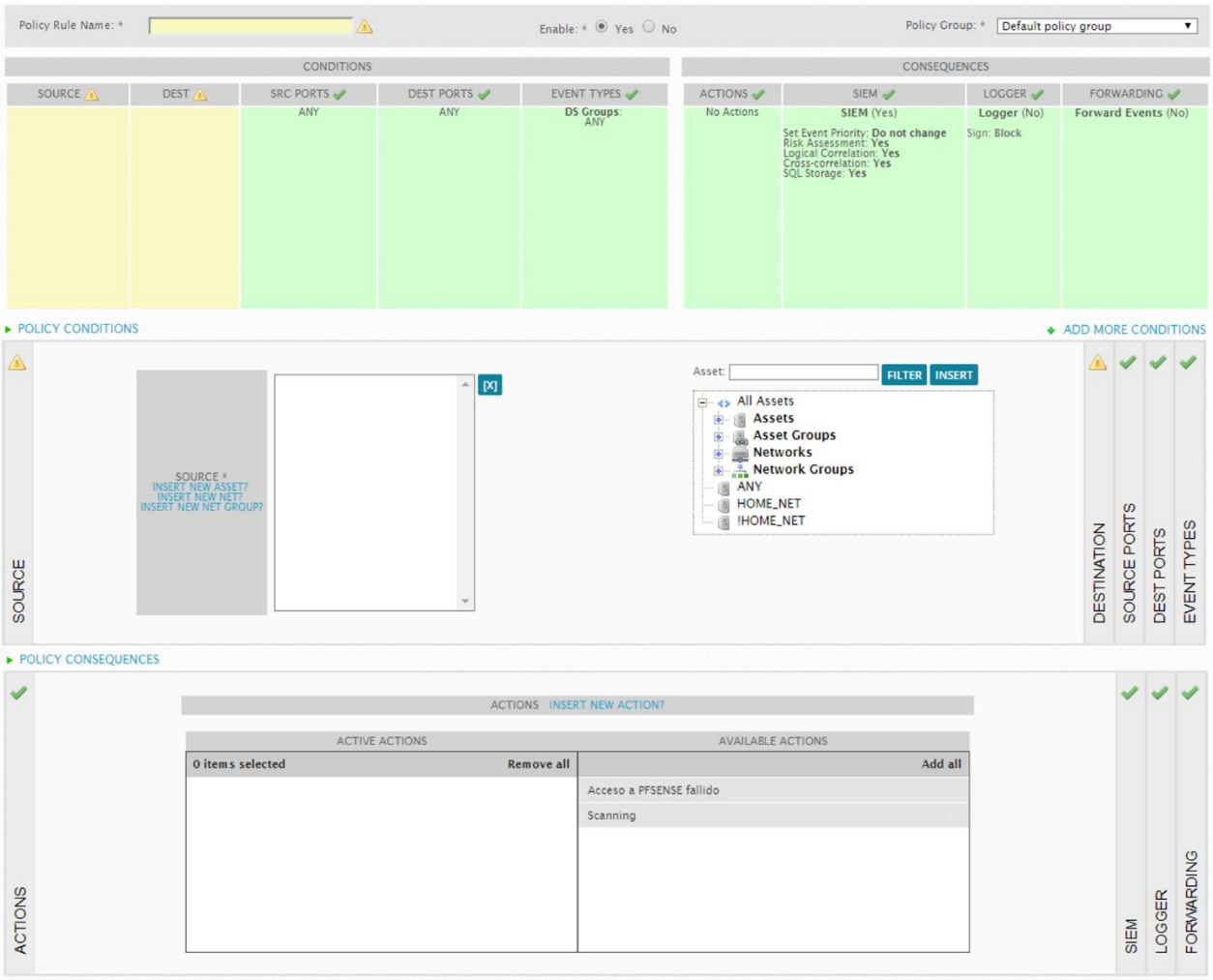


Ilustración 53. Configuración de política en OSSIM (Elaboración propia).

Política intentos de acceso fallidos a pfsense

A continuación, se creará una regla para generar alertas cuando haya intentos de acceso fallidos de ingreso al PFSENSE.

1. Ir a CONFIGURATION y seleccionar THREAT INTELLINGENCE

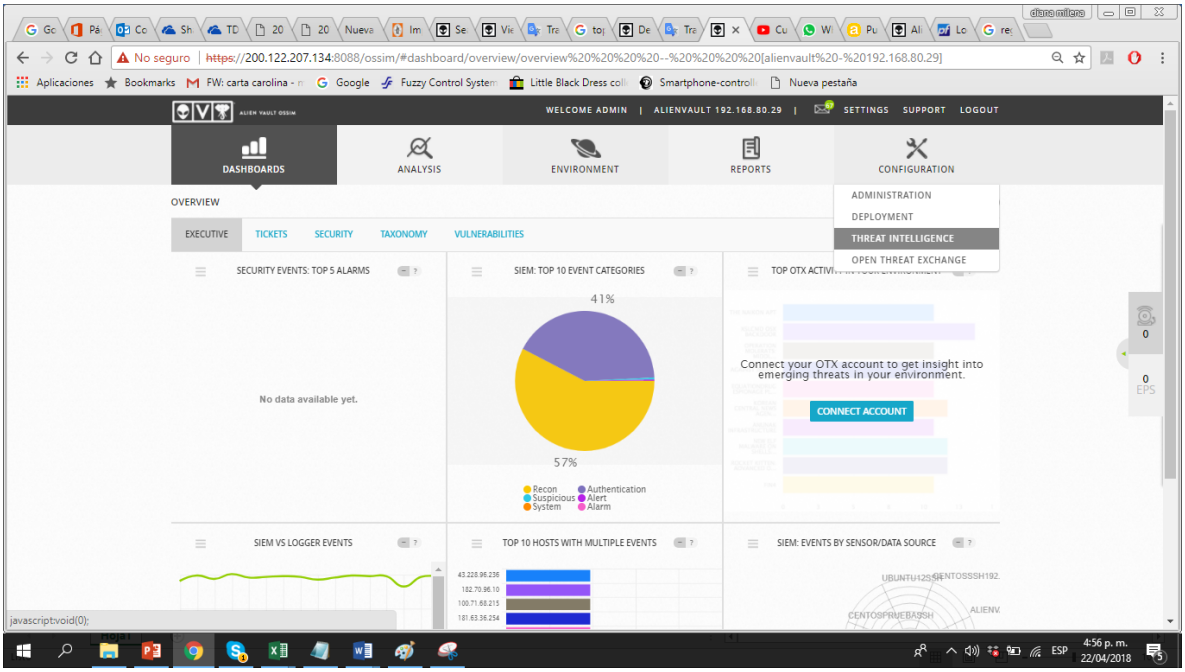


Ilustración 54. Ingreso a configuración de política (Elaboración propia).

2. Ir a ACTIONS y dar clic en NEW

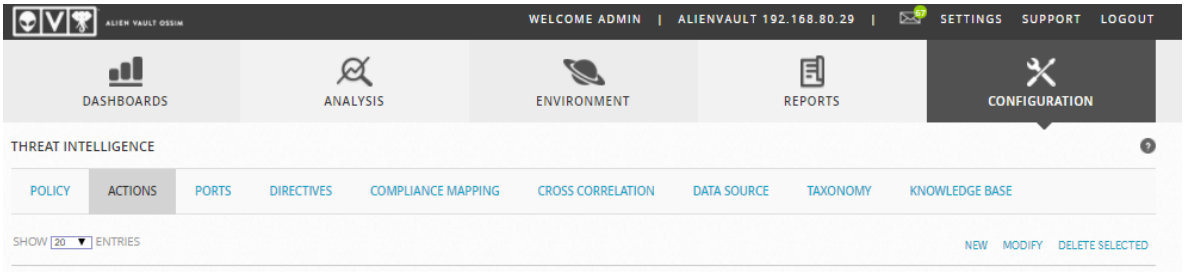


Ilustración 55. Ingresar nueva política (Elaboración propia).

3. Se ingresan los siguientes parámetros

   NAME: Acceso a PFSENSE fallido

   DESCRIPTION: Genera una alerta cuando se identifica desde la ip fuente un intento fallido a la consola de gestión de pfsense.

   TYPE: Open a ticket

   CONDITION: Any

   IN CHARGE: admin

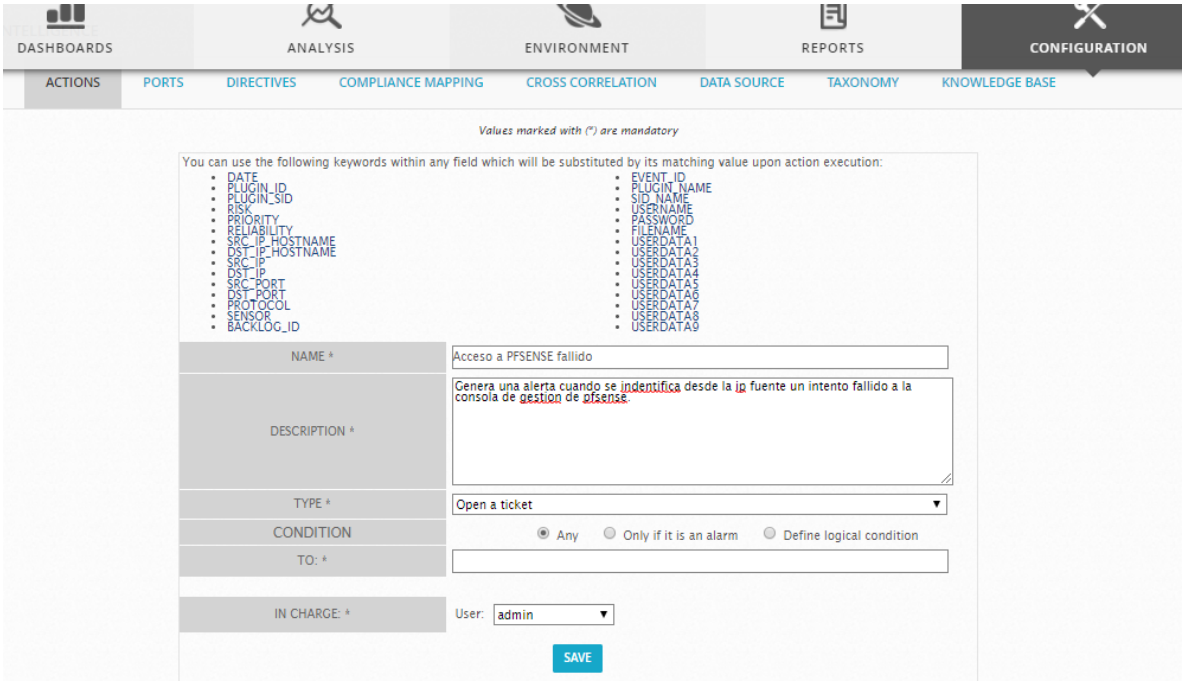


Ilustración 56. Configuración de parámetros para una acción (Elaboración propia).

4. Ir a POLICY, y dar clic en New.

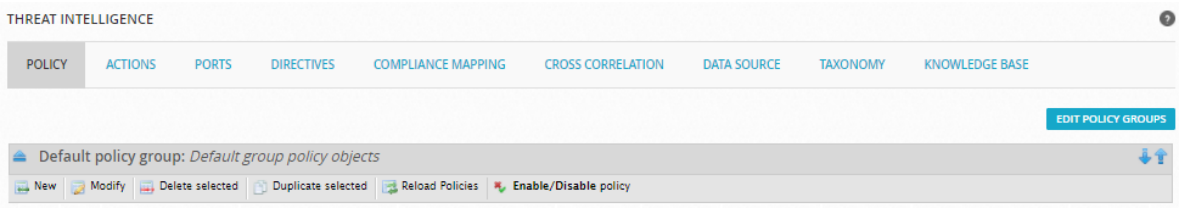


Ilustración 57. Crear nueva política en OSSIM (Elaboración propia).

5. Se abre el ayudante para la creación de políticas, luego se debe definir un nombre para la politica a crear, en SOURCE, se ingresan los IP fuente del evento, en este caso ANY para detectar cualquier IP qué tenga un intento fallido en PFSENSE.

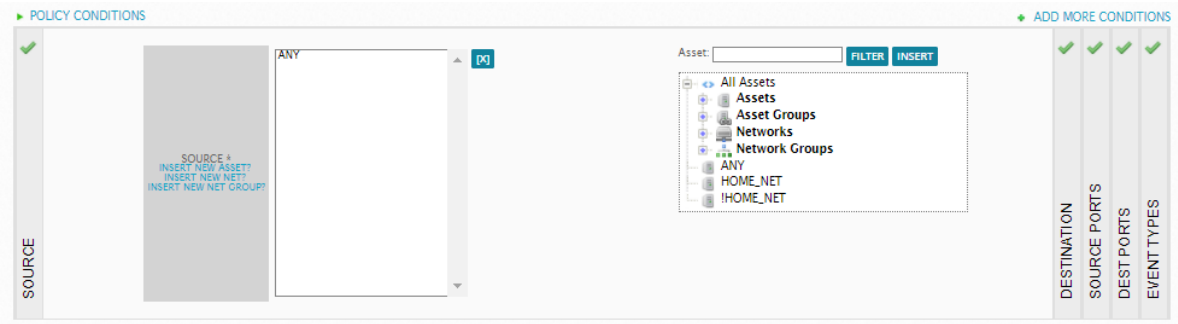


Ilustración 58. Configuración política - IP Fuente (Elaboración propia).

6. DETINATION: se ingresa la dirección ip destino del evento, en este caso se ingresa la del PFSENSE 192.168.80.3.

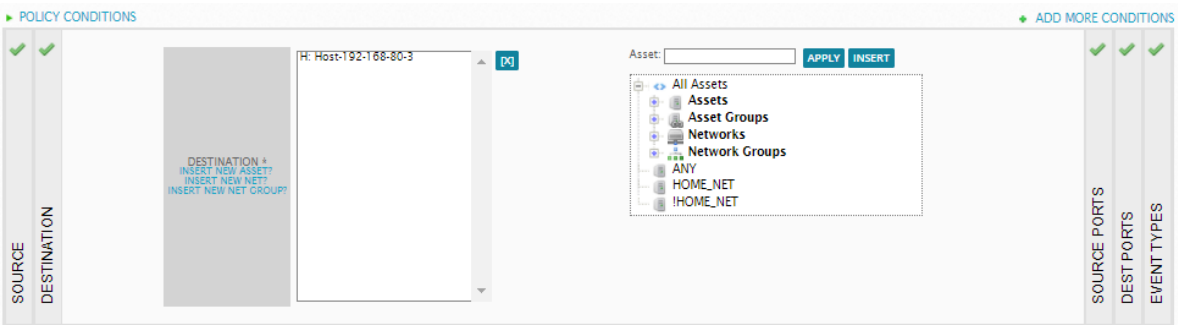


Ilustración 59. Configuración política - IP destino (Elaboración propia).

7. SOURCE PORTS, puerto de origen TCP/UDP del evento, en este caso se selecciona ANY

Ilustración 60. Configuración política - puertos Fuente (Elaboración propia).

8. DEST PORTS, se seleccionan los puerto destino TCP/UDP, para este caso se crea un nuevo grupo de puertos danto clic en INSERT NEW PORT GROUP.

Ilustración 61. Configuración política - puertos destino (Elaboración propia).

9. Se ingresa la siguiente información

NAME: HTTP

PORTS: 443 – tcp

8088 – tcp

80 – tcp

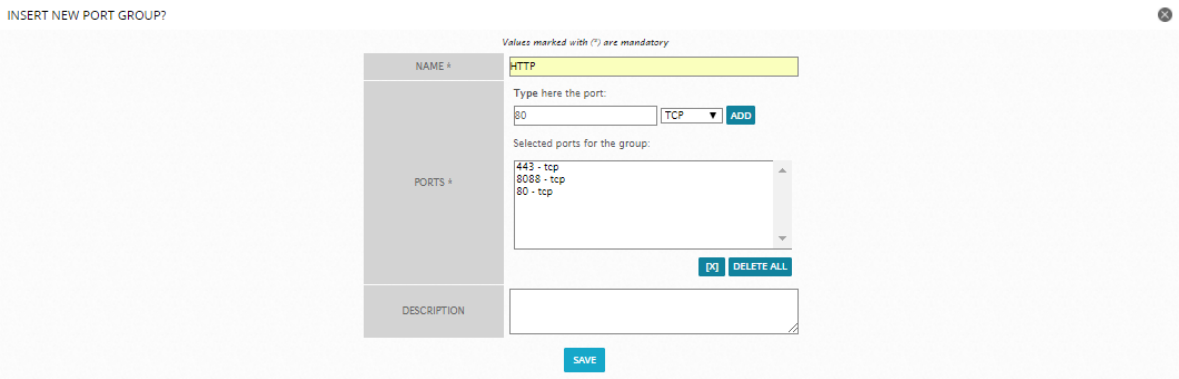


Ilustración 62. Configuración política - puertos destino (Elaboración propia).

10. EVENT TYPES Define eventos para ser procesados por esta política. Para este caso se crea un nuevo grupo de eventos dado clic en INSERT NEW DS GROUP.

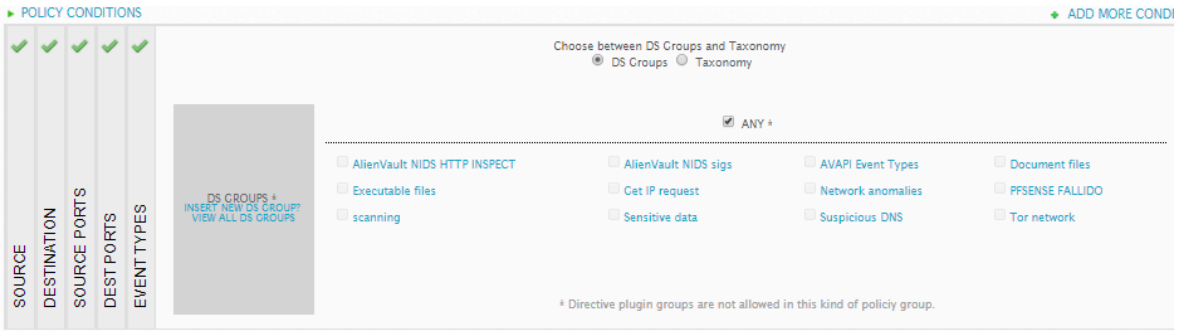


Ilustración 63. Configuración política - nuevo grupo eventos (Elaboración propia).

11. Clic en ADD NEW GROUP.

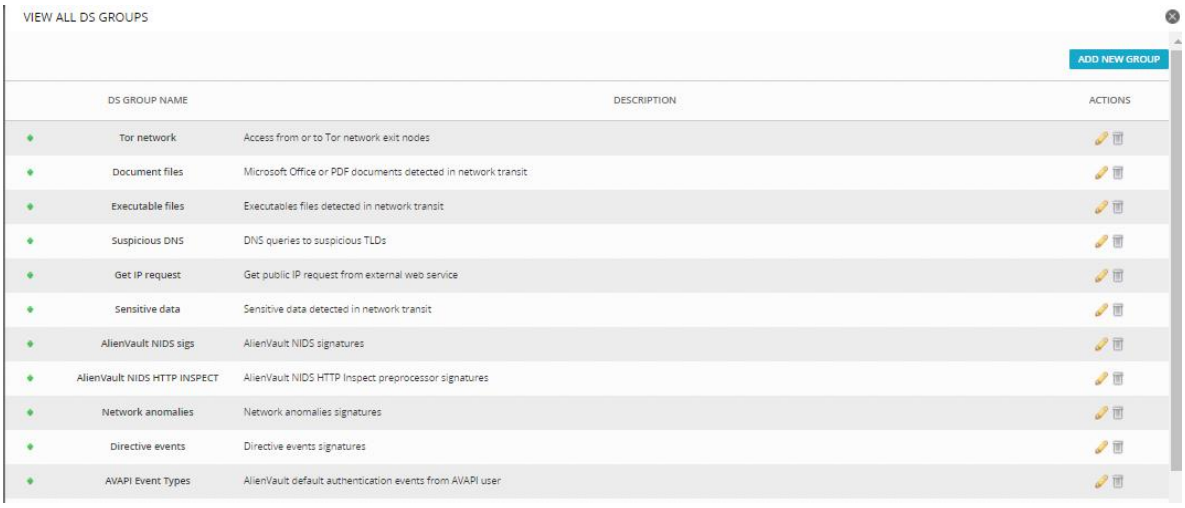


Ilustración 64. Configuración política - nuevo grupo eventos (Elaboración propia).

12. Se busca el evento 7010 y se le asigna el nombre de PFSENSE FALLIDO.

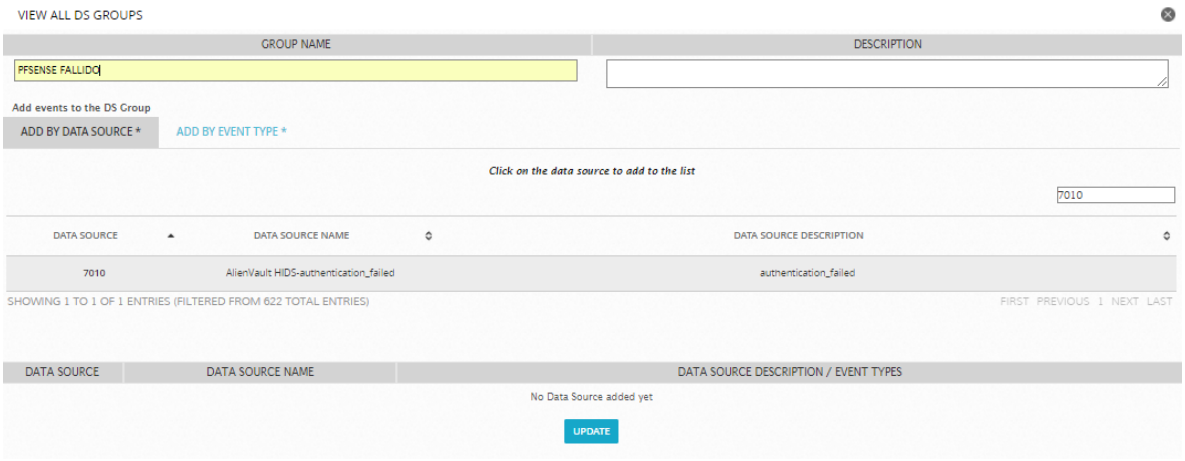


Ilustración 65. Configuración política - agregar evento (Elaboración propia).

13. Se des selecciona ANY y se selecciona PFSENSE FALLIDO y finalmente se guarda la política.

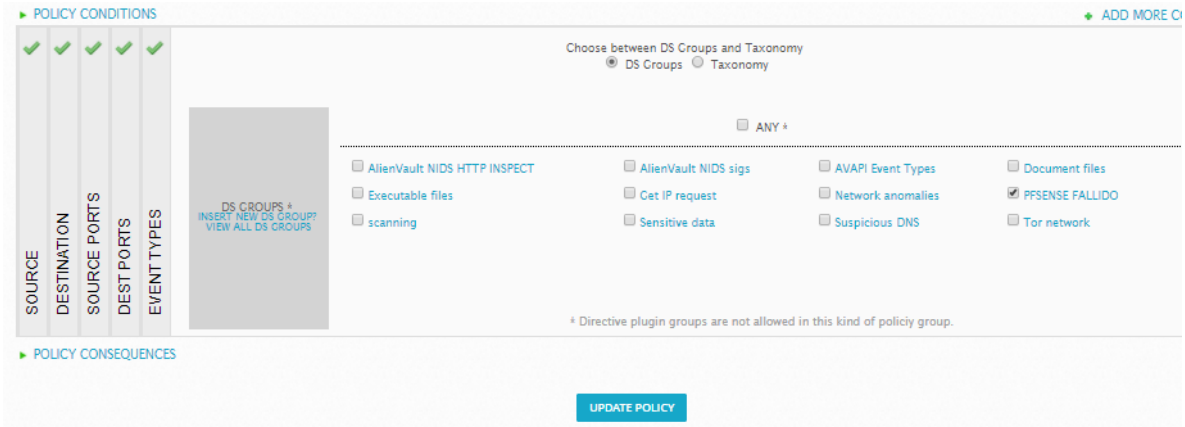


Ilustración 66. Configuración política - selección de tipo evento (Elaboración propia).

FIRMA ESTUDIANTES Leidy Moreno

Daniel Cano.

FIRMA ASESOR Miguel Angel Roldan

FECHA ENTREGA: 17/07/2018

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____