UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

PROGRAMA DE MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
COHORTE 2021

Tema: INTEGRACIÓN DE UN CORRELACIONADOR DE EVENTOS DE SEGURIDAD DE LA RED INSTITUCIONAL

Trabajo de Titulación, previo a la obtención del Título de Cuarto Nivel de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones.

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Desarrollo

Autor: Ingeniero Henry Rodrigo Peralvo Mejía
Director: Ingeniero Milton Neptalí Román Cañizares Magíster

Ambato – Ecuador

2023

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Héctor Fernando Gómez Alvarado. PhD, e integrado por los señores: Ingeniero Santiago Mauricio Altamirano Meléndez Magíster e Ingeniero José Vicente Morales Lozada, PhD, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: *"INTEGRACIÓN DE UN CORRELACIONADOR DE EVENTOS DE SEGURIDAD EN LA RED INSTITUCIONAL"* elaborado y presentado por el *señor Ingeniero Henry Rodrigo Peralvo Mejía,* para optar por el Título de Cuarto Nivel de Magíster en Tecnologías de la Información Mención Seguridad en Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado. PhD.
Presidente y Miembro del Tribunal

Ing. Santiago Mauricio Altamirano Meléndez. Mg.
Miembro del Tribunal

Ing. José Vicente Morales Lozada. PhD.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Integración de un correlacionador de eventos de seguridad en la red institucional, le corresponde exclusivamente a: Ingeniero Henry Rodrigo Peralvo Mejía, Autor bajo la Dirección del Ingeniero Milton Neptalí Román Cañizares, Magíster, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniero Henry Rodrigo Peralvo Mejía
c.c.:1802634798
AUTOR

Ingeniero Milton Neptalí Román Cañizares Magíster
c.c.: 0502163447
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniero Henry Rodrigo Peralvo Mejía
c.c.: 1802634798

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

INDICE DE FIGURAS

AGRADECIMIENTO

Agradezco a mi tutor Ingeniero Milton Román Cañizares, quien con su acertada guía ha sido parte importante en el desarrollo del presente trabajo de investigación.

A los docentes de la maestría, quienes con su experiencia y sabiduría han transmitido sólidos conocimientos en el programa.

A la Universidad Técnica de Ambato por permitirme aplicar el trabajo de investigación en su prestigiosa institución y, en especial, a los profesionales encargados de la seguridad y la red institucional que, a través de su predisposición y colaboración, facilitaron el aporte necesario para plasmar el presente proyecto.

A los compañeros maestrantes, quienes en el desarrollo de los módulos cursados brindaron su apoyo y se estableció un agradable equipo de colaboración.

DEDICATORIA

Este trabajo está dedicado a mi familia:

A mis hijos, fuente de motivación e inspiración para ser mejor cada día.

A mi esposa, quien con el apoyo brindado permanentemente ha permitido fortalecer la consecución de este gran objetivo.

A mis padres por inculcarme valores como honestidad y responsabilidad.

A mi hermano Fidel, quien constantemente ha reforzado las metas trazadas.

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

TEMA:

INTEGRACIÓN DE UN CORRELACIONADOR DE EVENTOS DE SEGURIDAD EN LA RED INSTITUCIONAL

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Desarrollo*
AUTOR: *Ingeniero Henry Rodrigo Peralvo Mejía*
DIRECTOR: *Ingeniero Milton Neptalí Román Cañizares Magíster*
FECHA: *Treinta de marzo de dos mil veintitrés*

RESUMEN EJECUTIVO

El presente trabajo de investigación tiene por objeto la implementación de un correlacionador de eventos de seguridad en la red DMZ de la Universidad Técnica de Ambato a través de la herramienta SIEM open source AlienVault OSSIM, la misma que posee características además de la correlación de eventos, la evaluación de vulnerabilidades, detección de intrusiones, monitoreo de comportamiento. La aplicación de este sistema de seguridad permitirá un mejor control ante las diferentes amenazas a las que están expuestos los activos de la red y ofrecerá al administrador de seguridad filtrar eventos específicos para realizar diversas tareas de monitoreo, vigilancia, diagnóstico y toma de decisiones en una sola interfaz de trabajo. Para llevar a cabo la implementación, en primer lugar, se realiza un análisis de la situación actual en base al levantamiento de información del entorno de trabajo, es decir, los equipos que conforman este segmento de red, su distribución y diseño. Posteriormente, en base a las necesidades de los administradores de red y seguridad, y necesidades institucionales, se analiza y selecciona la herramienta que más se adapta para el proceso. Finalmente, se procede a la instalación y configuración de la herramienta. Se integra los activos seleccionados y se logra la configuración necesaria. A través de políticas y acciones creadas se procede a su comprobación mediante filtros y ataques (Fuerza bruta, Inyección SQL, XSS) que evidencien el

funcionamiento y la obtención de resultados deseados. Entre los activos de los cuales se recepta los eventos en tiempo real existen varios equipos críticos que generan un alto flujo de datos, lo cual pone a prueba la capacidad de la herramienta de trabajar con grandes cantidades de información. La implementación de sistemas y procesos que ayuden a la mitigación de ataques y vulnerabilidades permite además cumplir con normas y estándares de seguridad en las instituciones.

DESCRIPTORES: *ALARMAS, AMENAZAS, ATAQUES, CORRELACIONADOR DE EVENTOS, DASHBOARD, IDS, MONITOREO, SIEM, SOFTWARE LIBRE, VULNERABILIDADES.*

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Introducción

A nivel mundial el crecimiento acelerado del uso de internet, las redes de área local y en el uso de plataformas que permiten que los usuarios tengan acceso a los servicios brindados por distintas instituciones, convierte en una necesidad el uso de herramientas que faciliten la administración de la red en busca de mitigar las amenazas que se presentan constantemente. La Universidad Técnica de Ambato brinda servicios a través de plataformas intranet como extranet para toda la comunidad universitaria, así como para público en general. El presente proyecto "Integración de un correlacionador de eventos de seguridad en la red institucional" brinda un análisis e implementación de una herramienta basada en SIEM (Security Information and Event Management) a través de software libre enfocada en la correlación de eventos, que permitirá al administrador de red y al administrador de seguridad del área DMZ de la Universidad Técnica de Ambato tener un mejor control sobre los activos críticos que la conforman. Este proyecto consta de seis capítulos que se detallan a continuación.

En el capítulo 1, se aborda el tema del trabajo, el alcance, justificando la relevancia de la aplicación del presente proyecto, así como la exposición de los objetivos general y específicos, en el capítulo 2 se señala los antecedentes investigativos y fundamentación teórica que fundamentan la investigación, en el capítulo 3 se muestra la metodología aplicada en el presente proyecto, en el capítulo 4 se presenta los resultados obtenidos, el análisis y discusión en base a la obtención de análisis previos, el capítulo 5 se muestra las conclusiones, recomendaciones, bibliografía y anexos, el capítulo 6 presenta la propuesta.

Una de las limitaciones que se mostró en el presente proyecto fue el acceso restringido a determinado segmento de la red DMZ, debido a que se trata de dispositivos de disponibilidad crítica, por tanto, fueron excluidos del desarrollo.

1.2 Justificación

Las organizaciones con el fin de brindar los servicios a los que están enfocados realizan a través del uso de redes de información y activos, las acciones que permiten que está información cumpla con su objetivo que es satisfacer el requerimiento de los usuarios. El utilizar estos medios, que actualmente tienen un crecimiento exponencial, hace que los recursos institucionales estén expuestos a ataques por parte de agentes de amenazas. Para hacer frente a estas amenazas existen alternativas para mitigar su impacto, este proyecto se enfoca en facilitar una herramienta que brinde el apoyo para que la gestión diaria de los administradores de seguridad y de red no sea una tarea compleja y que permita cubrir los aspectos importantes para fortalecer la seguridad de la red de una institución o de un determinado segmento de esta. La Universidad Técnica de Ambato al momento no dispone de una herramienta que permita la gestión ágil de todos los eventos de seguridad que ocurre en tiempo real, de tal forma que se garantice una red constantemente controlada, capaz de realizar la correlación de eventos y el procesamiento de esta información, para aumentar la capacidad de detección, priorizar los eventos según el contexto en que se producen, y monitorizar el estado de seguridad de la red (ISO 27001:2013, 2013), y a la vez proveer una colección de herramientas para garantizar al administrador, una vista de los aspectos relativos a la seguridad en su sistema aplicando la utilización de software libre (Decreto Ejecutivo 1425, 2008).

Los ataques son cada vez más sofisticados y numerosos, tal que como respuesta se llevan a cabo el desarrollo de métodos, plataformas y sistemas de seguridad cada vez más complejos y avanzados para contener estas amenazas, que se ha convertido en una característica de la propia red (Azizov, 2020). Los administradores de red se han visto en la ardua tarea de prever y combatir estas amenazas aplicando diferentes herramientas disponibles de forma aislada.

Pero en virtud de lo extenso y complejo que puede volverse el escenario, es oportuno aplicar una herramienta que permita el monitoreo integrado de la seguridad.

Por razones de los altos costos de licenciamiento de software de seguridad se ha visto oportuno seleccionare una herramienta SIEM de código abierto, cuya implementación, prestaciones y servicios que brinda son de gran utilidad.

La obtención de resultados se logra a través de una adecuada configuración, definición de políticas, directivas y acciones, la posterior adquisición de habilidades en el manejo de la herramienta, el análisis de reportes.

1.3 Objetivos

1.3.1 General

Implementar un sistema de recolección y análisis de logs que permita detectar ataques informáticos basado en la correlación de eventos en la infraestructura de red DMZ administrada por la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato.

1.3.2 Específicos

- Diagnosticar los ataques informáticos que representen riesgos sobre los activos de información de la infraestructura de red DMZ.
- Analizar las diferentes soluciones de localización de ataques informáticos basados en la correlación de eventos basado en software libre para su aplicación en la red DMZ.
- Implementar un sistema de detección de ataques basado en la correlación de eventos usando una herramienta adecuada sobre los activos que manejan información crítica, que se encuentran en la red DMZ.

CAPÍTULO II

ANTECEDENTES INVESTIGATIVOS

La mayoría de las organizaciones tienen acceso a información sensible a través de la red, y el hecho de no proteger de manera adecuada dicha información podría tener consecuencias importantes como pérdidas operativas, financieras y legales graves (ISO 27001:2013, 2013).

La información actualmente es uno de los activos más valiosos de una organización, por tanto, mantener su integridad, confidencialidad y disponibilidad es fundamental para lograr los objetivos del negocio.

También, es importante señalar que, debido al avance de las tecnologías de la información y comunicación, se ha dado un acelerado crecimiento de la ciberdelincuencia, facilitando su proliferación debido a que los ciberdelincuentes cada vez disponen de más herramientas para realizar operaciones y requieren menos conocimientos especializados y profundos, logrando impactos más críticos en los sistemas informáticos. Además, siempre se debe tener conciencia que desde dentro de la organización, existe la posibilidad de causar daño intencionado en los sistemas.

Con la llegada de las redes sin fronteras, impulsadas ya sea por la necesidad de movilidad de los sistemas actuales, en algunos casos aceleradas por la aparición de la pandemia de COVIT 2019 o por razones de modernización de los sistemas, se ha vuelto indispensable que más servicios se habiliten para poderlos utilizar desde cualquier lugar, dentro o fuera de la institución, en cualquier momento y con diversos perfiles de usuario, desde diferentes dispositivos de manera externa a la institución. Todos los requerimientos mencionados anteriormente conducen a un mayor y complejo compromiso la gestión de control y monitoreo de la seguridad informática. Por lo tanto, la misión de los profesionales de seguridad siempre estará enfocada en proteger los activos de la organización y mantener la continuidad del negocio.

Es prioritario detectar ataques oportunamente y disponer de las medidas para contrarrestarlos, a través del uso de procesos que permitan la respuesta a los incidentes, minimizando los daños que pueden provocar (Alamanni, 2014).

En los últimos años Ecuador se ha mantenido en los primeros lugares en la región como uno de los países con más ciberataques, lo cual es una advertencia para que las organizaciones tomen mejores medidas que permitan contrarrestar estas amenazas, para que no afecten el normal desarrollo de sus actividades y puedan alcanzar sus objetivos.

Los ataques más representativos ocurridos a instituciones públicas en el año 2021 fueron los efectuados en la CNT y la ANT, lo cual demuestra que las amenazas siempre están latentes y compromete a estar actualizados en aplicar mecanismos que hagan frente a las mismas.

La metodología aplicada para el análisis de la implementación de un SIEM es a través de la identificación de ventajas y desventajas de aplicarlo en una organización, realizar el diseño, la selección de la herramienta más adecuada (Rigau Pedraza, 2019).

No muchas organizaciones aprovechan la importancia que tiene la gestión de logs para visualizar riesgos, vulnerabilidades, trazabilidad de incidentes (Avella & Calderón, 2015). Las herramientas SIEM permiten gestionar de manera centralizada los eventos e información de seguridad y los puede hacer a través de una interfaz gráfica de fácil uso.

Según Bravo & Villafuerte (2015), indican que la seguridad informática requiere de una herramienta que ayude a los administradores de red a tomar decisiones oportunas sobre información crítica y servicios que beneficien a la organización y su buen funcionamiento.

De acuerdo con Madrid & Múnera (2008), la existencia de variedad de herramientas que en ocasiones hace que se las emplee en conjunto para gestionar diferentes frentes en la red trae consecuencias como: falta de uniformidad en formato de registros; exceso de alertas, la cantidad de alertas que se genera en ambientes de gran tamaño sobrepasa la capacidad de trabajo del administrador, entre otras. En este sentido las herramientas SIEM tiene como características principales el análisis y la normalización de registros automático.

Para la gestión óptima de logs en medianas empresas Avella & Calderón (2015) recomiendan filtrar los logs para evitar falta de eficacia, gasto de recursos y tiempo, es decir, descartando aquellos logs que no supongan información útil o relevante.

Bravo & Villafuerte (2015) en una de sus conclusiones al finalizar la implementación manifiestan que contribuye un aporte muy importante al administrador de red para la toma de decisiones en el área de la seguridad al integrar diferentes dispositivos de variadas marcas y sistemas operativos.

2.1 Fundamentación Teórica

Seguridad de la Información

Para Areitio (2008), el objetivo principal de la seguridad de la información es permitir que una organización logre todos sus objetivos comerciales o de misión mediante la implementación de sistemas que presten especial atención y tengan en cuenta los riesgos organizacionales relacionados con las TIC.

Según la norma ISO/IEC 27002:2007, la seguridad de la información es la protección de la información frente a los diferentes tipos de amenazas para garantizar la continuidad del negocio minimizando los riesgos.

SIEM

Viene de dos conceptos: SIM (Security Information Manager) que es la gestión de la seguridad de la información, cuya función principal es almacenar datos en un repositorio central y SEM (Security Event Manager) que es la gestión de eventos de seguridad, que centraliza el almacenamiento y correlaciona los eventos y logra el servicio de monitoreo.

Evento

De acuerdo con ISO 31000:2018 (2018), un evento es una ocurrencia o cambio de un conjunto particular de circunstancias.

Incidente de Seguridad

Para Chicano Tejada (2015), un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad, y disponibilidad de la información. La ISO 27001:2005 define que un incidente de seguridad es un evento no deseado o no esperado que puede comprometer significativamente las operaciones de negocio y amenazar la seguridad e la información.

Activo

Se trata de cualquier elemento que posea valor para la organización, entre otros tenemos: bases de datos, software, equipos (computadores, servidores, dispositivos de red), procesos, servicios.

Amenaza

De acuerdo con Avella & Molano (2015), las amenazas son eventos que pueden dar como resultado un incidente en todo tipo de organización, y como consecuencia lograr daños materiales o intangibles en sus activos.

Vulnerabilidad

Según ISO/IEC 27002:2018, debilidad de un activo o control que puede ser explotado por una o más amenazas.

Riesgo

Es una combinación de las consecuencias de un evento y la probabilidad que se materialice. El riesgo de seguridad de la información está relacionado con la capacidad de que las amenazas exploten las vulnerabilidades de un activo (ISOTools Excellence, 2020).

Los Ataques Informáticos

Según Mieres (2009) un ataque informático se basa en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, hardware, y en las personas que componen el área informática con el objetivo de obtener un beneficio económico o razones personales, causando un efecto negativo en la seguridad del sistema.

Impacto

Es el resultado evaluado de un evento en particular.

2.2 Sistema de Gestión de Eventos de Seguridad

Características

Onpremise. Solución local en equipos virtuales o físicos.

Network. Integración y explotación de eventos de la red.

Endpoint. Integración y explotación de host.

Monitoreo Centralizado. De todas las amenazas potenciales.

Identificar amenazas reales y falsos incidentes.

Aportar mayor grado de conocimiento sobre los incidentes para facilitar resolución.

Componentes principales de un SIEM

- Agregación de datos. – Se encarga de la recopilación de datos de registro generados por variadas fuentes en una red, la misma que consta servidores, base de datos, aplicaciones, firewalls, enrutadores entre otros.
- Análisis de datos de seguridad. – Se trata de componentes de análisis de seguridad con tableros que proveen la información de manera visual y fácil de gestionar, con conexión en tiempo real y que ayuda a identificar actividades maliciosas. Con esta información el administrador puede detectar anomalías, correlaciones y patrones.
- Correlación y monitoreo de eventos de seguridad. – Es uno de los principales componentes de las herramientas SIEM. En base a reglas de correlación integradas o creadas por el usuario permite realizar un análisis de atributos en común en los eventos para posteriormente buscar soluciones a inconvenientes de seguridad.
- Análisis forense. – Permite a través de los registros almacenados generar informes y realizar un seguimiento cuando ocurrió una violación de seguridad específica.
- Detección y respuestas a incidentes. – Un incidente puede ser una violación de datos, así como puede ser una infracción a políticas institucionales establecidas. Entre las respuestas a incidentes que ayuda el SIEM se puede mencionar la automatización a través de un flujo de trabajo.
- Respuesta de eventos en tiempo real. – Las herramientas SIEM a través de su recopilación y correlación de registros en tiempo real genera una alerta automática de tal manera que el personal especializado actuará inmediatamente para mitigar el ataque o evitarlo.
- Inteligencia de amenazas. – Se trata de información contextual para identificar las amenazas y poder tomar medidas para solucionar.
- Gestión de cumplimiento de TI. – Las herramientas SIEM ayudan a cumplir con los estándares y regulaciones que ordenan organismos gubernamentales.
- Recolección de datos y eventos
- Agregación de y correlación de estos datos en tiempo real

- Interfaz apropiada para actividades de gestión, monitoreo y visualización de los eventos.

Nota. Adaptado de “Componentes de la arquitectura SIEM”, por ManageEngine Log 360 (2022).

Mecanismos de gestión de Logs

El proceso de recolección de logs se realiza a través de protocolos de red, estos tienen su propio mecanismo de enviar los logs, entre los diferentes mecanismos mencionaremos los más comunes:

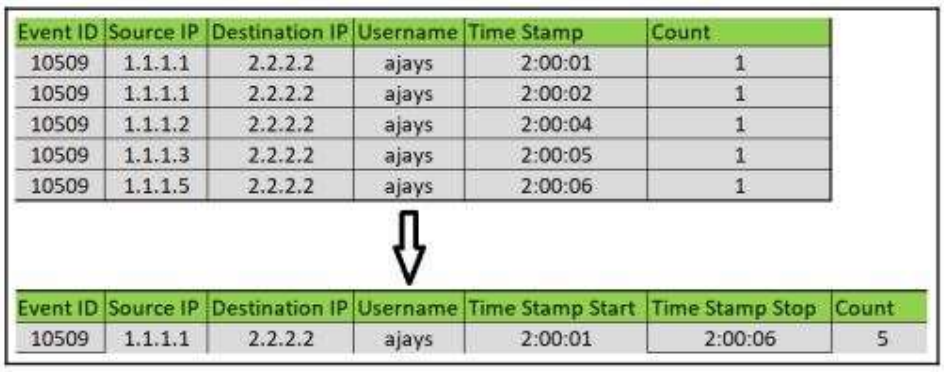
- Syslog. – Protocolo cliente/servidor que envía mensajes a través del protocolo UDP por el puerto 514 en texto plano.
- SNMP. - Es un protocolo de la capa de aplicación para administrar y monitorizar elementos de la red.
- Windows Event log. – Es un protocolo propietario de Microsoft para recolección y transmisión.
- Rsyslog. - Es una versión mejorada de Syslog que principalmente se diferencia de este por tener un mejor rendimiento.

2.3 Gestión centralizada de registros

2.3.1 Recopilación de eventos y registros o agregación de datos

La recopilación de registros es el núcleo de una herramienta SIEM. Las herramientas SIEM recopilan registros de eventos de diversos sensores los cuales han sido habilitados en los activos a tratarse. Los eventos brindan datos de actividades, analizan la seguridad de segmento de red determinada.

Como ejemplo a continuación podemos indicar que el ID de evento 10509 se generó a raíz de un error de inicio de sesión y estos registros viajan al SIEM. Se puede correlacionar este evento con un ataque o un incidente.



Event ID	Source IP	Destination IP	Username	Time Stamp	Count
10509	1.1.1.1	2.2.2.2	ajays	2:00:01	1
10509	1.1.1.1	2.2.2.2	ajays	2:00:02	1
10509	1.1.1.2	2.2.2.2	ajays	2:00:04	1
10509	1.1.1.3	2.2.2.2	ajays	2:00:05	1
10509	1.1.1.5	2.2.2.2	ajays	2:00:06	1

Event ID	Source IP	Destination IP	Username	Time Stamp Start	Time Stamp Stop	Count
10509	1.1.1.1	2.2.2.2	ajays	2:00:01	2:00:06	5

Figura 1. Ejemplo varios inicios erróneos de sesión.

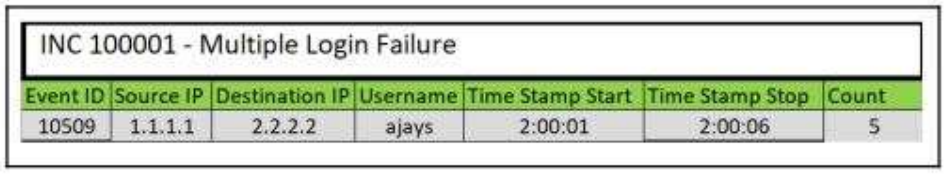
Practical network scanning, Singh (2018).

2.3.2 Correlación de eventos

De acuerdo con Singh Chauhan (2018), la correlación de eventos es el proceso en el que la herramienta SIEM relaciona varios eventos para crear un evento más significativo.

Usando el mismo ejemplo anterior, existió 5 intentos fallidos de inicio de sesión en la misma cuenta de usuario desde varios equipos de origen. eventos para generar un incidente o evento de importancia.

Avella & Calderón (2015) señalan que la correlación tiene como meta obtener relaciones entre uno o varios registros de una misma fuente o diversas fuentes. La correlación permite un análisis eficiente para determinar un ataque.



INC 100001 - Multiple Login Failure

Event ID	Source IP	Destination IP	Username	Time Stamp Start	Time Stamp Stop	Count
10509	1.1.1.1	2.2.2.2	ajays	2:00:01	2:00:06	5

Figura 2. Ejemplo de correlación.
Practical network scanning, Singh (2018).

Gracias al registro de esta correlación el sistema emitirá alertas.

2.3.3 Informes y alertas

Los sistemas SIEM activan alertas de acuerdo con las reglas configuradas.

2.3.4 Tableros (Dashboard)

Los tableros como parte de las herramientas SIEM permiten a los administradores visualizar de manera amplia las actividades, la detección de anomalías, el seguimiento de indicadores de seguridad.

2.3.5 Automatización

Permite reducir los tiempos de identificación y respuesta a posibles ataques y amenazas de seguridad. Esto se logra con la aplicación de alarmas, envío de tiques, envío de mails a administrador, así como la ejecución de scripts automáticos para dar una respuesta a un evento de importancia.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Ubicación

El proceso de investigación se desarrolló en la Universidad Técnica de Ambato, misma que consta de tres predios ubicados en el sector de Ingahurco, Huachi y Querochaca. La ubicación específica en donde se realizó la investigación fue en el predio de Huachi donde se encuentra alojado el data center institucional.

3.2 Equipos y materiales

Para el desarrollo del presente proyecto se utilizó los equipos y materiales descritos en la tabla 1.

TABLA 1. LISTA DE EQUIPOS Y MATERIALES A UTILIZARSE

Item	Rubro	Valor
1	Computador	900.00
2	Internet	200.00
3	Material Bibliográfico	100.00
4	Material de Oficina	50.00
5	Otros	100.00
Total		**1350.00**

3.3 Tipo de investigación

Modalidad de Investigación

Investigación de campo

Porque permite recoger información requerida en el lugar de los hechos como lo es la DMZ institucional.

Investigación experimental

Los datos serán obtenidos de manera experimental de un grupo de activos de la red DMZ con los parámetros requeridos por la institución con el fin de analizar y obtener resultados esperados.

Investigación mixta

Se aplica el enfoque cuali-cuantitativo. Cualitativo para obtener la información a través de la entrevista, así como para seleccionar la herramienta SIEM adecuada a implementar.

Se aplica el enfoque cuantitativo porque a través de datos obtenidos de los activos que forman parte del estudio se logra establecer los criterios para la implementación y gestión.

3.4 Prueba de Hipótesis

Hernández Sampieri (2014), manifiesta que, una vez planteado el problema de estudio, el investigador construye un marco teórico del cual deriva una o varias

hipótesis y las somete a prueba mediante el empleo de diseños de investigación apropiados.

3.4.1 Hipótesis de Investigación

Implementar un sistema de recolección y análisis de logs genera una mejora en la detección de ataques informáticos basado en la correlación de eventos en la infraestructura de red DMZ de la Universidad Técnica de Ambato.

3.4.2 Hipótesis Nula

Implementar un sistema de recolección y análisis de logs no genera una mejora en la detección de ataques informáticos basado en la correlación de eventos en la infraestructura de red DMZ de la Universidad Técnica de Ambato.

3.5 Población o muestra

Arias-Gómez & Villasís (2016) manifiesta que "La población de estudio es un conjunto de casos, definido, limitado y accesible, que formará el referente para la elección de la muestra que cumple con una serie de criterios predeterminados" (p. 201).

La institución en su Data Center cuenta con 70 servidores entre ellos 30 servidores físicos, 40 servidores virtuales, 1 Firewall, 4 Switches, un servidor de almacenamiento en red. Los Servidores prestan servicios como base de datos, aplicaciones, aulas virtuales, Directorio Activo, Antivirus entre otros a su comunidad universitaria.

Población accesible

Debido a que muchos de los equipos son de producción y contienen información y procesos muy sensibles, y luego de realizar el análisis con el personal a cargo, se

decidió aplicar la implementación y configuraciones en un grupo de equipos de la DMZ con el fin de no poner en riesgo la operatividad de todos los servicios que brinda esta área crítica de la institución, se define un alcance basado en los mismos objetivos , por lo tanto, se trabajó con los equipos descritos a continuación en la tabla 2.

TABLA 2. DETERMINACIÓN DE LA POBLACIÓN

EQUIPO	Número de Equipo
Servidor de Bases de Datos	1
Servidor WEB	2
Servidor Active Directory	3
Firewall	4
Switch Distribución	5
Antivirus Central	6
Servidor genérico	7
Total	**7**

3.6 Recolección de información

Selección de las técnicas a emplear en el proceso de recolección de información

Para la obtención de la información en la etapa inicial de diagnóstico se utilizó la técnica de la observación para la recopilación de información de activos que formarán parte del estudio, así como la aplicación de la técnica de la entrevista, la cual estuvo dirigida al director de Tecnologías de Información y Comunicación institucional.

En la fase de implementación de la solución se aplicó la técnica de la observación para el análisis de logs capturados a través del uso de la herramienta informática seleccionada.

Instrumentos de recopilación de información

Lista de cotejo: Instrumento de evaluación que logra detallar los criterios a seguir para resolver con eficacia actividades de aprendizaje.

Guion de Entrevista: A través de un guion de entrevista para obtener la información que permite conocer la situación inicial de la gestión de seguridad en la red institucional. Se encuentra en Anexo 3.

La Validez de expertos es el grado en que un instrumento realmente mide la variable de interés, de acuerdo con expertos en el tema. (Hernández Sampieri, 2014).

Se validó la confiabilidad del guion de entrevista estructurada a través del criterio de tres expertos, los mismos que forman parte del personal de la Dirección de Tecnologías de Información de la Universidad.

La Observación: Permite explorar y describir lugares para comprender su significado, así como facilita comprender procesos, situaciones, eventos en un momento determinado.

Para determinar la diferencia entre los logs locales ubicados en cada equipo en comparación con los logs centralizados ubicados en el servidor, se utilizó la técnica de la observación no participante mediante una lista de cotejo. Ver Tabla 7.

3.7 Procesamiento de la información y análisis estadístico

Análisis de la Observación

La aplicación de la técnica de la observación con la finalidad de obtener información acerca los diversos activos que conforman la red DMZ permitirá tener una idea clara en el desarrollo del presente proyecto.

Análisis de la Entrevista

La entrevista aplicada al director de Tecnologías Institucional fue realizada con la finalidad de conocer información destacada que permita definir los procesos que conduzcan al mejoramiento de la gestión de seguridad informática a través de la implementación de una herramienta SIEM.

Análisis Estadístico de la lista de cotejo

Una vez obtenida la información en base a la lista de cotejo se ingresó los datos al programa Microsoft Excel 2016 para aplicar la función estadística apropiada que nos permita obtener los resultados presentados en la tabla 9.

Plan de Análisis e Interpretación de Resultados

Al contar con valores dados por las fichas de cotejo en la cual se divide en datos de logs locales pertenecientes a los hosts seleccionados y en datos de logs centralizados que están localizados en el servidor SIEM, los mismos que constan con aplicación de filtros basados en reglas, se ha decidido trabajar con el estadístico t para muestras apareadas.

3.8 Variables respuesta o resultados alcanzados

En la tabla 3, se muestra los resultados obtenidos después del empleo de las técnicas de recolección de información aplicadas.

TABLA 3. VARIABLES DE RESPUESTA

Variable	Definición	Dimensión	Indicador	Técnica/Instrumento

Servidores	Computador especializado utilizado para almacenar información y brindar servicios centralizados	Servidor WEB Servidor BD Active Directory	Ataques y Vulnerabilidades Inyección SQL Ataques de Fuerza Bruta	Entrevista/ Guion de Entrevista Entrevista/Guion de Entrevista Entrevista/Guion de Entrevista
Dispositivos de red	Activo que cumple una función específica en un segmento de la red	Firewall Switches	Malas configuraciones Acceso no autorizado	Entrevista/Guion de Entrevista Entrevista/Guion de Entrevista
Dispositivos de seguridad	Cada uno de los componentes que permiten fortalecer la seguridad de la red	Antivirus Central	Ataques de Fuerza Bruta	Entrevista/Guion de Entrevista
Servidor en general	Servidor que puede tener un perfil determinado	Servidor de archivos, aplicaciones, seguridad	Escaneo de puertos	Entrevista/Guion de Entrevista

Los ataques informáticos	Aprovechar alguna debilidad o falla en hardware o software causando un efecto negativo en la seguridad del sistema.	Amenazas	Network IDS, Host IDS	Observación/Lista de cotejo
		Vulnerabilidades	Monitoreo continuo	Observación/Lista de cotejo
		Ataques	Correlación de eventos	Observación/Lista de cotejo

Metodología o estrategia empleada

Fase 1

Diagnosticar los ataques informáticos que representen riesgos en la red DMZ institucional

Actualmente el procedimiento para detectar ataques y vulnerabilidades en la red DMZ institucional se apoya principalmente en uso del firewall y en varias herramientas para búsqueda de vulnerabilidades que ofrecen posibles alternativas de solución, además existe una solución antivirus para cada equipo en la institución.

Mediante la ejecución de tareas programadas las herramientas obtienen información importante que ayudan a solventar inconvenientes de seguridad en los activos de la red. El firewall institucional brinda opciones de seguridad y servicios apoyado en la aplicación de políticas institucionales de seguridad de la información que ayudan a administrarla de una manera más eficiente.

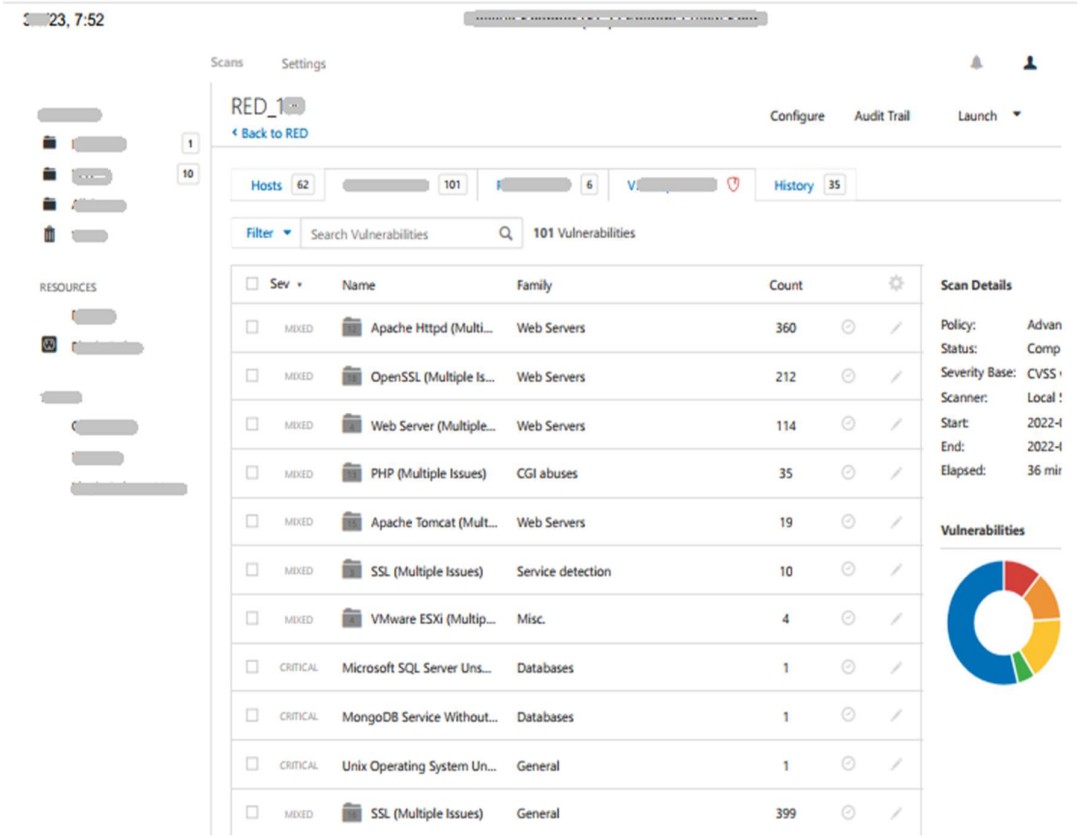


Figura 3. Uso actual de herramientas para detección de vulnerabilidades.

Fase 2

Analizar soluciones de tipo SIEM basados en software libre para su aplicación

Herramientas SIEM Open Source

Con el fin de encontrar una solución que permita cubrir las necesidades de la institución sin que esto implique gastar grandes sumas de dinero y que incluso podrían ser periódicas, pero también considerando que la herramienta cumpla con los requisitos necesarios se ha analizado algunas herramientas SIEM de tipo Open Source:

- OSSEC. – Es un sistema de detección de intrusos basado en host de código abierto. Su función consiste en el análisis de registros, verificación de integridad, monitoreo del registro de Windows, detección de rootkits. Se ejecuta en los sistemas operativos más usados como son Linux, OpenBSD, FreeBSD, Mac OS X, Solaris y Windows.
- NXlog. – Es una herramienta que recopila y reenvía registros, compatible con diversas plataformas. Posee altas capacidades de filtrado de mensajes y reescritura de registros, Posee una arquitectura modular y multiproceso. Su sistema permite recopilar registros de la red remotamente a través de UDP, TCP o TLS/SSL. Es compatible con plataformas como Windows, Linux, Android, Open BSD.
- AlienVault OSSIM. – Es una herramienta muy completa que permite la recopilación, normalización y correlación de eventos de seguridad. Cuenta con experiencia en el área de tal manera que la herramienta se ajusta a la necesidad de cada organización, posee fácil administración.
- Apache Metron. – Es una herramienta que contiene varias soluciones de código abierto en una consola centralizada. Posee capacidades de agregación de registros, índices de captura de paquetes, análisis de comportamiento, almacenamiento.
- ELK Stack. – Posee una colección de tres productos de código abierto: Elasticsearch, Logstash y Kibana las cuales se puede utilizar para visualización y el análisis de eventos de TI. Tiene indexación y almacenamiento de datos de series temporales.

Comparativa para selección de herramienta adecuada

TABLA 4. COMPARATIVA DE HERRAMIENTAS SIEM OPEN SOURCE

Características	**OSSEC**	**NXlog**	**OSSIM**	**Apache Metron**	**ELK Stack**
Gestión Centralizada	X	X	X	X	X
Recolección 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 de Eventos	X	X	X		X
Monitoreo en tiempo real	X		X	X	X

Normalización	X	X	X	X	X
Descubrimiento de Activos			X		
Reportes	X	X	X	X	X
Interfaz gráfica	X	X	X	X	X
Modo recolección de Eventos	Agente/Sin Agente	Agente/Sin Agente	Agente/Sin Agente	Agente	Agente
Soporte LINUX	X	X	X	X	X
Soporte Windows	X	X	X		X
Soporte MAC	X		X		X
Soporte BSD	X	X	X		

Selección de la herramienta

Una vez realizado el análisis de características principales que posee cada una de las herramientas SIEM para la integración de un correlacionador de LOGS en la red DMZ institucional, se escoge la herramienta AlienVault OSSIM, debido a que cuenta con mejores características técnicas, flexibilidad de configuración y facilidad de uso, tal como se evidencia en la tabla 4.

Las características de administración y monitoreo de seguridad de OSSIM se valoran con base en su capacidad de recopilar datos de dispositivos, transformar los datos en un conjunto común de campos de datos que definen eventos, luego procesan, filtran y correlacionan los eventos para identificar posibles amenazas y vulnerabilidades.

Componentes de AlienVault OSSIM

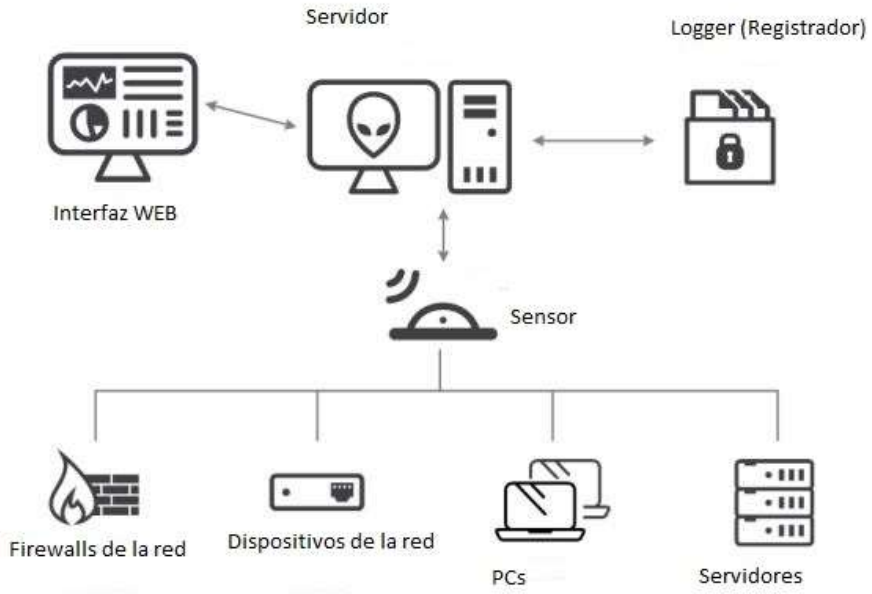


Figura 4. Componentes de AlienVault OSSIM

Nota. Adaptado de USM Appliance Deployment Guide (2021)

Los tres componentes principales de AlienVault que trabajan juntos para monitorear y proveer seguridad en el entorno son:

Sensor OSSIM. – Su función es recopilar y normalizar la información de los activos que forman parte de la red. El sistema posee una gran variedad de complementos para procesar registros y datos sin procesar de los diferentes equipos que se encuentran en el segmento de red monitoreado

Servidor OSSIM. – Cumple la función de agregar y correlacionar información que el sensor recopila. Brinda gestión, generación de informes y administración desde el panel de interfaz web de usuario.

Logger (USM). – Su tarea es archivar de manera segura los eventos sin procesar para investigación forense, USM Appliance Deployment Guide (2021). Este componente no se incluye en la versión libre AlienVault OSSIM.

Herramientas integradas en AlienVault OSSIM

AlienVault OSSIM posee herramientas integradas que son un conjunto de aplicaciones que lo convierten en un robusto sistema SIEM que ha ido madurando con el transcurrir de los años. Entre las más importantes mencionamos OSSEC, SNORT, OPENVAS, ARPWATCH, las mismas que se describen a continuación:

TABLA 5. HERRAMIENTAS PRINCIPALES INTEGRADAS EN ALIENVAULT OSSIM

Herramienta	**Función principal**
Pads (pasiva)	Anomalías y detección de nuevos servicios.
ArpWatch (pasiva)	Detección de anomalías en las direcciones MAC a partir de tráfico generado por los activos de la red ArpWatch identifica cambios en las direcciones MAC asociadas a cada dirección IP. Utilidad en OSSIM: Inventario, cambio de IP, ARPSpoofing.
Snort	NDIS. Escaneo de puertos. Gusanos. Malware. Violaciones.
Nepenthes (pasiva)	Honeypot. Nepenthes emula servicios y vulnerabilidades conocidas con el objeto de recoger información de los atacantes. Utilidad en OSSIM: conocer qué equipos están infectados. Creación de directivas y firmas en base a ataques. Colección de malware.
OSVDB (activa)	Creación de reglas de correlación. Relación a identificadores de cada vulnerabilidad. Complementa la información ofrecida por OpenVas.

Nagios (activa)	Utilidad en OSSIM. Disponibilidad de los activos. Puede realizar comprobaciones en remoto o disponiendo de un agente en la máquina monitorizada. Dispone de un gran número de plugins para diferentes entornos y herramientas.
P0f (activa)	Detección de cambios de Sistema Operativo. Gestión de Inventario. Accesos no autorizados en la red.
Ntop (activa)	Estadísticas de uso de la red. Información sobre activos. Detección de abuso de la red.
Netflow (activa)	Protocolo de red de Cisco para información de tráfico analizado.
Kismet (pasiva)	Sniffer y detector de intrusos en redes Wireless. Utilidad en OSSIM: Serialización de redes inalámbricas. Detección de varios AP. Cumplimiento de normativa (PCI).
Nmap (activa)	Escáner de puertos. Nmap escanea redes y equipos mediante un escaneo configurable. Utilidad en OSSIM: Descubrimiento de activos. identifica puertos abiertos. Determina qué servicios se están ejecutando. Determina qué sistema operativo y versión utiliza. Obtiene algunas características del hardware de red los activos escaneados.
OSSEC (activa)	OSSEC es una arquitectura agentes-servidor. En OSSIM recoge los eventos colectados en el servidor OSSEC.
OCS (activa)	Sistema de agentes distribuidos en cada máquina. Recoge información para el inventario de cada máquina.
OpenVas (activa)	Escaneo de vulnerabilidades. Prevención de ataques. Permite definir la agresividad de los escaneos que realiza.

Nota. Adaptado de Ferruzola, Bermeo & Arévalo (2022).

Capacidades y Herramientas relacionadas de OSSIM

AlienVault OSSIM tiene la capacidad de: Descubrir activos, evaluar vulnerabilidades, detectar intrusos, controlar el comportamiento, visualizar

información en tiempo real. Además, tiene la capacidad de implementar reglas de correlación personalizadas y, configurar complementos (plugins) de acuerdo con la necesidad.

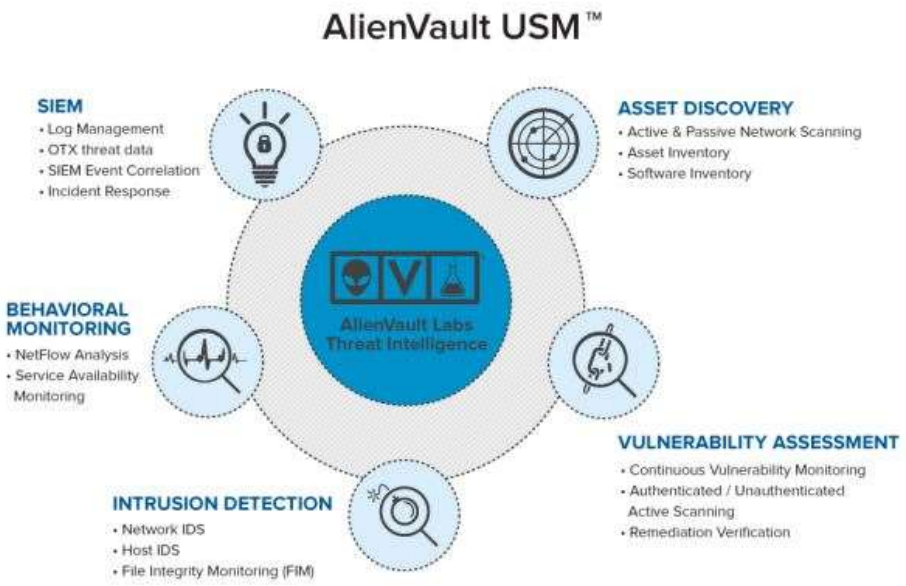


Figura 5. Capacidades y Herramientas relacionadas que conforman OSSIM-USM

Nota. Adaptado de USM Appliance User Guide (2021)

Descubrimiento de activos. - A través de las herramientas integradas relacionadas a inventario brinda la visibilidad de los dispositivos que se encuentran en la red. Las características incluyen:

- Escaneo de red activo y pasivo.
- Inventario de activos
- Inventario de servicios

Evaluación de vulnerabilidades. – Reconoce activos y dispositivos cuyo software carezca de parches, configuraciones inseguras y otras vulnerabilidades en la red. Características:

- Monitoreo continuo de vulnerabilidades

- Escaneo activo autenticado / no autenticado
- Verificación de remediación

Detección de intrusos. – Organiza la respuesta a incidentes, gestiona las amenazas a través de tecnologías de red de seguridad integradas. Características:

- IDS basado en red (NIDS)
- IDS basado en host (HIDS)
- Supervisión de integridad de archivos (FIM)

Supervisión de comportamiento. – Detecta anomalías y otros patrones sobre nuevas amenazas, también indica el comportamientos sospechosos e infracciones políticas de usuarios y dispositivos no autorizados. Características:

- Análisis de Netflow
- Supervisión de la disponibilidad del servicio
- Análisis de protocolo de red / captura de paquetes

Administración de eventos e información de seguridad (SIEM). – Permite que identifique y corrija amenazas en la red dando importancia al riesgo y la respuesta. Características:

- Datos de amenazas OTX integrado (en versión OSSIM es limitado)
- Correlación de eventos SIEM
- Respuesta a incidentes

Fase 3

Implementación de la herramienta SIEM seleccionada para la detección de ataques informáticos

Una vez determinada la población en la cual se aplicará el proyecto como se señala en la tabla 3, se procede a instalar, configurar y emplear las actividades adicionales para que la herramienta funcione de acuerdo con las necesidades.

Se cumplen las siguientes actividades:

Instalación de AlienVault OSSIM
Descubrir Activos y Redes en el segmento
Añadir agentes HIDS
Habilitación Complementos (Plugins)
Definición de Políticas y Acciones en Activos Monitoreados
Comprobación de políticas a través de ataques y vulnerabilidades en activos seleccionados

Instalación de AlienVault OSSIM

Requerimientos de hardware:

Servidor. Para la implementación de esta aplicación la Universidad cuenta con un servidor adecuado, el cual posee las siguientes características:

- Procesador 8 núcleos
- 16 GB RAM
- 500 GB Almacenamiento
- 2 tarjetas de red Ethernet 1 GBPS

El programa se descarga desde el sitio oficial
https://cybersecurity.att.com/products/ossim/download

El detalle de la instalación se muestra en el Anexo 3.

Descubrir Activos en la Red

Permite al sistema conocer todo su entorno para identificar amenazas y vulnerabilidades.

En esta sección puede:

- Escanear las redes y encontrar activos

- Ingresar activos manualmente.
- Importar activos desde un archivo CSV

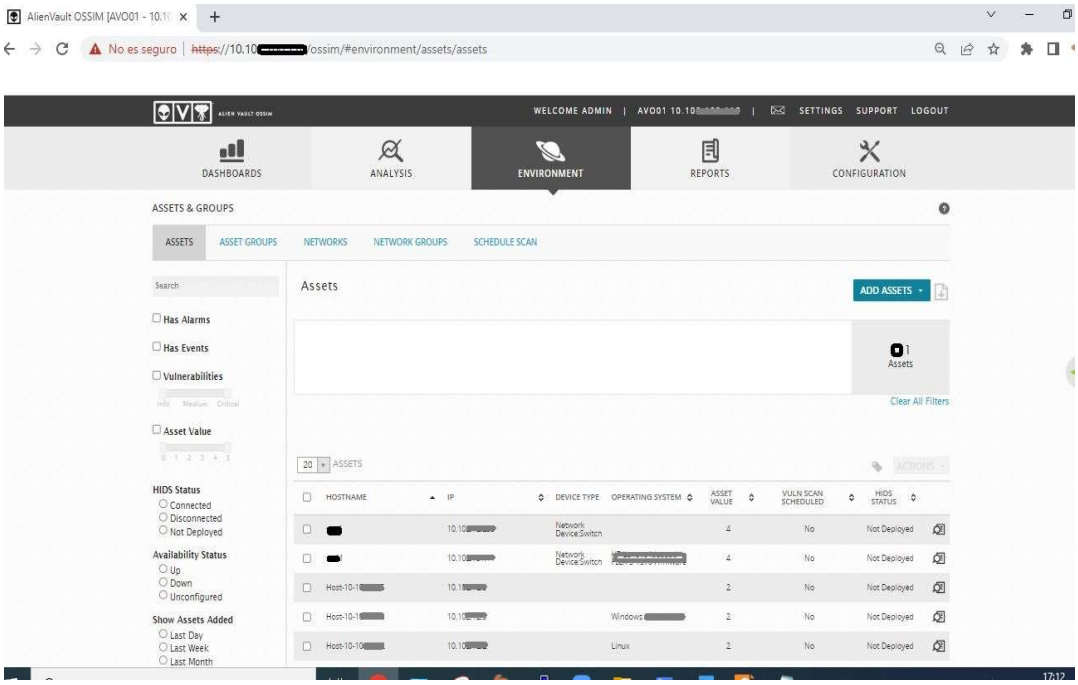


Figura 6. Pantalla Activos

Configuración de Dispositivos para Monitorear

Para realizar las pruebas y determinar resultados como se indicó en la tabla 3, se procede a configurar los activos seleccionados.

Añadir agentes HIDS

Implementación en Servidores

Se recomienda implementar un sistema de detección de intrusos para:

- Supervisar la integridad de archivos
- Detectar rootkits
- Recopilar registros de eventos

Para servidores Windows

El proceso es a través de la interfaz web y consta de los siguientes pasos:

1. Estando ubicado en el activo hacer clic en el botón Actions, escoger la opción Deploy HIDS Agent.
2. Ingresamos un usuario y contraseña de una cuenta del activo con propiedades de administrador y luego hacemos clic en el botón Deploy.
3. Para conectar el agente HIDS recién creado con el servidor:

a. Ir a Enviroment/Detection / Agents

Se mostrará la lista de agentes HIDS

b. Seleccione el agente HIDS sin valor en la columna Activo y haga clic en el enlace. y aparecerá la página conectar un activo al agente HIDS
c. Escriba la dirección IP del activo
d. Hacer clic en botón Save

Para servidores LINUX

Para añadir un agente HIDS en la herramienta OSSIM

1. Ir a Enviroment/ Detection
2. Ir a HIDS/Agents/Agent Control/Add Agent
3. En New Agent, seleccionar el host desde el árbol de hosts.

En esta parte se debe definir el nombre del agente con el nombre del Host y la IP respectivamente.

4. Hacemos clic en Save para grabar.
5. En esta instancia ya podemos extraer el código para el agente haciendo clic en el icono de llave y procedemos a copiar.
6. En el host Linux ingresamos a través de consola y ejecutamos "/var/ossec/bin/manage_agent" y presionamos enter, luego escogemos "I" para importar el código que fue previamente copiado en la interfaz web de OSSIM.
7. Luego editamos el archivo de configuración de agentes digitando en donde se especifica la ip del servidor OSSIM "/var/ossec/etc/ossec.conf".
8. Iniciamos el agente HIDS desde la carpeta /var/ossec/bin si aún no se está ejecutando con la siguiente instrucción:

. /ossec-control start , luego verificamos con la siguiente instrucción:

. /ossec-control status

9. Finalmente ejecutamos el siguiente comando para que se inicie el servicio cada vez que el equipo se reinicie:

chkconfig ossec-hids on

Habilitación Complementos (Plugins)

AlienVault OSSIM brinda la lógica para extraer datos específicos de seguridad de dispositivos para producir eventos administrados por el servidor OSSIM. Esta herramienta incluye una lista amplia de fuentes de datos comunes que permita gestionar los eventos (Cybersecurity AT&T, 2021)

Los complementos se pueden agregar de varias maneras, independientemente en activos, de manera general desde el Sensor, o creando manualmente un nuevo complemento a través de la consola.

En el Anexo 2 se explica la configuración en dispositivos LINUX, Windows, y equipos activos de red como Switch.

Para comprobar la llegada de logs a sensor desde equipos Linux se muestra a continuación:

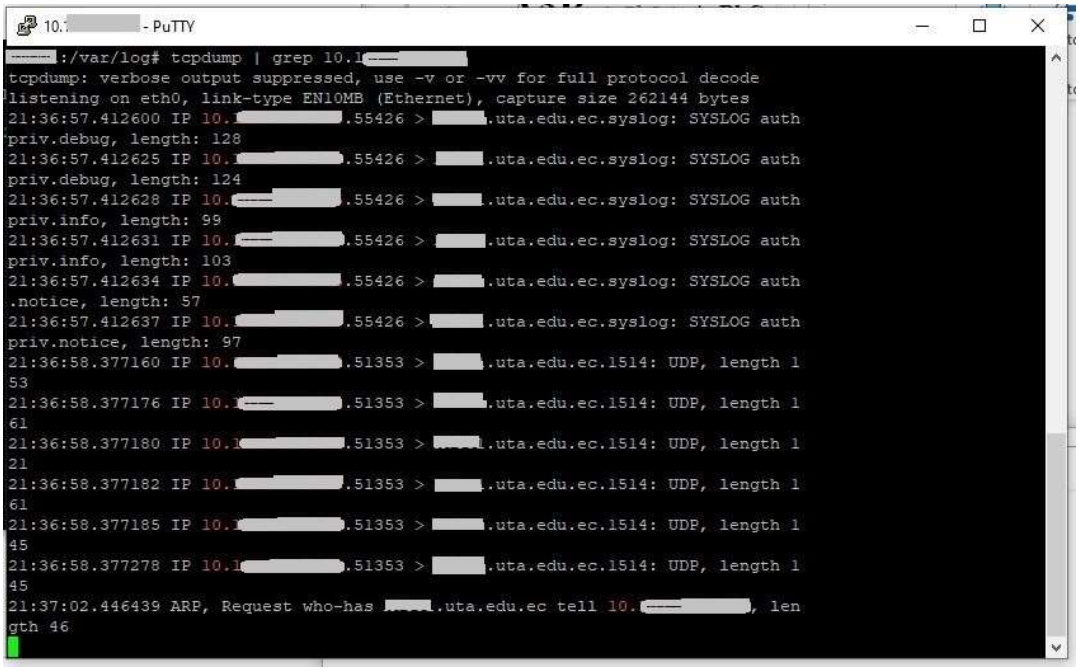


Figura 7. Comprobación llegada de logs desde host Linux con complemento personalizado

Para comprobar la llegada de logs a sensor desde equipos Windows se muestra a continuación:

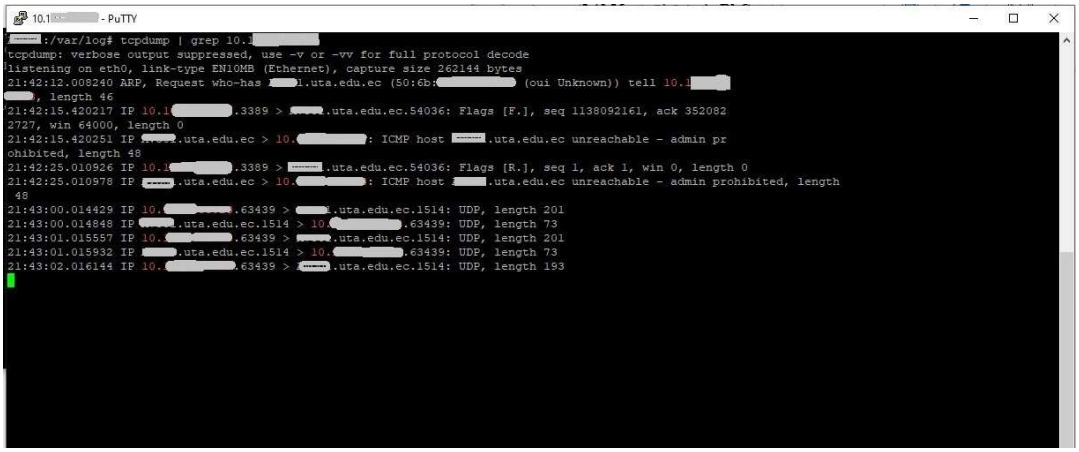


Figura 8. Comprobación llegada de logs desde host Windows con complemento personalizado

Para comprobar la llegada de logs a sensor desde equipo Switch1 se muestra a continuación:

Figura 9. Comprobación llegada de logs desde equipo switch

Para comprobar la llegada de logs a sensor desde equipo Firewall, se muestra a continuación:

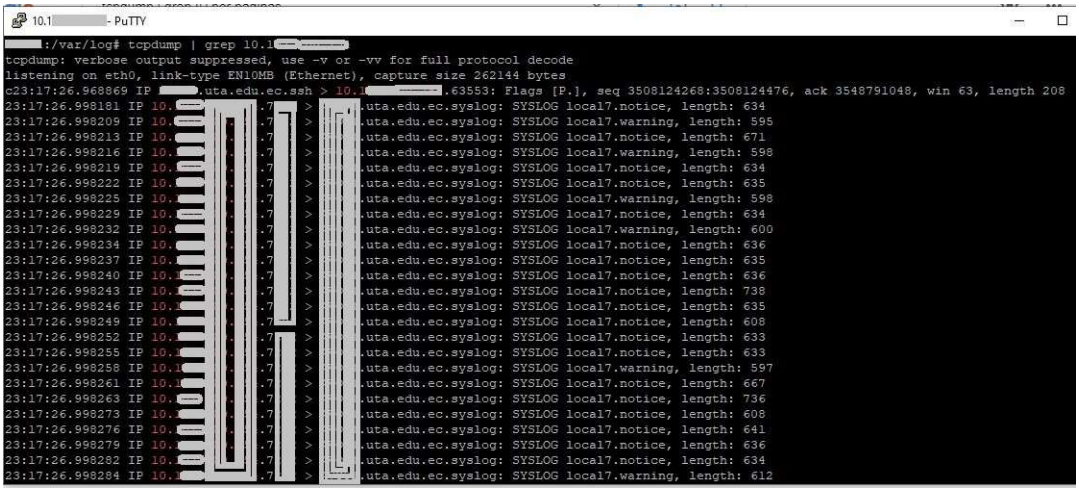


Figura 10. Comprobación llegada de logs desde equipo Firewall

Definición de Políticas y Acciones en Activos Monitoreados

Crear políticas que serán aplicadas en la gestión de activos los realizamos a través de la interfaz web de la herramienta OSSIM en la sección Configuration/Threat Intelligence/Policy

Activo: Servidor BD1

Política: Detectar ataque XSS

Acción: Crear un tique en el cual se informe a través de qué IP, puerto origen y destino se realizó.

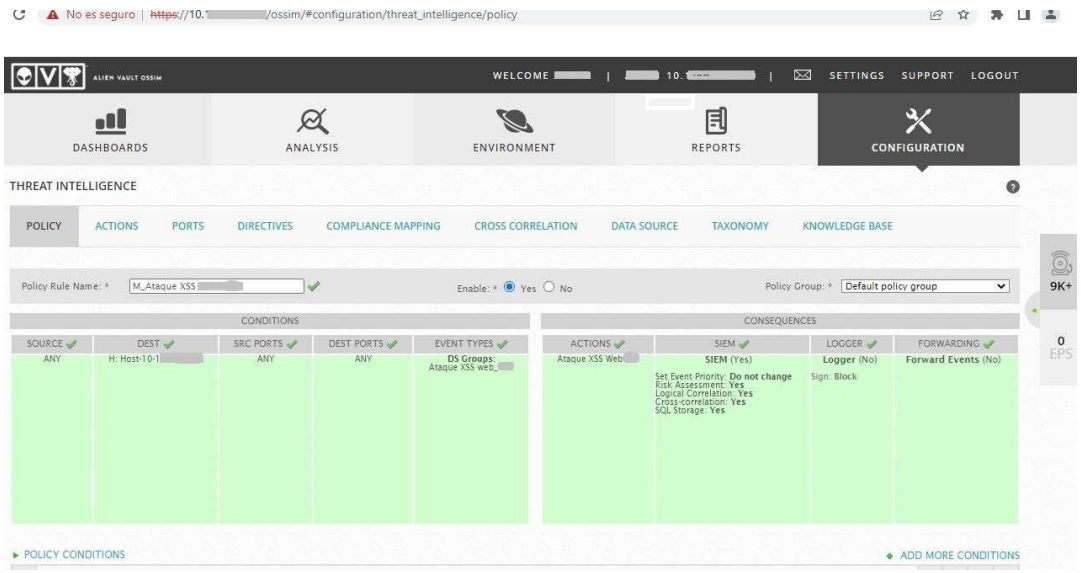


Figura 11. Creación de política para detectar ataques XSS en activo BD1

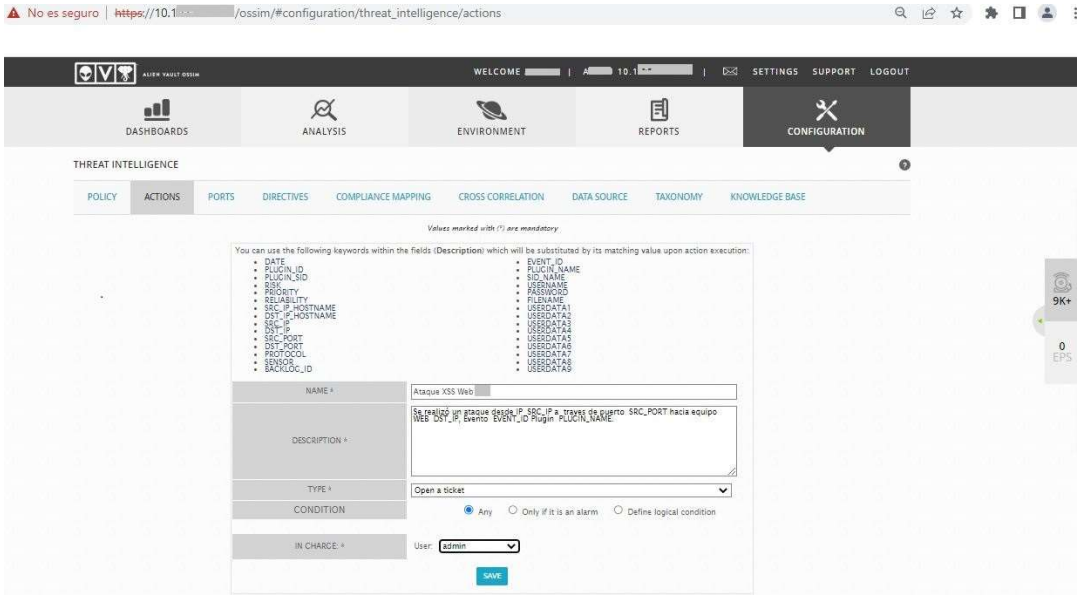


Figura 12. Definición de acción una vez detectados ataques XSS en activo BD1

Activo: Servidor WEB1

Política: Detectar ataque de Inyección de SQL en este activo

Acción: Crear un tique para informar del evento.

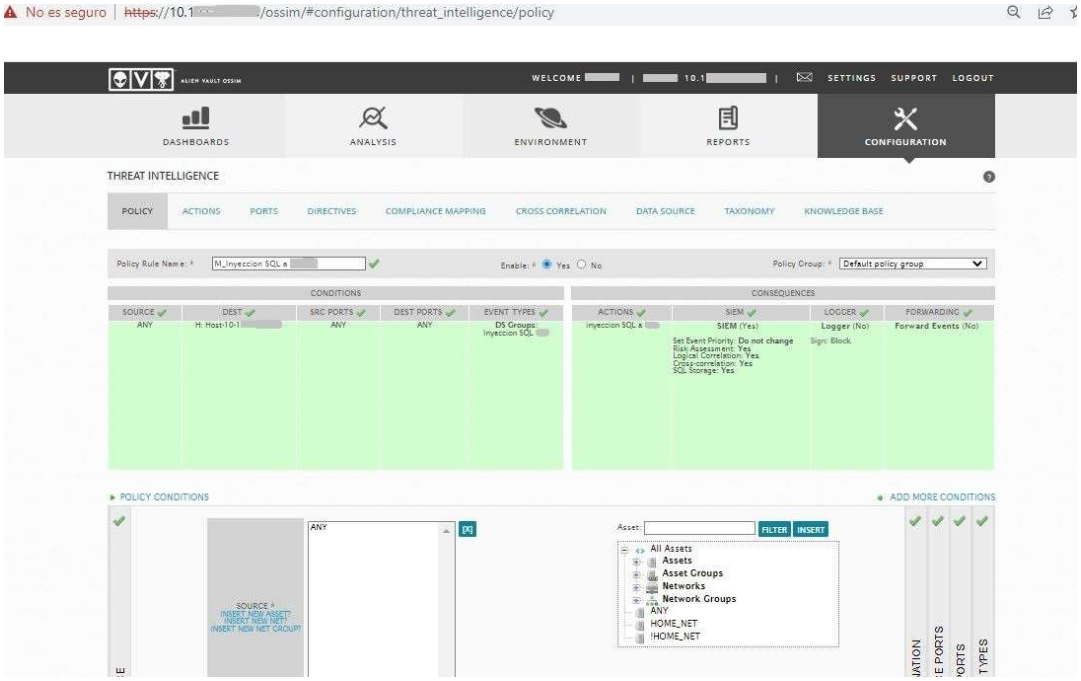


Figura 13. Creación de política para detectar Inyección SQL en activo Servidor WEB1

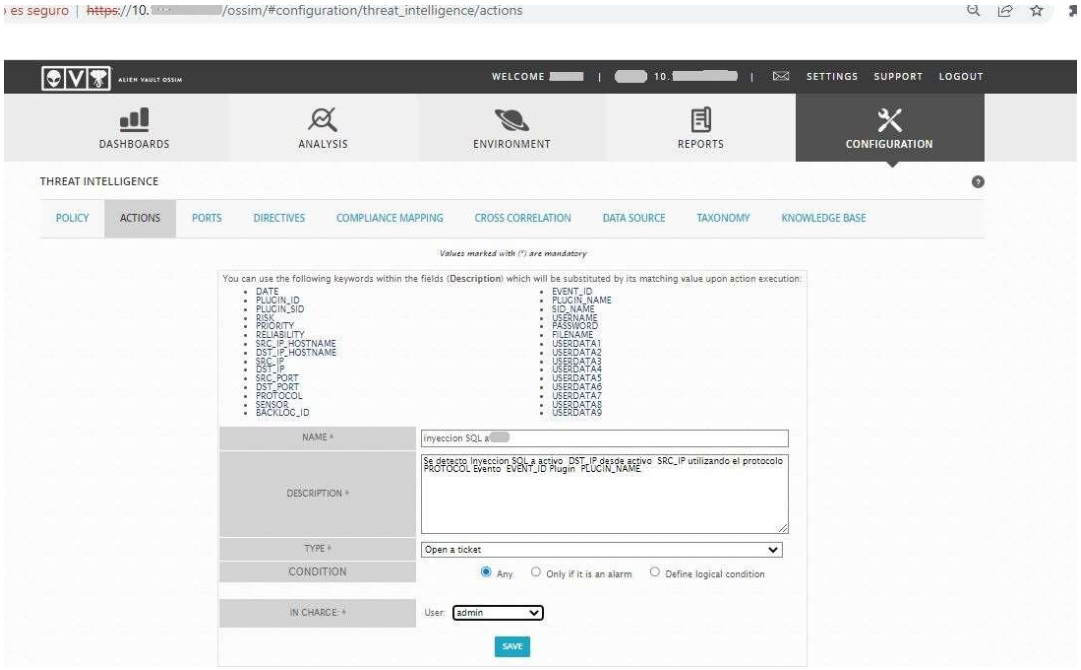


Figura 14. Definición de acción una vez detectado Inyección SQL en activo WEB1

Activos: Servidores de Active Directory

Política: Detectar ataque de Fuerza Bruta en estos activos

Acción: Crear un tique para informar del evento.

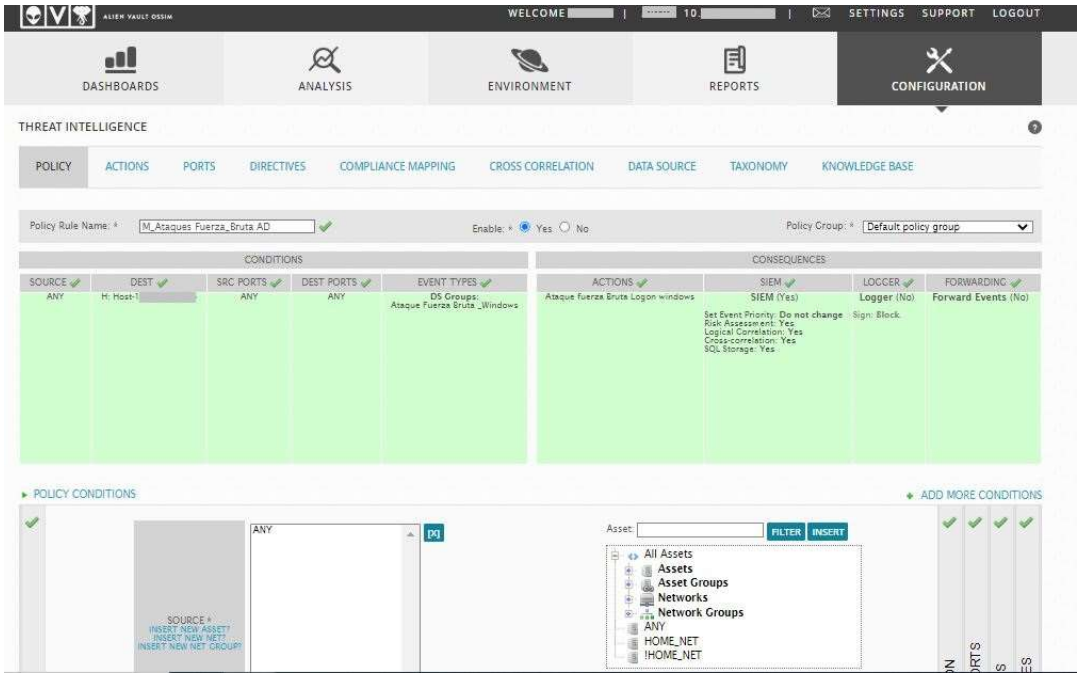


Figura 15. Creación de política para detectar ataque de Fuerza Bruta en activo Active Directory

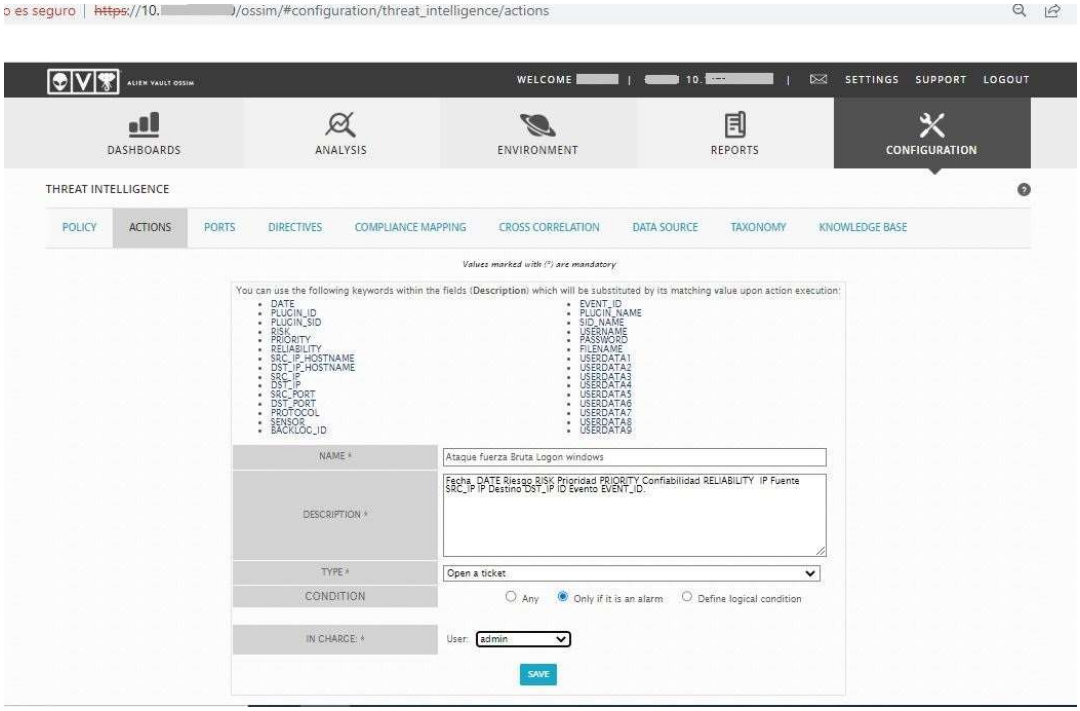


Figura 16. Definición de acción una vez detectado ataque de Fuerza Bruta en activo AD

Activo: Switch1

Política: Detectar ataque de Fuerza Bruta en este activo

Acción: Crear un tique para informar del evento.

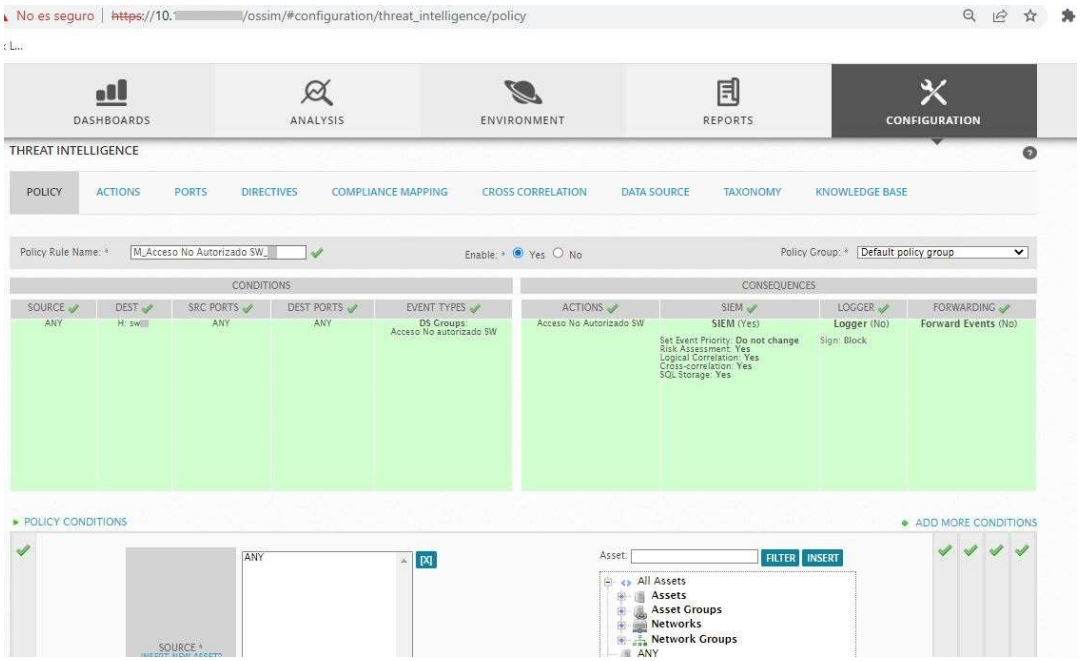


Figura 17. Creación de política para detectar ataque de Fuerza Bruta en activo Switch1

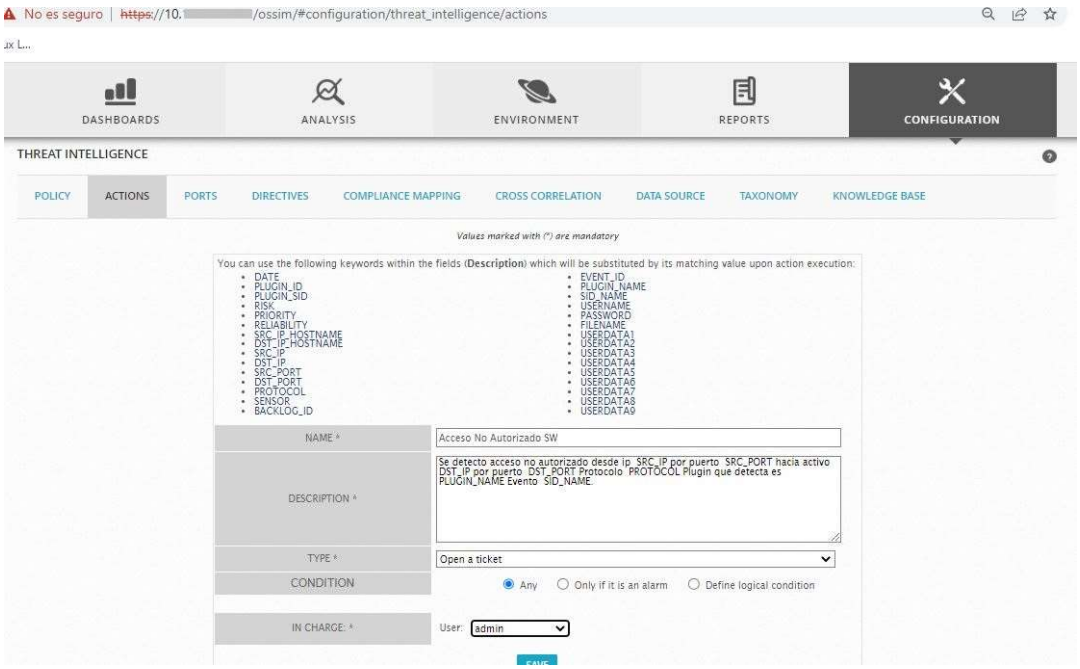


Figura 18. Definición de acción una vez detectado ataque de Fuerza Bruta en activo Switch1

Comprobación de políticas a través de ataques y vulnerabilidades en activos seleccionados

Los resultados de la comprobación de políticas a través de ataques y vulnerabilidades en activos seleccionados se evidencian a continuación.

Activo: Servidor BD1

Política: Detectar ataque XSS

Acción: Crear un tique en el cual se informe a través de qué IP, puerto origen y destino se realizó.

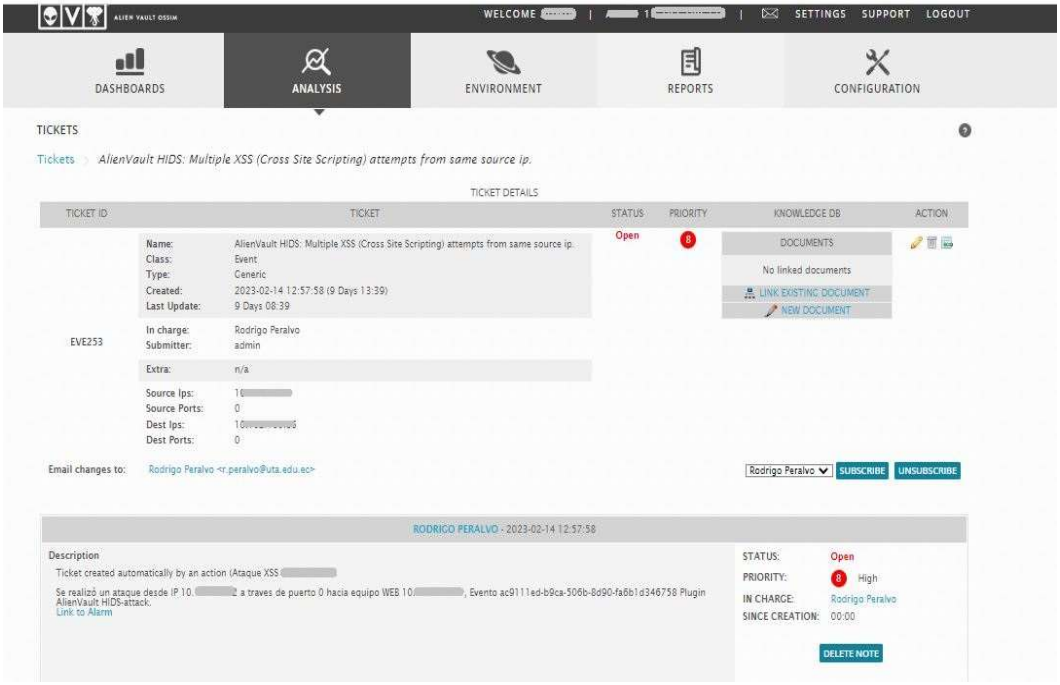


Figura 19. Debido a ataque XSS, el sistema genera un tique para su revisión

Activo: Servidor WEB1

Política: Detectar ataque de Inyección de SQL en este activo

Acción: Crear un tique para informar del evento.

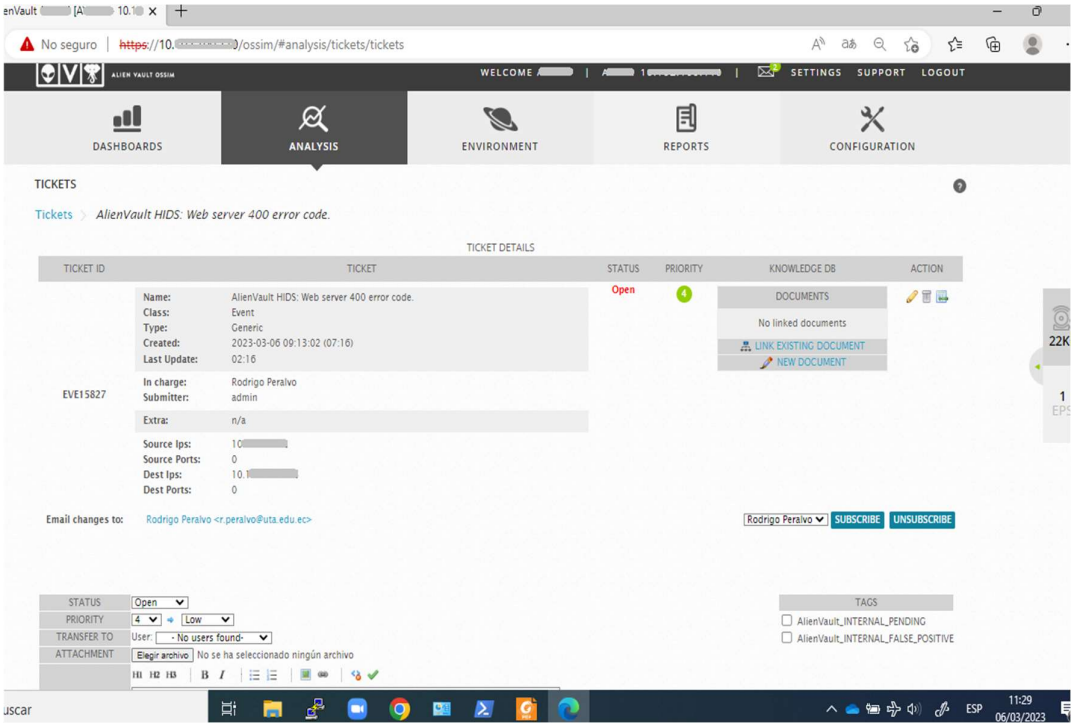


Figura 20. Debido a un ataque Inyección de SQL, el sistema genera un tique para su revisión

Activos: Servidores de Active Directory

Política: Detectar ataque de Fuerza Bruta en estos activos

Acción: Crear un tique para informar del evento.

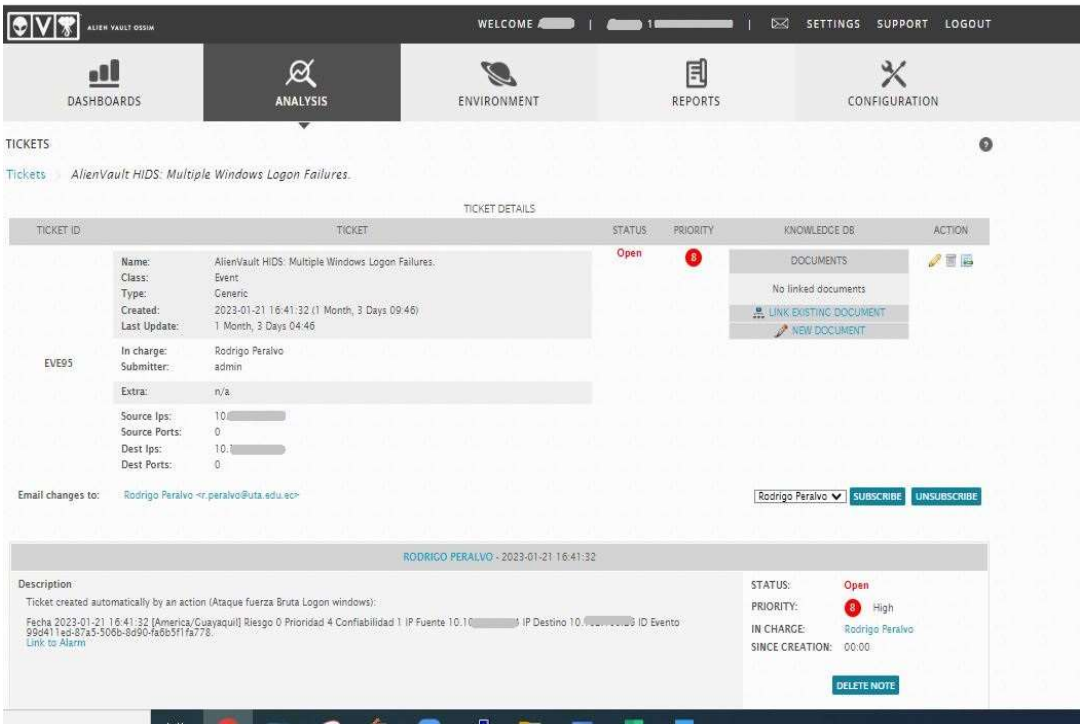


Figura 21. Debido a ataque de Fuerza Bruta, el sistema genera un tique para su revisión

Activo: Switch1

Política: Detectar ataque de Fuerza Bruta en este activo

Acción: Crear un tique para informar del evento.

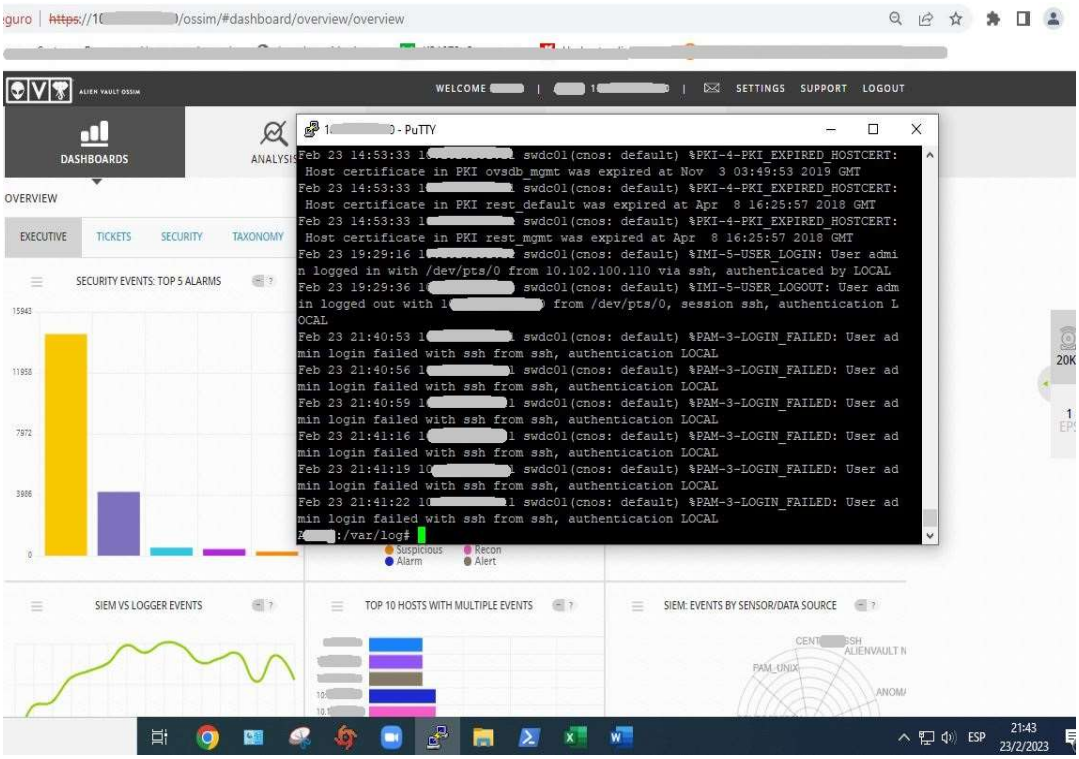


Figura 22. Debido a ataque de Fuerza Bruta, a través de modo consola se puede evidenciar los datos

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Análisis de los resultados

4.1.1 Resultados Pre-Implementación

Observación

El resultado de la aplicación de la técnica de la observación consta en la tabla 6.

TABLA 6. RESULTADO DE LA OBSERVACIÓN

Activo	**Principales funciones**	**Principales Amenazas**
Servidor WEB	Almacena y transmite información solicitada de un sitio web a navegador de usuario.	Control de acceso roto. fallas criptográficas. Inyección (SQL, XSS). Diseño inseguro. configuración incorrecta de seguridad. entre otros.
Servidor de Base de Datos	Equipo especializado que almacena y organiza la información en tablas, índices y registros.	Inyección SQL. Copias no autorizadas de datos confidenciales. explotación de

		bases de datos vulnerables y mal configuradas.
Servidor Active Directory	Equipo que contiene servicios como Almacenamiento y estructura de AD. Roles de controlador de dominio. Interoperación con DNS y directiva de grupo, Descripción de confianza.	Privilegios excesivos. usuarios con permisos para agregar equipos al dominio. Almacenar contraseñas usando hashes LM.
Switches	Maneja Vlans. Seguridad en puertos. Autenticación/Control de acceso. Monitorización. QoS. Redundancia.	Vulnerabilidad de ejecución remota. Falla de omisión de autenticación. Falla de inyección de comandos.
Dispositivos de Almacenamiento	Equipos que brindan almacenamiento y uso compartido de archivos. Almacenan imágenes y videos de acceso frecuente. Crean repositorio interno.	Acceso no autorizado.
Servidores en general	Equipo que permite almacenamiento de archivos, bases de	Servicios inutilizados y puertos abiertos.

	datos, servicios y protocolos de comunicación.	Servicios sin sus parches. Administración desatendida. Servicios intrínsecamente inseguros.
Servidores virtuales	Equipo virtual que funciona de acuerdo con recursos asignados dentro de un servidor físico.	Las vulnerabilidades de los entornos físicos son también aplicables a los entornos virtuales.

Entrevista al director de Tecnologías UTA-DITIC

El resultado de la Entrevista facilitó el análisis de la importancia y necesidad de disponer de más y mejores herramientas tecnológicas que permitan minimizar el riesgo de amenazas informáticas en el área de la DMZ institucional. Permitió conocer cómo se maneja actualmente la seguridad informática en este segmento de red, así como las herramientas y procedimientos que se aplican para gestionar las vulnerabilidades y ataques informáticos.

4.1.2 Resultados Pos-Implementación

A través de la implementación de la herramienta AlienVault OSSIM se logró validar la recolección, normalización, análisis y correlación de eventos facilitado por esta herramienta que ofrece la gestión mediante interfaz gráfica.

La recolección de datos de logs que se encuentran en equipos locales y de los logs que se encuentran centralizados en la herramienta OSSIM se obtuvo de la siguiente manera, para la toma de datos de logs locales en cada uno de los activos se realizó a través de la captura de texto plano de los archivos que contiene la información, para la toma de datos de los logs centralizados que se encuentran en el sensor de OSSIM se realizó a través de consultas filtradas en la interfaz Web de la herramienta. La información recolectada se evidencia en la tabla 7.

TABLA 7. TOMA DE DATOS DE LOGS LOCALES Y LOGS CENTRALIZADOS

Activo	**Fecha**	**Hora Inicio**	**Hora Final**	**Logs Local**	**Logs Centr.**
WEB1	29/01/2023	08:00:00	12:59:00	111	7
BD1	30/01/2023	08:00:00	12:59:00	49	9
AD1	02/02/2023	07:30:40	07:31:00	138	43
Firewall1	30/01/2023	23:03:23	23:04:28	97	2
SW1	18/01/2023	08:30:00	21:30:00	12	2
AV	29/01/2023	11:00:00	11:59:00	32	4
Serv. Genérico	29/01/2023	08:00:00	12:00:00	80	7

4.1.2.1 Activo Servidor BD1

Al recoger eventos localizados en el activo Base de Datos 1, muestra una cantidad de 49 logs para ser tratados, luego, en el Sensor OSSIM son normalizados y finalmente en el módulo servidor OSSIM estos eventos que fueron agregados están listos para brindar información en el sistema de qué eventos son naturales o preocupantes, muestra a través de la interfaz gráfica 9 logs pertenecientes al activo BD1, lo cual indica una cantidad menor, esto debido a que el sistema filtró los eventos en base a políticas, directivas y procedimientos con los mismos. La figura 23 muestra su resultado.

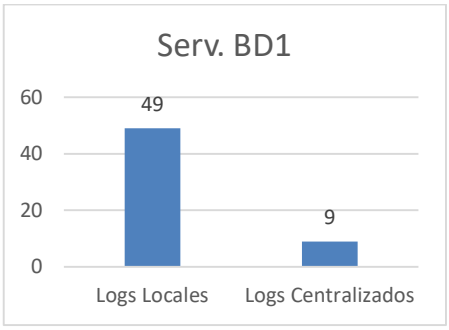


Figura 23. Eventos locales en activo BD1 origen comparados con eventos centralizados en servidor OSSIM

4.1.2.2 Activo Servidor WEB1

Al recoger eventos localizados en el activo Servidor WEB1, muestra una cantidad de 111 logs para ser tratados, luego, en el Sensor OSSIM son normalizados y finalmente en el módulo servidor OSSIM estos eventos que fueron agregados están listos para brindar información en el sistema de qué eventos son naturales o preocupantes, muestra a través de la interfaz gráfica 7 logs pertenecientes al activo WEB1, lo cual indica una cantidad menor, esto debido a que el sistema filtró los eventos en base a políticas, directivas y procedimientos con los mismos. La figura 24 muestra su resultado.

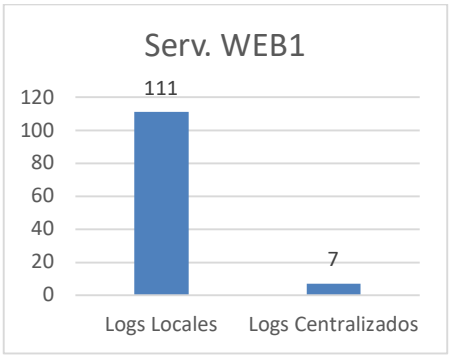


Figura 24. Eventos locales en activo WEB1 origen comparados con eventos centralizados en servidor OSSIM.

4.1.2.3 Activo Servidor Active Directory

Al recoger eventos localizados en el activo Active Directory, muestra una cantidad de 138 logs para ser tratados, luego, en el Sensor OSSIM son normalizados y finalmente en el módulo servidor OSSIM estos eventos que fueron agregados están listos para brindar información en el sistema de qué eventos son naturales o preocupantes, muestra a través de la interfaz gráfica 43 logs pertenecientes al activo AD, lo cual indica una cantidad menor, esto debido a que el sistema filtró los eventos en base a políticas, directivas y procedimientos con los mismos. Es importante destacar que la muestra tomada de este activo se la llevó en una porción de un minuto y fracción debido a que tiene un alto número de peticiones. La figura 25 muestra su resultado.

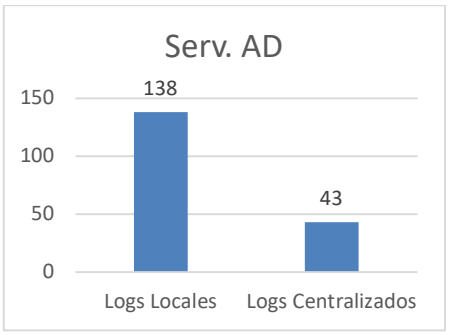


Figura 25. Eventos locales en activo AD origen comparados con eventos centralizados en servidor OSSIM

4.1.2.4 Activo Firewall

Al recoger eventos localizados en el activo Active Firewall1, muestra una cantidad de 97 logs para ser tratados, luego, en el Sensor OSSIM son normalizados y finalmente en el módulo servidor OSSIM estos eventos que fueron agregados están listos para brindar información en el sistema de qué eventos son naturales o

preocupantes, muestra a través de la interfaz gráfica 2 logs pertenecientes al activo Firewall1, lo cual indica una cantidad menor, esto debido a que el sistema filtró los eventos en base a políticas, directivas y procedimientos con los mismos. Es importante destacar que la muestra tomada de este activo se la llevó en una porción de un minuto y fracción debido a que tiene un alto número de peticiones. La figura 26 muestra su resultado.

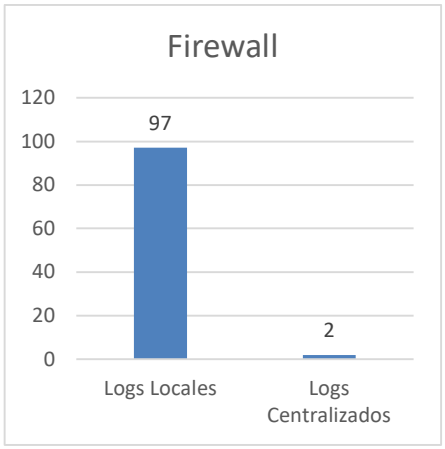


Figura 26. Eventos iniciales locales en activo FIREWALL1 origen comparados con eventos centralizados en servidor OSSIM

4.1.2.5 Activo Switch1

Al recoger eventos localizados en el activo Switch1, muestra una cantidad de 12 logs para ser tratados, luego, en el Sensor OSSIM son normalizados y finalmente en el módulo servidor OSSIM estos eventos que fueron agregados están listos para brindar información en el sistema de qué eventos son naturales o preocupantes, muestra a través de la interfaz gráfica 2 logs pertenecientes al activo Switch1, lo cual indica una cantidad menor, esto debido a que el sistema filtró los eventos en base a políticas, directivas y procedimientos con los mismos. La figura 27 muestra su resultado.

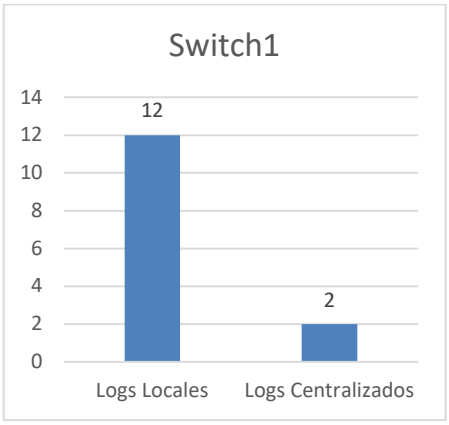


Figura 27. Eventos iniciales locales en activo SW1 origen comparados con eventos centralizados en servidor OSSIM

4.1.2.6 Activo Antivirus Central

Al recoger eventos localizados en el activo Antivirus Central, muestra una cantidad de 32 logs para ser tratados, luego, en el Sensor OSSIM son normalizados y finalmente en el módulo servidor OSSIM estos eventos que fueron agregados están listos para brindar información en el sistema de qué eventos son naturales o preocupantes, muestra a través de la interfaz gráfica 4 logs pertenecientes al activo Antivirus Central, lo cual indica una cantidad menor, esto debido a que el sistema filtró los eventos en base en base a políticas, directivas y procedimientos con los mismos. La figura 28 muestra su resultado.

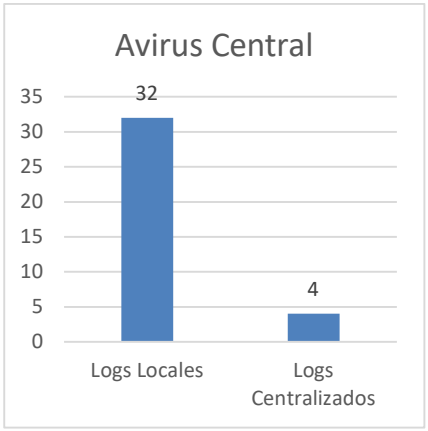


Figura 28. Eventos iniciales locales en activo AV origen comparados con eventos centralizados en servidor OSSIM

4.1.2.7 Activo Servidor genérico

Al recoger eventos localizados en el activo Servidor genérico, muestra una cantidad de 80 logs para ser tratados, luego, en el Sensor OSSIM son normalizados y finalmente en el módulo servidor OSSIM estos eventos que fueron agregados están listos para brindar información en el sistema de qué eventos son naturales o preocupantes, muestra a través de la interfaz gráfica 7 logs pertenecientes al activo Servidor Genérico, lo cual indica una cantidad menor, esto debido a que el sistema filtró los eventos en base a políticas, directivas y procedimientos con los mismos. La figura 29 muestra su resultado.

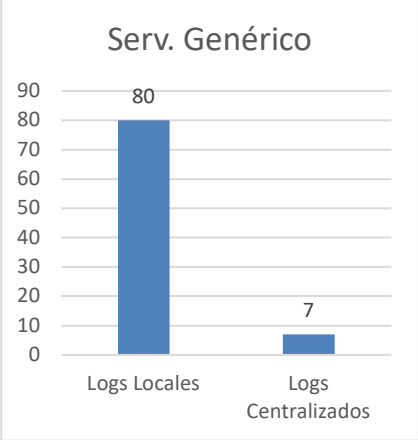


Figura 29. Eventos iniciales locales en activo SERVIDOR GENÉRICO origen comparados con eventos centralizados en servidor OSSIM

Se tuvo un análisis previo a la implementación para delimitar la población o muestra, el área física de estudio es el Data Center institucional, se seleccionó un número específico de activos para ser analizados en base a criterio de administrador de seguridad exceptuando los activos que por su criticidad y sensibilidad no pudieron aplicarse al estudio debido a ser equipos de producción y representar procesos muy

sensibles para la Institución. Entonces una vez definida la lista de equipos los cuales se tipifico su dimensión como consta en la tabla 4 se procedió a extraer los datos, es decir, los eventos de seguridad, para poder analizarlos de manera independiente.

4.2 Variables Respuesta o Resultados Alcanzados

Como se cuenta con los valores dados por la ficha de cotejo de manera local previo al experimento y de manera centralizada luego de la implementación se ha decidido trabajar con el estadístico t para muestras emparejadas, donde se comprobará la hipótesis si el resultado del p valor es menor a 0.05 que corresponde al 95% de confianza. En la tabla 9 se muestra el procedimiento del cálculo.

4.3 Discusión

El aplicar el uso de la herramienta AlienVault OSSIM con la participación en el presente proyecto de varios activos críticos que manejan un alto volumen de peticiones en la DMZ de una institución de educación superior de gran tamaño como lo es la Universidad Técnica de Ambato, permite poner a prueba su beneficio efectivo, aspectos no encontrados en anteriores estudios, lo cual facilita información útil para futuros trabajos relacionados.

4.4 Normalidad

La prueba de normalidad en la que se debe aceptar la hipótesis nula y se consideran todas las categorías que estaban ponderadas se muestran en la tabla 9.

TABLA 8. MUESTRA DE TODOS LOS EQUIPOS EN REFERENCIA A SUS LOGS LOCALES Y LOGS CENTRALIZADOS

Orden	Equipo	Logs Locales	Logs Centralizados
1	Equipo BD1	49	9

2	Equipo WEB1	111	7
3	Equipo AD	138	43
4	Equipo FW	97	2
5	Equipo SW1	12	2
6	Equipo AV	32	4
7	Equipo SG	80	7

Luego de realizar proceso estadístico se verifica que se cuenta con una muestra paramétrica, como consta en la tabla 9.

TABLA 9. PRUEBA T PARA MEDIAS DE DOS MUESTRAS EMPAREJADAS

	Logs Locales	**Logs Centralizados**
Media	74,1428	10,5714
Varianza	2043,809524	211,6190476
Observaciones	7	7
Coeficiente de correlación de Pearson	0,651666848	
Diferencia hipotética de las medias	0	
Grados de libertad	6	
Estadístico t	4,497933504	
P(T<=t) una cola	0,002056488	
Valor crítico de T (una cola)	1,943180281	
P(T<=t) dos colas	0,004112976	
Valor crítico de t (dos colas)	2,446911851	

Por otra parte, el valor de P, que es el nivel de significancia cuyo valor es 0.00205, es menor que el valor determinado para 0.05 por lo que permite rechazar la hipótesis nula H0 y aceptar la hipótesis de investigación.

CAPÍTULO V

CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS

5.1 Conclusiones

- El conocimiento de la topología de la red, las características y funciones de cada uno de los activos que conforman el segmento de red a estudiar, así como conocer los riesgos informáticos a los que están expuestos los activos, son aspectos muy importantes para definir la trazabilidad en el desarrollo de este proyecto.

- El estudio y análisis de varias herramientas SIEM, su diseño, características, beneficios y limitaciones, permite una apropiada selección que cubra los requerimientos demandados en el entorno, así también facilita a los administradores un documento de apoyo al momento de migrar o escalar de acuerdo con las necesidades de la institución.

- La implementación del correlacionador de eventos SIEM en la DMZ institucional permite identificar posibles amenazas en base a la configuración apoyada en políticas, acciones y directivas, la detección de patrones de comportamiento de diferentes activos brindando información más efectiva en la gestión de la seguridad de la red.

- La aplicación de esta herramienta en la muestra seleccionada permite un mejor control y visibilidad de los activos administrados, así como una supervisión y análisis integral de los mismos.

- La herramienta ha sido instalada, configurada y aplicada políticas y reglas que han permitido verificar su funcionamiento, y evidenciar la mejora en el procesamiento de eventos de seguridad. La herramienta está lista para su utilización en el segmento DMZ.

- Una de las principales limitaciones en la aplicación del presente proyecto fue el acceso que debido a la confidencialidad y criticidad contienen la mayoría de los activos que conforman la DMZ, no se obtuvo el acceso total a cada uno de ellos para un mayor alcance.

5.2 Recomendaciones

- Se recomienda mayor acceso a los equipos por parte de personal autorizado que facilite aplicar un mayor análisis de todos los sistemas que conforman la DMZ institucional lo cual permitirá mayor alcance en la mitigación de riesgos informáticos.

- Para un trabajo futuro se recomienda afinar las reglas y políticas a aplicarse en los diversos activos, así como cubrir la mayor cantidad de activos pondrá a prueba la capacidad del modelo implementado.

- Obtener una capacitación avanzada en la configuración y uso de esta herramienta SIEM para lograr mejores resultados.

- Simular un ambiente controlado en el cual se puedan realizar pruebas exhaustivas que permitan un mayor análisis y explotación de la presente herramienta.

5.3 Bibliografía

Alamanni, M. (2014). Características OSSIM. *Linux Journal*, 68-83.

Areitio, J. (2008). *Seguridad de la información.* Madrid: Universidad de Deusto.

Arias-Gómez, J., & Villasís, M. (2016). *El protocolo de investigación III.* México: Revista Alergia México.

Asensio, G. (2008). *Gestión de la seguridad con OSSIM.* Bilbao: IT Deusto.

AT&T Cybersecurity. (05 de 06 de 2022). *AT&T Cybersecurity*. Obtenido de AT&T Cybersecurity: https://cybersecurity.att.com/products/ossim

Avella, D., & Molano, H. (2015). *Identificación de vulnerabilidades y amenazas informáticas en laboratorios SIEFRIED.* Bogotá: Fundación Universitaria Panamericana.

Avella, J., & Calderón, L. (2015). *Guía Metodológica para la Gestión centralizada de registros en SIEM.* Bogotá: Universidad Católica de Colombia.

Azizov, D. (2020). *Arquitectura DMZ Perimetral.* Barcelona: Universidad de Barcelona.

Bravo, A., & Villafuerte, A. (2015). *Implantación de una herramienta OSSIM para monitoreo de la red.* Guayaquil: Escuela Politécnica del Litoral.

Chicano Tejada, E. (2015). *Gestión de incidentes de Seguridad Informática. IFCT0109 .* Málaga: Editorial IC.

CSIRT. (2021). *Implementación del mes.* Santiago de Chile: CSIRT Gobierno de Chile.

Cybersecurity AT&T. (27 de 04 de 2021). USM Appliance Deployment Guide. En Cybersecurity AT&T, *USM Appliance Deployment Guide* (págs. 20,193). Dallas, USA: Cybersecurity AT&T. Obtenido de https://cybersecurity.att.com: https://cybersecurity.att.com/documentation/

Cybersecurity AT&T. (2021). USM Appliance User Guide. En C. AT&T, *USM Appliance User Guide* (pág. 12). Dallas, USA: Cybersecurity AT&T.

Decreto Ejecutivo 1425. (2008). *Decreto Ejecutivo 1024.* Quito: Presidencia de la República del Ecuador.

Ferruzola, E., Bermeo, O., & Arévalo, L. (2022). Análisis de los sistemas centralizados de seguridad informática. *Ecuadorian Science Journal*, 23-31.

Hernández Sampieri, R. (2014). *Metodología de la Investigación.* México: McGraw Hill.

Incibe. (16 de 01 de 2020). *www.incibe.es.* Obtenido de www.incibe.es: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

ISO 27001:2013. (25 de 09 de 2013). *Guía de implantación para la seguridad de la información.* Obtenido de www.nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

ISO 31000:2018. (2018). *Administración/Gestión de riesgos - Lineamientos guía.* Ginebra, Suiza: Norma Internacional ISO.

ISOTools Excellence. (23 de 01 de 2020). *https://www.pmg-ssi.com/.* Obtenido de https://www.pmg-ssi.com/: https://www.pmg-ssi.com/2020/01/la-gestion-de-riesgos-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

Madrid, J., & Múnera, L. (2008). *Implementación y mejora de la consola de seguridad informática OSSIM.* Cali, Colombia: Universidad ICESI.

ManageEngine. (10 de 09 de 2022). *ManageEngine Log 360.* Obtenido de ManageEngine Log 360: https://manageengine.com.mx/log-management/componentes-siem

Medina, E. (2015). *Hacking Ético: Una herramienta para la seguridad informática.* Bogotá: Universidad Piloto de Colombia.

Microsoft. (15 de 11 de 2022). *Qué es un SIEM?* Obtenido de www.microsoft.com: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

Mieres, J. (2009). Debilidades de seguridad comúnmente explotadas. *Evil Fingers*, 1-17.

MINTEL. (2022). *Recomendaciones para prevenir la explotación de vulnerabilidades en los portales WEB.* Quito: Boletín Nº 4.

PCI Security Standard Council. (2013). *Normas de seguridad de datos v3.* Wakefield, MA USA: PCI Security Standard Council.

Rigau Pedraza, A. (2019). *Ventajas e implementación de un sistema SIEM.* Barcelona: Universidad Oberta de Catalunya.

Singh Chauhan, A. (2018). *Practical network scanning.* Birmingham UK: Pack Publishing.

Universidad Adventista de Chile. (2018). *Guía para validar instrumentos de investigación.* Chillán. Chile: Universidad Adventista de Chile.

5.4 Anexos

Anexo 1

Instalación de la herramienta SIEM AlienVault OSSIM

Una vez realizada la descarga del programa, procedemos a ejecutar.
Seleccionar la primera opción.

Figura 30. Pantalla inicial de instalación de AlienVault OSSIM

En las siguientes pantallas escogemos lenguaje de instalación, ubicación regional, país, configuración local, configuración del teclado.

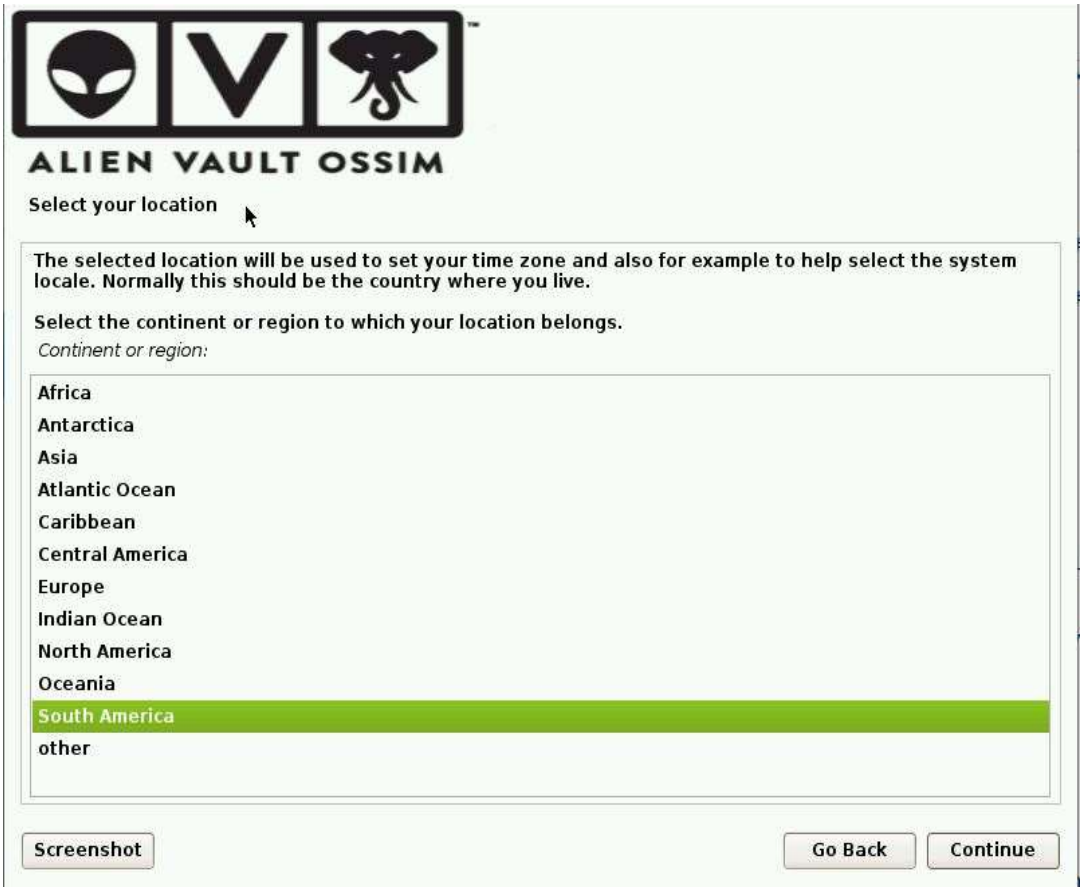


Figura 31. Selección de región donde estará ubicado el Servidor OSSIM

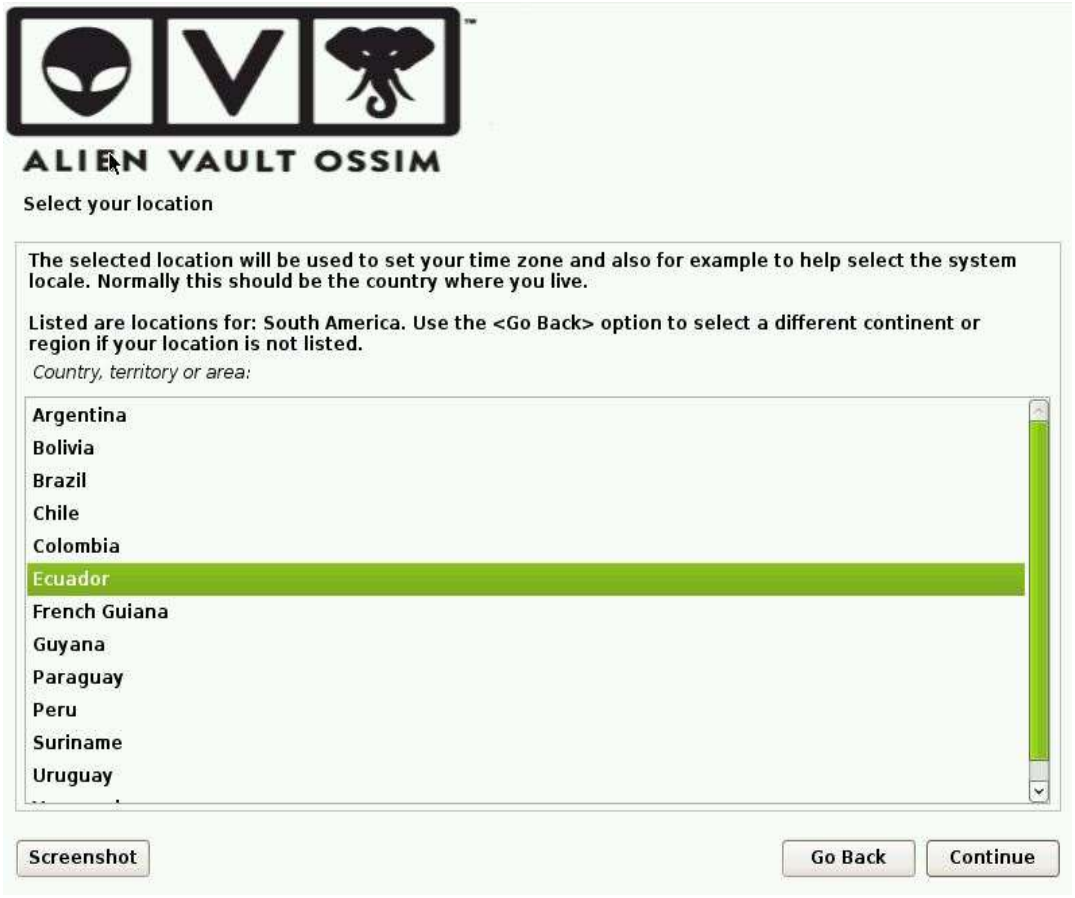


Figura 32. Selección de país para adecuada configuración de localidad

Figura 33. Selección de preferencias locales según configuración UTF

Figura 34. Instalación de componentes de OSSIM

Figura 35. Configuración de redes

Luego fijamos la máscara, el Gateway y el (los) DNS separados por comas.

Figura 36. Establecimiento de contraseña de sistema

Una vez terminada la fase de instalación se muestra la pantalla inicial en modo consola y la información para poder ingresar al interfaz web.

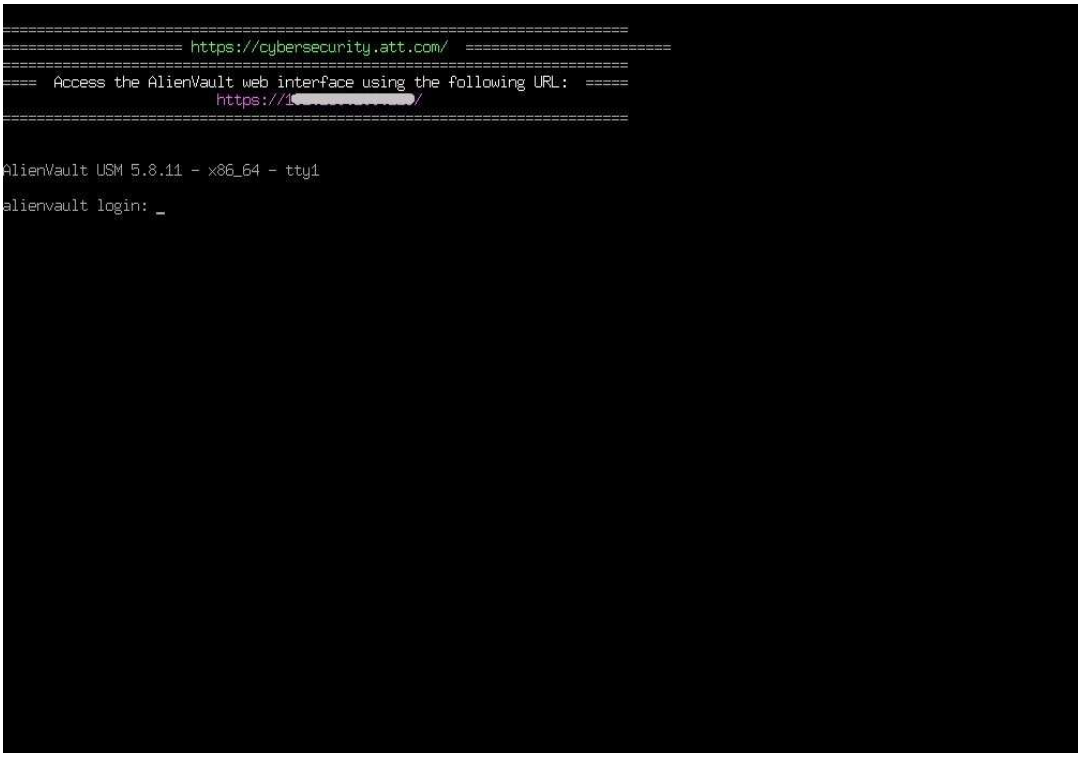


Figura 37. Ingreso en modo consola

La segunda parte de la configuración lo realizamos a través de la interfaz web. Aquí se crea la cuenta Administrador con los datos del usuario e institución.

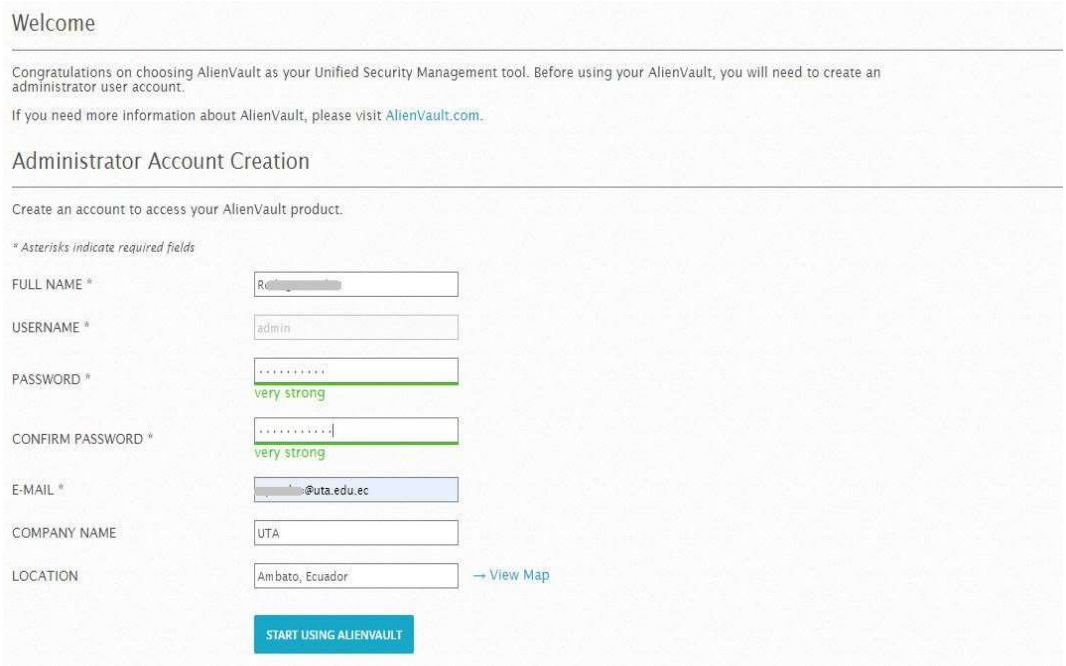


Figura 38. Creación de credenciales para el sistema a través de interfaz web

A continuación, se muestra el asistente para configuración inicial. En este apartado lo importante es definir como trabajarán las interfaces de red. Bajo en el esquema Todo en Uno AlienVault OSSIM configura la interfaz de administración para supervisión de la red, la recopilación de registros y análisis, y el análisis y escaneo. Pero si se desea separar estos procesos se puede trabajar con varias tarjetas de red.

Figura 39. Asistente para tareas iniciales de configuración del sistema

Anexo 2

Configuración de Plugins

Activos LINUX-Centos

En el equipo CentOS ingresamos al modo consola y nos trasladamos al siguiente directorio:

cd /etc/rsyslog.d

Creamos el archivo que permitirá indicar al equipo que se enviarán los logs al servidor OSSIM:

nano alienvault.conf

*. * @10.x.xx.xxx

A continuación, reiniciamos el servicio:

cd /etc/init. d/

systemctl restart rsyslog

En el equipo Alienvault:

Dejamos en espera para comprobación de recepción de paquetes:

tcpdump -i eth0 -v -w /dev/null src 10.x.xx.x

En Centos: ejecutar:

sudo su

En este instante se envían paquetes de centos a AlienVault

Luego en equipo AlienVault:

Configuramos el filtrado

cd /etc

nano rsyslog.conf

cambiar en línea

*.conf por nombre_pc.conf

luego

cd rsyslog.d

nano nombre_pc.conf

aquí configuramos el filtrado rsyslog con:

if ($fromhost-ip == '10.x.xx.x') then -/var/log/nombre_pc.log

& ~

Reiniciamos el servicio rsyslog

Luego comprobamos que desde la máquina Centos se insertan correctamente los logs:

cd /var/log

tail -f nombre_pc.log

En este instante se deben insertar correctamente.

Configuración de archivo .cfg

cd /etc/ossim/agent/plugins

copiamos un modelo de archivo .cfg similar al activo que estamos tratando

cp ssh.cfg nombre_pcssh.cfg

Editamos este archivo nuevo:

en sección DEFAULT

reemplazamos

auth.log por nombre_pc.log

Además, reemplazamos el puerto:

'4003' por '9001'

A continuación, ejecutamos:

alienvault-setup

y procedemos a seleccionar y marca (ACTIVAR) el nuevo plugin que hemos creado nombre_pcssh en el menú de interfaz consola de AlienVault

Finalmente ejecutamos

alienvault-reconfig

En equipos Centos:

reiniciamos el servicio SSH

systemctl restart sshd.service

Configuración de archivo .sql

En AlienVault:

cd /usr/share/doc/ossim-mysql/contrib/plugins

copiamos el archivo ssh.sql a nombre_pcssh.sql

reemplazamos el valor de puerto 4003 por 9001 hasta la línea 10 y el borramos el resto de código del archivo.

luego ejecutamos:

ossim-db < centos05ssh.sql

a continuación, ejecutamos:

ossim-db

Con esta última instrucción ingresamos a la interfaz de sql en la cual ejecutamos:

> select * from plugin where id = 9001;

y se debe haber insertado una línea en la base de datos.

salimos con el comando "quit"

Ahora hacemos un reconfig de AlienVault:

alienvault-reconfig

Para finalizar verificamos en interfaz web que consta este nuevo plugin en DEPLOYMENT/ALIENVAULT CENTER/SENSOR CONFIGURATION/COLLECTION

Luego reiniciamos el servicio rsyslog en AlienVault

service rsyslog restart

Y, comprobamos el funcionamiento de este plugin haciendo pruebas con procedimientos SSH.

Activos Windows

Para este caso utilizaremos el modo Habilitar complementos en el activo

Pasos:

1. Ir a ENVIROMENT/ASSETS & GROUPS/ASSETS
2. Seleccionar el activo que en el cual se requiere habilitar el complemento.
3. Hacemos clic en la lupa para ampliar las opciones.
4. Hacemos clic en el botón Complementos.
5. Hacemos clic en Editar Complementos.
6. Seleccionamos un proveedor, un modelo y versión (en caso de existir).
7. Hacer clic en agregar Complemento.
8. Se puede agregar hasta 10 complementos por activo.

Activos como Dispositivos de almacenamiento, switches y otros

Para este tipo de dispositivos lo hacemos a través de la interfaz web, es decir, lo hacemos de la misma manera que se realizó para el activo Windows en los pasos anteriores.

Anexo 3

TABLA 10. FORMULARIO PARA ENTREVISTA

ENTREVISTA A DIRECTOR DE TECNOLOGÍAS DITIC-UTA	
Nombre del entrevistador	
Ciudad	
Fecha	
Estimado entrevistado: El objeto de la siguiente entrevista es conocer a acerca de procedimientos y uso de mecanismos para mitigar ataques y vulnerabilidades en la DMZ Institucional	
Nombre del entrevistado	
Cargo	
1.- ¿Además de contar la DMZ con un firewall, cuenta con otras herramientas que ayuden a mitigar los ataques informáticos?	
2.- ¿En Servidores de Bases de Datos existe un procedimiento automatizado para identificar actividades sospechosas en función de un conjunto de reglas de eventos configurables que permita la toma de decisiones oportunas?	
3.- Existe procedimientos para ajustar el comportamiento del sistema y alertar sobre posibles problemas de seguridad y vulnerabilidad en el Active Directory?	
4.- En el firewall existen alertas sobre configuraciones erróneas o actualizaciones perdidas en este que comprometan su funcionamiento adecuado?	
5.- Los Switches están configurados para enviar logs hacia un equipo centralizado para facilitar la gestión de su seguridad?	
6.- Se detectan ataques de fuerza bruta sobre el Antivirus Central?	
7.- Existe una alerta automatizada para advertir de escaneo de puertos en servidores?	

Nota: Elaboración propia

Anexo 4

TABLA 11. FORMULARIO PARA VALIDEZ DE EXPERTOS

PREGUNTA		**PUNTUACIÓN EXPERTOS**					**VALIDACIÓN pregunta (SI/NO)**
N.º	**Evaluación**	**1**	**2**	**3**	**SUMA Puntuaciones**	**PROMEDIO puntuaciones**	
1	Adecuación						
	Pertinencia						
2	Adecuación						
	Pertinencia						
n	Adecuación						
	Pertinencia						

Nota. (Universidad Adventista de Chile, 2018)

CAPÍTULO VI

PROPUESTA

6.1 Datos Informativos

Título

"Integración de un correlacionador de eventos de seguridad en la red institucional."

Institución

La Universidad Técnica de Ambato fue creada el 18 de abril de 1969 mediante Ley No. 69-05. Como Universidad pública está regida por la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt) que ejerce la rectoría de la política pública en los ejes de su competencia. Desde sus inicios ha mostrado un crecimiento permanente y hoy es una de las universidades más importantes del país. Actualmente tiene como ejes principales: La Academia. La Investigación, Desarrollo e Innovación, La Vinculación con la Sociedad, La Gestión y la Internacionalización.

- Su Misión es:
    - Formar profesionales líderes competentes, con visión humanista y pensamiento crítico a través de la Docencia, la Investigación y la Vinculación, que apliquen, promuevan y difundan el conocimiento respondiendo a las necesidades del país.

- Su Visión es:

    - La Universidad Técnica de Ambato por niveles de excelencia se constituirá como un centro de formación superior con liderazgo y proyección nacional e internacional.

- Sus Valores son:

    - Compromiso con el desarrollo integral de los seres humanos en un entorno de
    - calidad y calidez y respeto a la naturaleza.
    - Responsabilidad.
    - Honestidad.
    - Equidad.
    - Solidaridad.
    - Respeto.
    - Lealtad.

- Sus Objetivos son:

    - Formar talento humano de grado y posgrado a través de diferentes modalidades, con liderazgo, responsabilidad social y ambiental, con sólidos conocimientos científicos, tecnológicos y culturales, que interpreten y comprendan la realidad socioeconómica del Ecuador, de Latinoamérica y del mundo y que emprendan de manera autónoma en iniciativas que propicien el desarrollo socioeconómico de la provincia, la región y el país.

    - Realizar investigación científica que permita generar innovación tecnológica, crecimiento productivo y desarrollo social, que contribuya a la superación de los problemas del Ecuador y del mundo, bajo los principios de eficiencia, calidad, pertinencia, integridad, autodeterminación para la producción del pensamiento y conocimiento.

    - Promover la innovación, la administración de la propiedad intelectual, y el asesoramiento efectivo a iniciativas de emprendimiento, respondiendo a las necesidades de la sociedad y construyendo redes de trabajo entre la academia, sectores sociales, administración pública y sectores de la producción.

- Vincular la labor universitaria con el desarrollo del entorno social, productivo y cultural, en base a los requerimientos de la sociedad y a través de la transferencia de ciencia y tecnología, la difusión de la cultura y la producción de bienes y/o servicios.

- Desarrollar la gestión universitaria sobre la base de un modelo de gestión que articule los requerimientos del contexto y el Plan Nacional de Desarrollo, que permita un crecimiento integral y sostenido de la Universidad Técnica de Ambato.

- Impulsar la internacionalización de la Universidad en la perspectiva de construcción de ciudadanía planetaria.

6.2 Antecedentes de la propuesta

Las instituciones en la actualidad están expuestas a un número creciente de amenazas, ya sea a nivel de red, a nivel de host, en otros casos amenazas externas, así como amenazas internas, por lo cual se convierte en un desafío detectar y prevenirlas, en este caso para poder mitigar estos riesgos existen herramientas y procedimientos para poder identificar vulnerabilidades y detectar amenazas.

La Universidad Técnica de Ambato, es una institución de Educación Superior con un acelerado crecimiento dada la demanda de carreras que existe en la región y el país, y en virtud de todos los servicios que ofrece como institución pública, su infraestructura tecnológica tiene la obligación de estar protegida con normas y políticas que son regidas por los órganos superiores de control.

6.3 Justificación

En las instituciones públicas a pesar de que con el pasar de los años se han ido implementando medidas de seguridad para hacer frente a las vulnerabilidades y ataques informáticos es necesario complementar estas medidas con el uso de mejores procedimientos y/o herramientas que ayuden a mitigar las amenazas. Los gobiernos particularmente de América Latina están conscientes de que los presupuestos que se asignan en las diversas áreas no son suficientes, por lo que se recomienda aportar soluciones con la implementación de herramientas Open Source, las mismas que facilitan un nivel de ciberseguridad inicial, pero ayudan a los administradores manejar conceptos y herramientas primarias, de tal manera que al realizar una transición a sistemas comerciales de mejor eficiencia y funcionalidad, puedan sacar el máximo provecho. CSIRT (2021).

6.4 Objetivos

6.4.1 General

Implementar un sistema de recolección y análisis de logs que permita detectar ataques informáticos basado en la correlación de eventos en la infraestructura de red DMZ administrada por la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato.

6.4.2 Específicos

Determinar los activos de la red DMZ en los cuales se aplicará las configuraciones para la gestión de vulnerabilidades y ataques informáticos a través de la herramienta SIEM AlienVault OSSIM.

Determinar las reglas y políticas a ser aplicadas en los activos seleccionados para realizar pruebas de ataques con la finalidad de comprobar la utilidad de la herramienta.

Elaborar una guía de los componentes principales que constan en el Dashboard de la herramienta AlienVault OSSIM.

6.5 Análisis de factibilidad

6.5.1 Factibilidad Operacional

Este proyecto es factible operacionalmente debido a que cuenta con el apoyo del director de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato, así como del personal encargado de seguridad y redes.

6.5.2 Factibilidad Técnica

La implementación del presente proyecto es posible ya que la Dirección cuenta con un equipo asignado que cumple con las características adecuadas para su configuración y puesta en marcha.

6.5.3 Factibilidad Económica

La implementación del proyecto no representa gastos económicos porque como se mencionó el equipo a utilizar se encuentra disponible en el data center institucional.

6.6 Fundamentación

De acuerdo con expertos en seguridad, ninguna organización puede considerarse inmune a ataques, y en base a este criterio no se trata de si sus sistemas se verán comprometidos sino cuándo y cómo sucederá, Alamanni (2014).

Es por esto muy importante que las instituciones cuenten con las herramientas necesarias que permita detectar ataques oportunamente y logren aplicar contramedidas que minimicen los efectos que puedan causar.

El SIEM proporciona a las organizaciones visibilidad sobre la actividad de su red para que puedan responder rápidamente a posible s ataques cibernéticos y cumplir con requisitos de cumplimiento. Microsoft (2022).

6.7 Metodología

Requerimiento institucional

El sistema que permita la integración de correlación de eventos de seguridad debe cumplir con los siguientes requerimientos:

- Debe ser On premise
- El servidor debe estar ubicado en el data center institucional
- Centralizar y agregar todos los eventos de seguridad relevantes y que sea disponibles
- Ofrecer soporte para variedad de fuentes
- Correlacionar y alertar
- Detectar amenazas avanzadas y desconocidas
- Permitir la investigación de incidentes.

6.7.1 Implementación de la herramienta SIEM seleccionada para la detección de ataques informáticos

Fase 1

Instalación de AlienVault OSSIM

Requerimientos de hardware:

Servidor. Para la implementación de esta aplicación la Universidad cuenta con un servidor adecuado, el cual posee las siguientes características:

- Procesador 8 núcleos

- 16 GB RAM
- 500 GB Almacenamiento
- 2 tarjetas de red Ethernet 1 GBPS

El programa se descarga desde el sitio oficial
https://cybersecurity.att.com/products/ossim/download

El detalle de la instalación se muestra en el Anexo 3.

Descubrimiento de Activos en la Red

- Trabajar con la red inicial descubierta en el momento de instalación o agregar nuevas redes con las que trabajará el sistema. Determinar el valor al activo
- Ingresar manualmente los activos seleccionados los cuales se gestionará en el sistema. Determinar en cada activo su valor. El valor de un activo o una red determina su criticidad, y permitirá al sistema brindar una adecuada alerta o información útil sobre sucesos al administrador.

Añadir agentes HIDS

El HIDS integrado en la herramienta OSSIM supervisa el comportamiento, así como el estado informático de un activo. Se encarga además de la supervisión de paquetes de red que un sistema envía y recibe.

Se procede a configurar cada uno de los activos, con sus diferentes sistemas operativos como Linux, Windows, Switch, Firewall.

Habilitación Complementos (Plugins)

El uso de complementos ayuda a extraer los logs de los activos administrados, por lo que OSSIM permite varias maneras de configurar los complementos:

- A través del activo agregando uno o varios complementos dependiendo de los servicios que presta el mismo.
- Se puede agregar el complemento de manera general desde el Sensor de OSSIM para varios equipos.
- Se puede configurar individualmente el complemento para un activo específico a través de comandos en la consola.

En el anexo IV se explica la configuración en dispositivos LINUX, Windows, y equipos activos de red como Switch.

La comprobación de la llegada de logs a sensor desde equipos configurados se muestra en el capítulo IV en las figuras 7 a 10.

Fase 2

Definición de Políticas y Acciones en Activos Monitoreados

Para crear políticas que serán aplicadas en la gestión de activos las realizamos a través de la interfaz web de la herramienta OSSIM en la sección Configuration/Threat Intelligence/Policy

Activo: Servidor Sitio Web1
Política: Detectar ataque XSS o DoS en este activo
Acción: Crear un tique en el cual se informe a través de qué IP, puerto origen y destino se realizó.

Activo: Servidor de Base de Datos1
Política: Detectar ataque de Inyección de SQL en este activo
Acción: Crear un tique para informar del evento.

Activos: Servidores de Active Directory
Política: Detectar ataque de Fuerza Bruta en estos activos

Acción: Crear un tique para informar del evento.

Activo: Switch1
Política: Detectar ataque de Fuerza Bruta en este activo
Acción: Crear un tique para informar del evento.

Fase 3

Resultados de la comprobación de políticas a través de ataques y vulnerabilidades en activos seleccionados.

Activo: Servidor Sitio Web1

Política: Detectar ataque XSS o DoS en este activo
Acción: Crear un tique en el cual se informe a través de qué IP, puerto origen y destino se realizó.
Resultado: El resultado se refleja en la figura 19.

Activo: Servidor de Base de Datos1
Política: Detectar ataque de Inyección de SQL en este activo
Acción: Crear un tique para informar del evento.
Resultado: El resultado se refleja en la figura 20.

Activos: Servidores de Active Directory
Política: Detectar ataque de Fuerza Bruta en estos activos
Acción: Crear un tique para informar del evento.
Resultado: El resultado se refleja en la figura 21.

Activo: Switch1
Política: Detectar ataque de Fuerza Bruta en este activo
Acción: Crear un tique para informar del evento.
Resultado: El resultado se refleja en la figura 22.

6.8 Administración

6.8.1 Supervisión de seguridad y análisis de dispositivos a través de OSSIM

6.8.1.1 Tableros de dispositivos de AlienVault OSSIM

Es un componente importante para el monitoreo y análisis de la seguridad de nuestro entorno. Brinda visibilidad general de la actividad en la red, así como facilita ver métricas de la seguridad de la red.

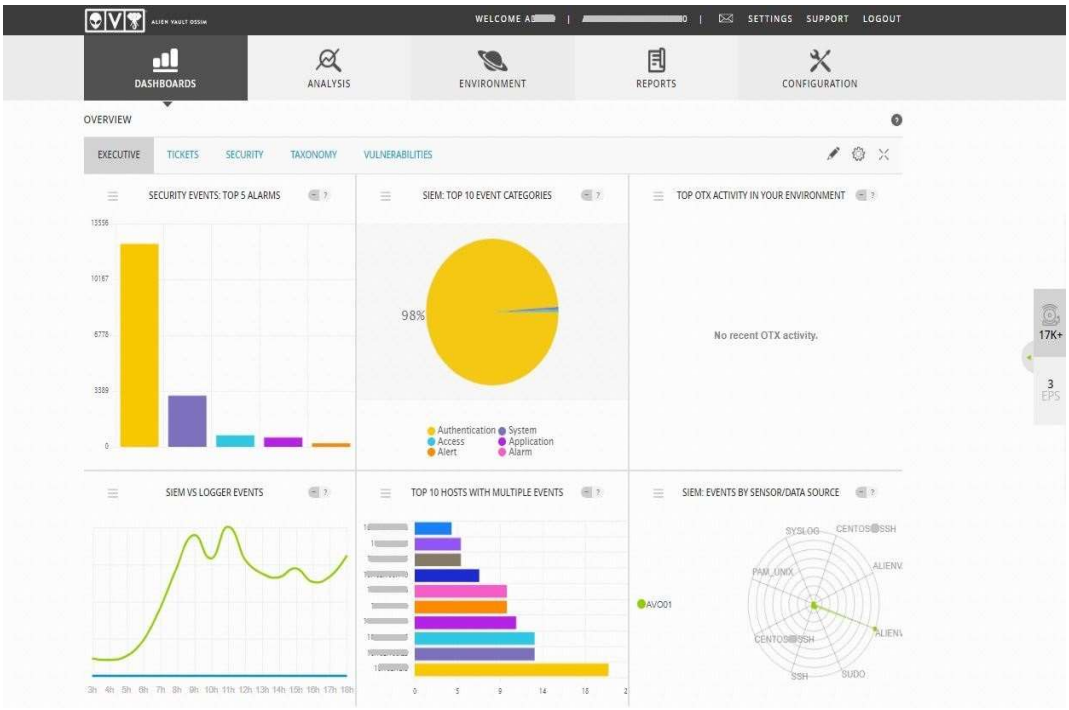


Figura 40. Tableros Descripción General

Los demás botones se resumen a continuación:

Tiques: Facilita métricas sobre los tiques creados dentro del sistema de emisión de tiques OSSIM

Seguridad: Proporciona métricas sobre diversas medidas de seguridad en el entorno como puede ser hosts activos, alarmas frecuentes, tendencias de informes de eventos de seguridad.

Taxonomía: Nos da métricas acerca de eventos basados en diferentes clasificaciones de eventos.

Vulnerabilidades: Proporciona métricas acerca de las características de las vulnerabilidades como puede ser gravedad, hosts más afectados.

6.8.1.2 Analizar alarmas, eventos, registros y tiques

Este menú nos permite las siguientes opciones:

Alarmas: Visualiza todas las alarmas generadas en OSSIM. Otra manera de visualizar las alarmas es haciéndolo mediante filtros.

Eventos de Seguridad (SIEM): Muestra los eventos que han sido generados a través del servidor OSSIM. Se puede adicionalmente buscar y filtrar eventos que aparecen en la pantalla, así como su detalle.

Registros sin procesar: Da acceso y muestra todos los eventos que el sistema guardó en archivos de registro, para almacenamiento a largo plazo e investigación forense. Esta opción está disponible en la versión de paga USM.

Tiques: Brinda acceso al sistema de gestión de tiques de OSSIM. Los tiques permiten un seguimiento del flujo de trabajo de actividades que tiene que ver con las alarmas detectadas u otro tipo de inconvenientes del cual se desea hacer un seguimiento.

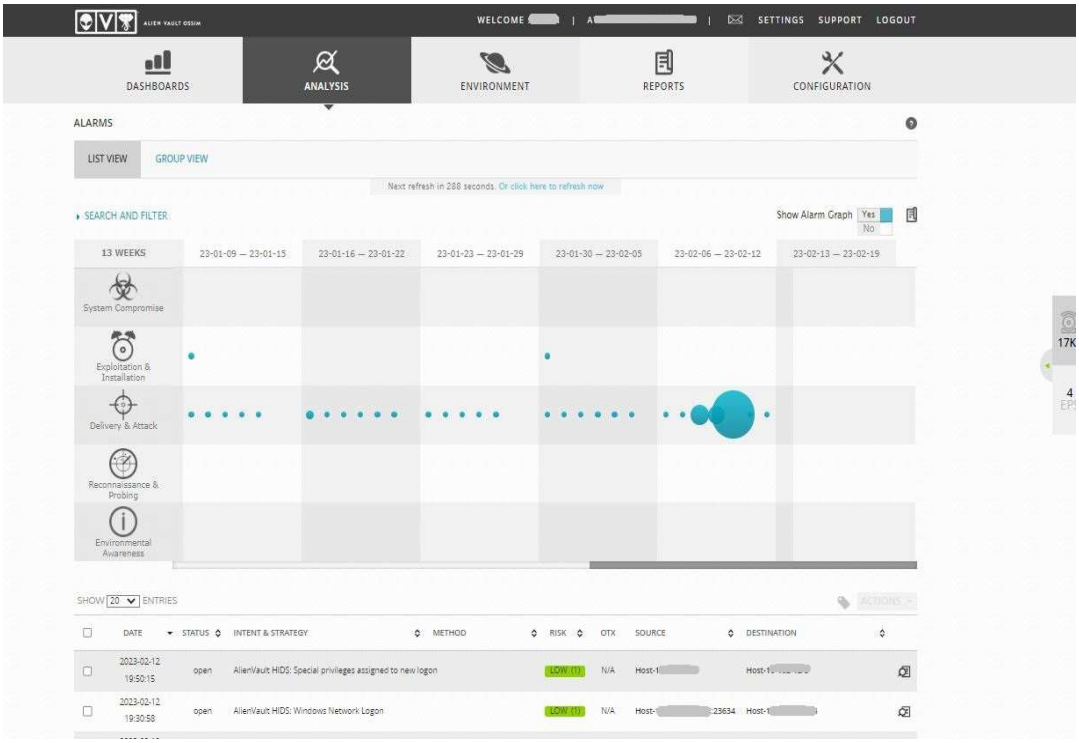


Figura 41. Tablero de Alarmas

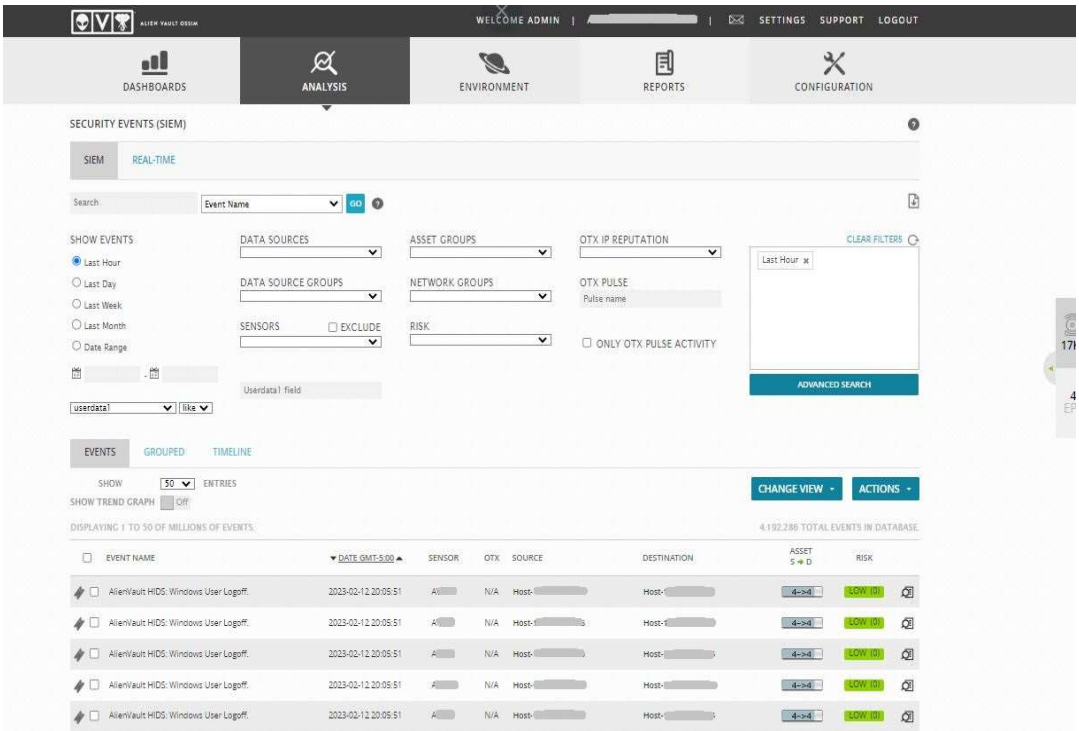


Figura 42. Tablero de Eventos de Seguridad SIEM

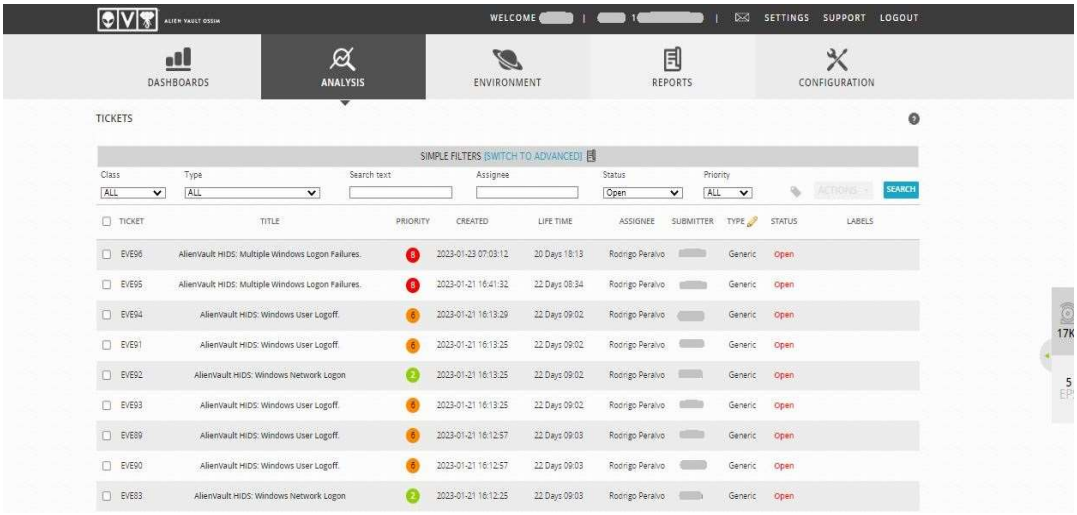


Figura 43. Tablero de Tiques

6.8.1.3 Gestión del Entorno de dispositivos OSSIM

El sistema OSSIM brinda adicionalmente al monitoreo y análisis de eventos y alarmas, aspectos de seguridad de la red como las siguientes:

Activos y grupos: Permite la administración de activos, redes y grupos.

Vulnerabilidades: Permite ver y escanear vulnerabilidades.

Netflow: Permite la capacidad de monitorear y trabajar con datos de Netflow

Captura de tráfico: Permite al usuario administrar la captura remota de tráfico a través del Sensor de OSSIM. Encontrará opciones de captura como tiempo de espera, tamaño de paquete, nombre de sensor, origen y destino del paquete.

Disponibilidad: Permite ver y configurar el monitoreo de disponibilidad.

Detección: Administra la detección de intrusos (IDS), permite además el análisis de registros, verificación de integridad, detección de rootkits, alertas basadas en tiempo.

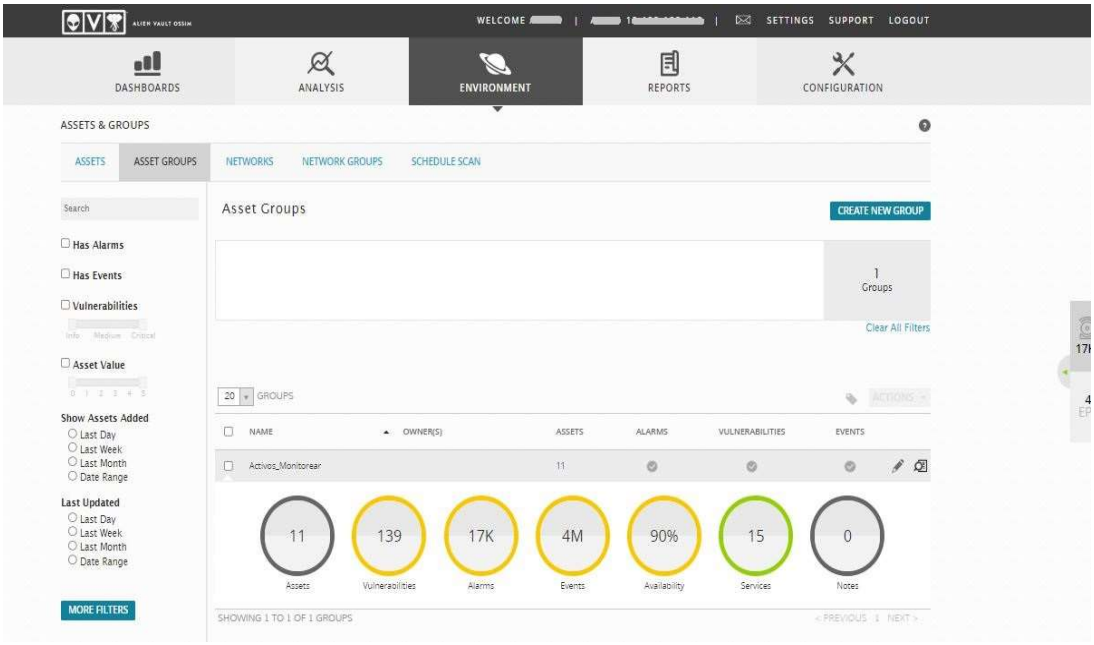


Figura 44. Tablero de Activos y Grupos

Esta sección permite agregar nuevas redes o activos, sus valores de criticidad, gestionar los eventos, agregar complementos, realizar análisis de vulnerabilidades.

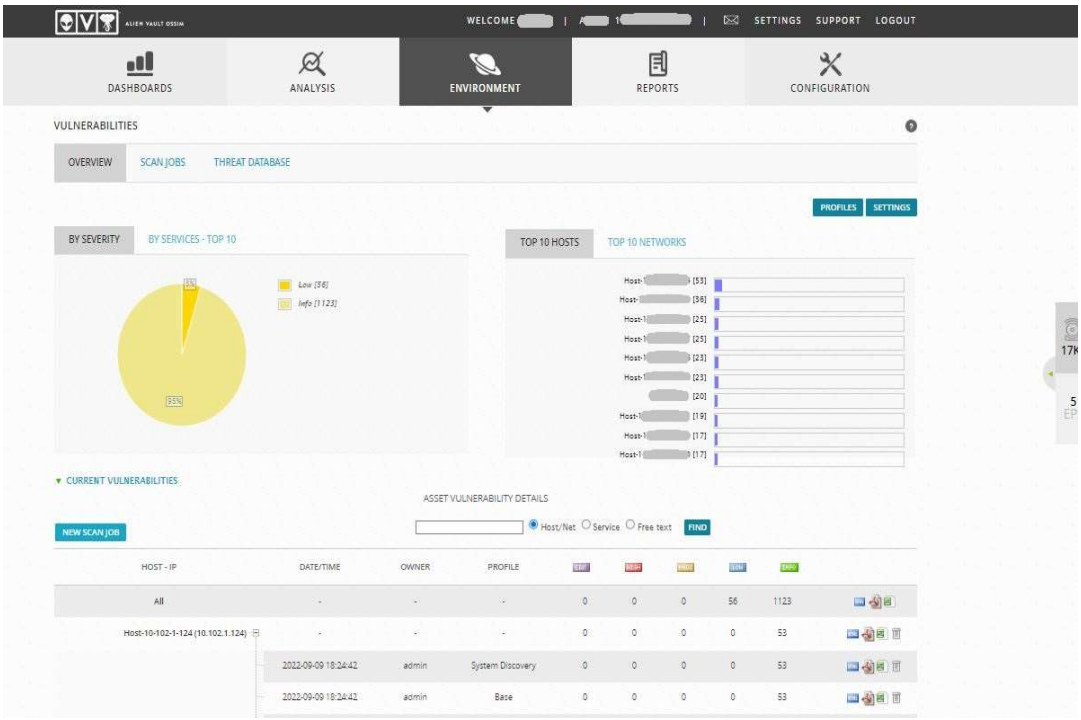


Figura 45. Tablero de Vulnerabilidades

Gestiona la evaluación de vulnerabilidades efectuadas en un activo, así como la programación de los activos. La evaluación de vulnerabilidades permite definir, identificar, clasificar y priorizar las vulnerabilidades en el sistema.

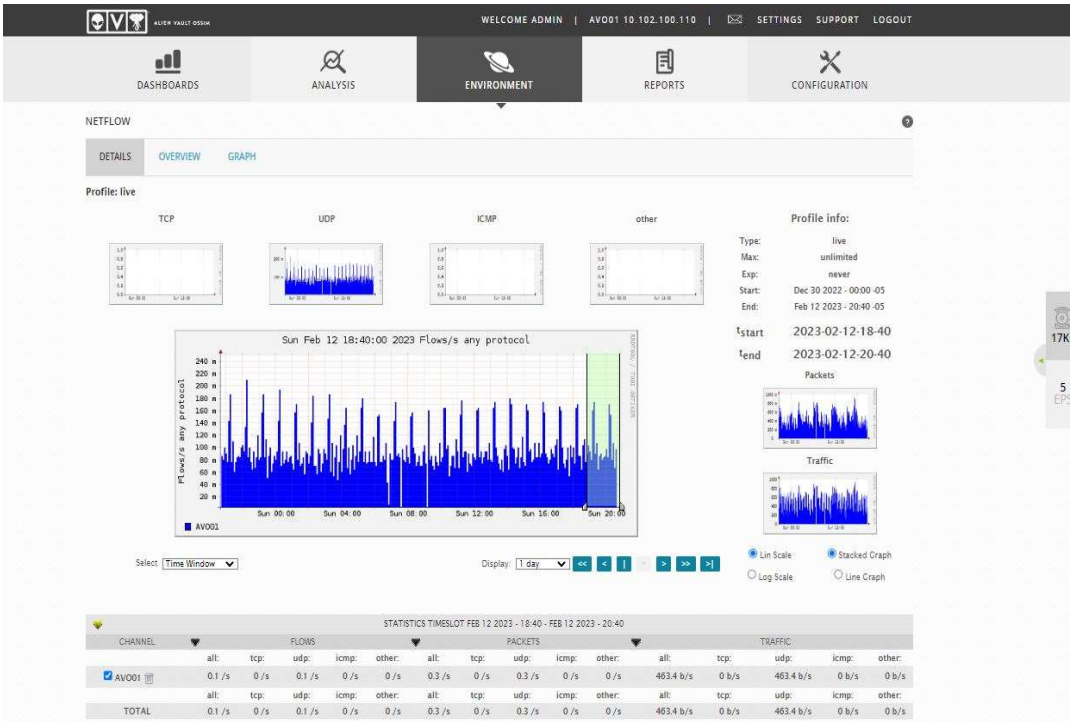


Figura 46. Tablero de Netflow

El monitoreo de Netflow permite capturar información de los flujos de red. Puede ayudar a identificar servicios inseguros y protocolos que no deben usarse.

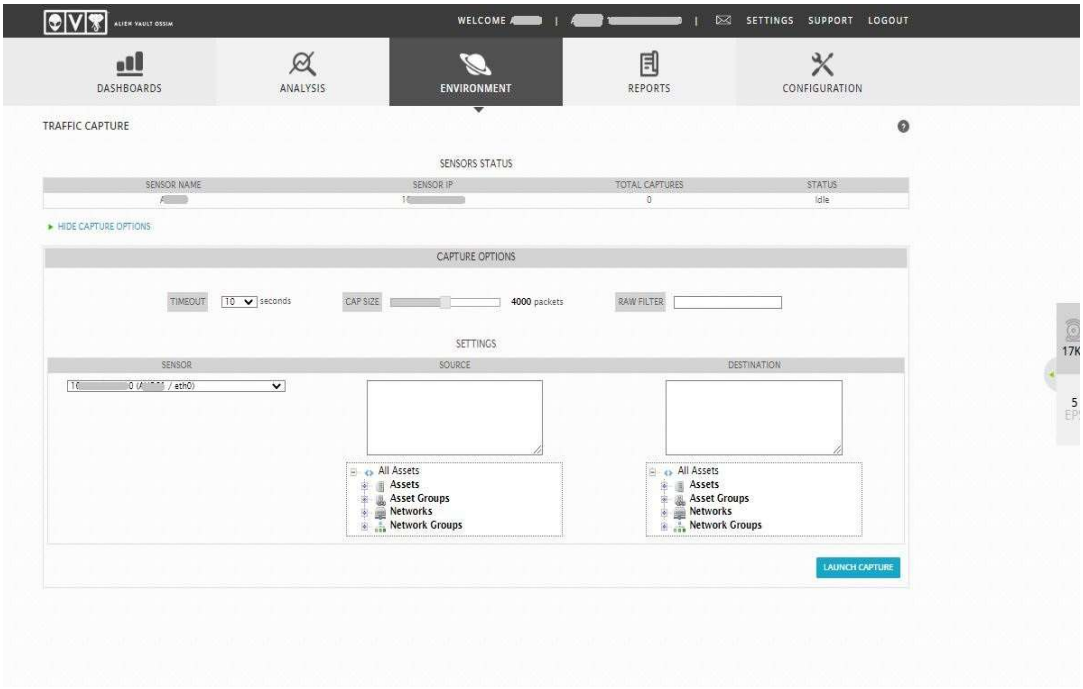


Figura 47. Tablero de Captura de Tráfico

La captura de paquetes permite al usuario capturar el tráfico de la red para su análisis, permitiendo además la captura llevarlo de ser necesario a otra herramienta externa para mayor estudio.

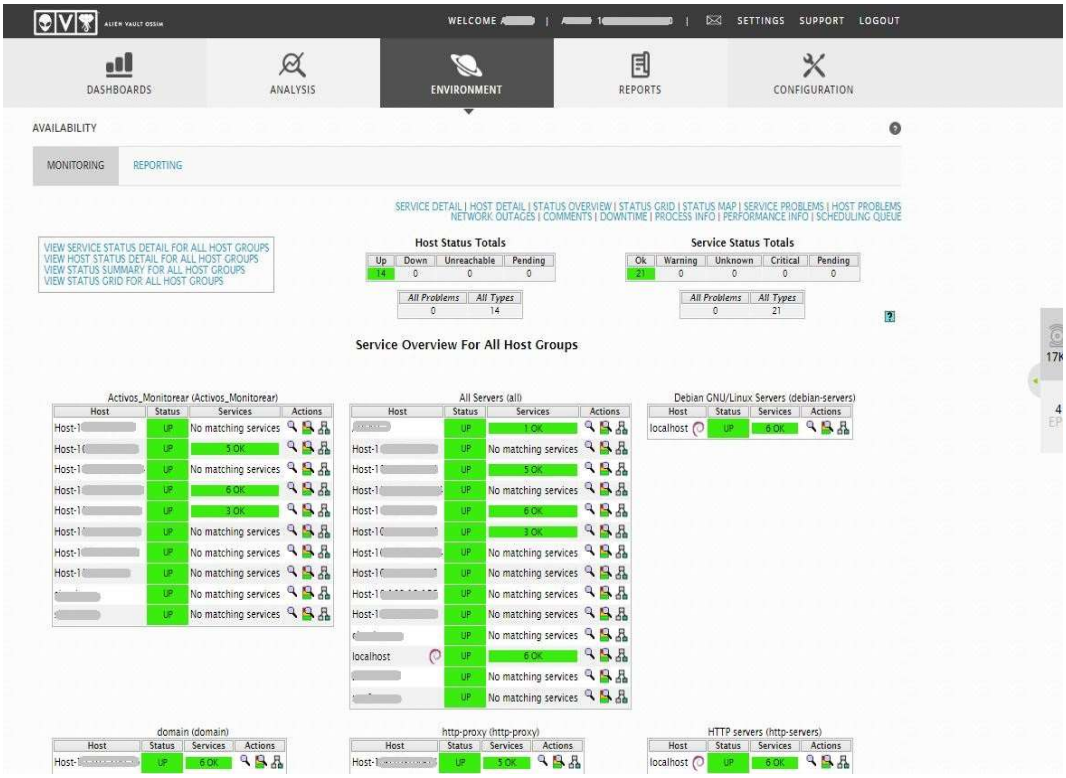


Figura 48. Tablero de Disponibilidad

Permite la visualización de cómo se encuentran los activos y sus servicios en lo referente a la disponibilidad y contiene opciones de configuración.

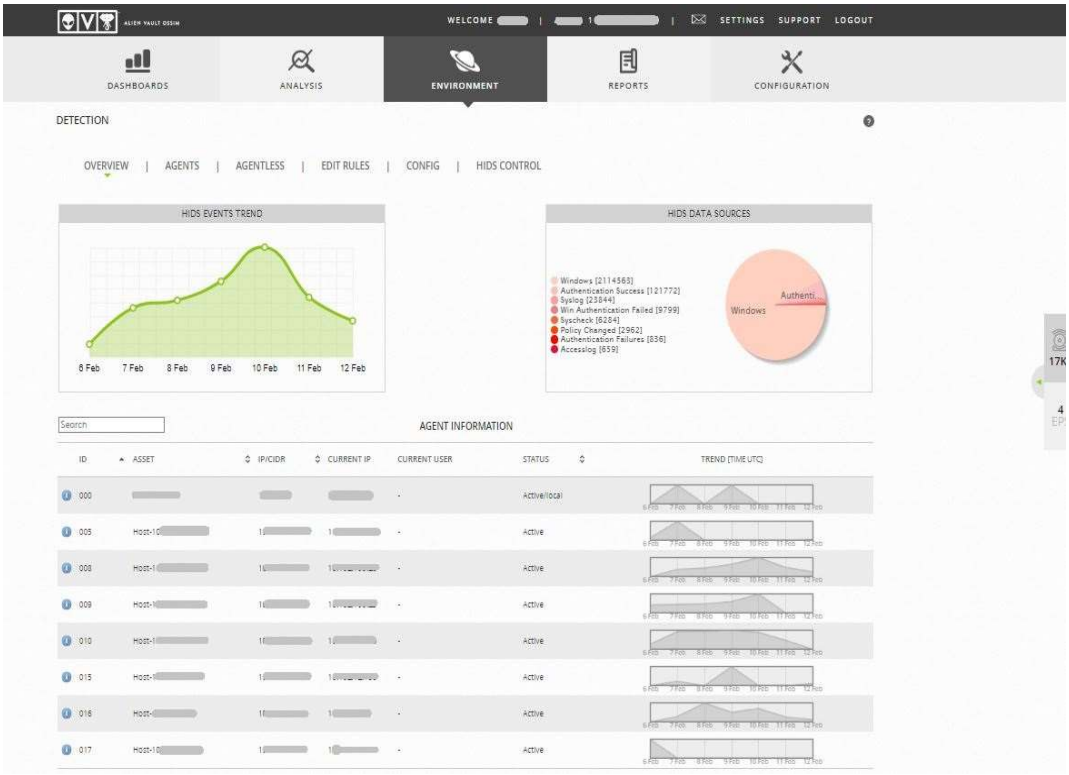


Figura 49. Tablero de Detección

Este componente es utilizado para la administración de detección de intrusos. Posee además el análisis de registros, verificación de integridad, detección de rootkits, alertas que se basan en el tiempo.

6.8.1.4 Informes

Incluye una diversidad de informes predefinidos que permiten a los usuarios mantenerlos informados acerca de activos, nivel de cumplimiento, alarmas y eventos de seguridad. Estas opciones de informes se encuentran agrupadas por categorías que facilitan al administrador y usuarios su aplicación.

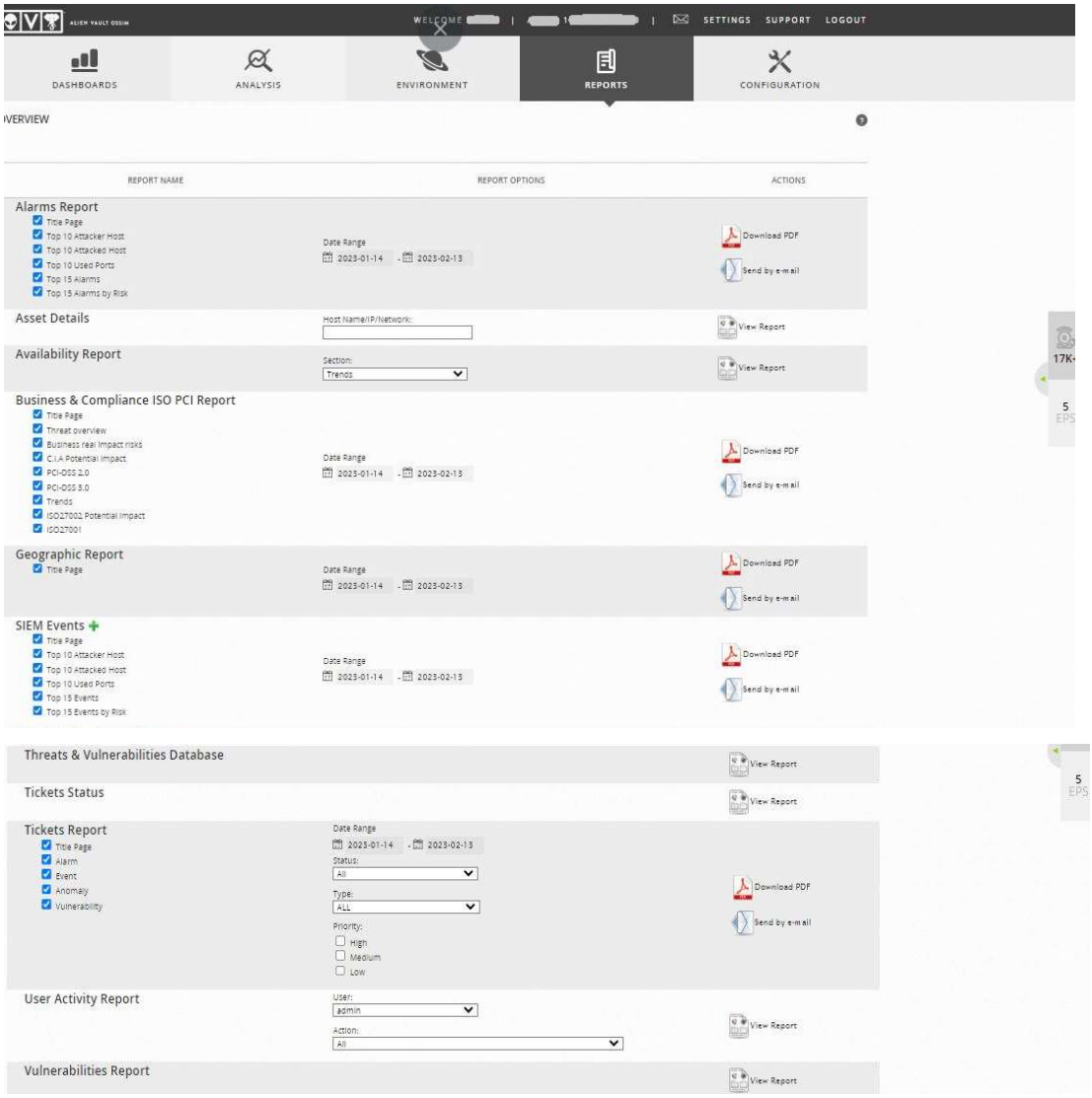


Figura 50. Tablero de Informes

6.8.1.4 Administración y Configuración de AlienVault OSSIM

Este componente es muy importante ya que permite ir realizando ajustes en el sistema de acuerdo con las necesidades. Tenemos las siguientes opciones:

Administración: Administra usuarios, configuración del sistema, así como opciones de respaldo y restaurar configuración.

Implementación: Proporciona opciones que permiten configurar y administrar componentes del sistema OSSIM.

Inteligencia sobre Amenazas: Brinda opciones para configurar políticas, acciones, puertos, directivas, reglas de correlación, fuentes de datos y clasificación de seguridad (taxonomía).

Open Threat Exchange (OTX): Facilita opciones para configurar ajustes de OTX y ver pulsos de OTX individuales e indicadores de compromiso (IoC).

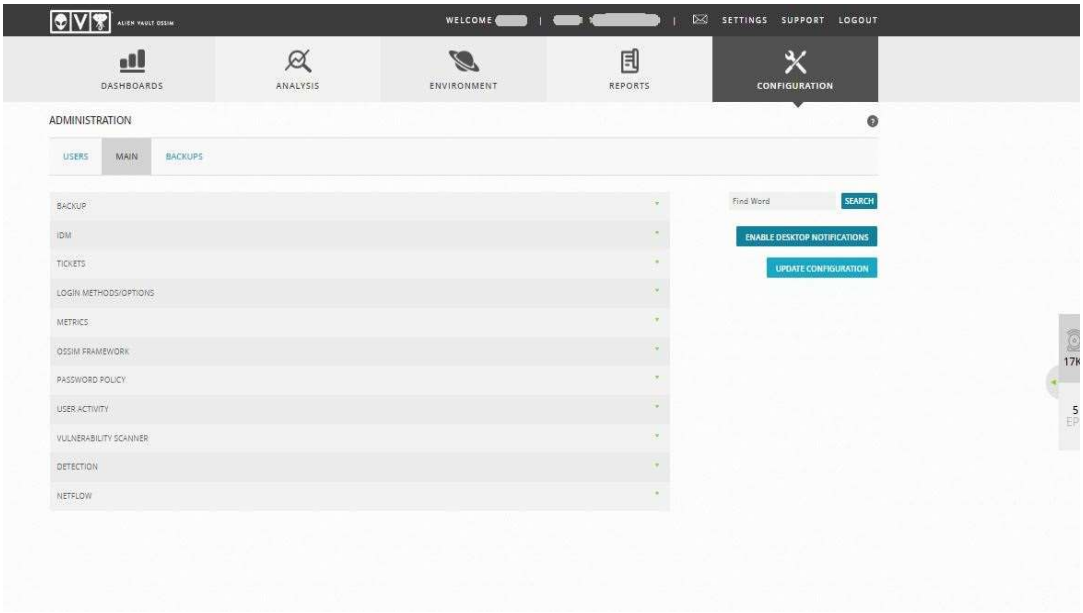


Figura 51. Tablero de Administración del Sistema

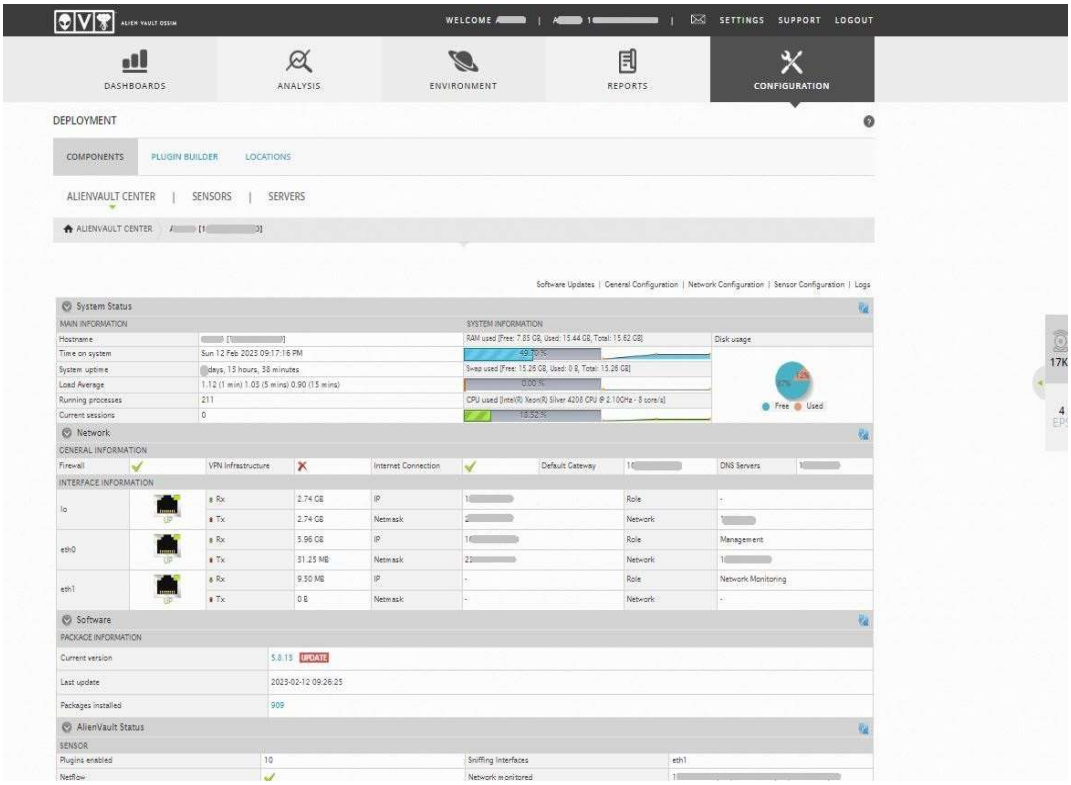


Figura 52. Tablero de Implementación del sistema

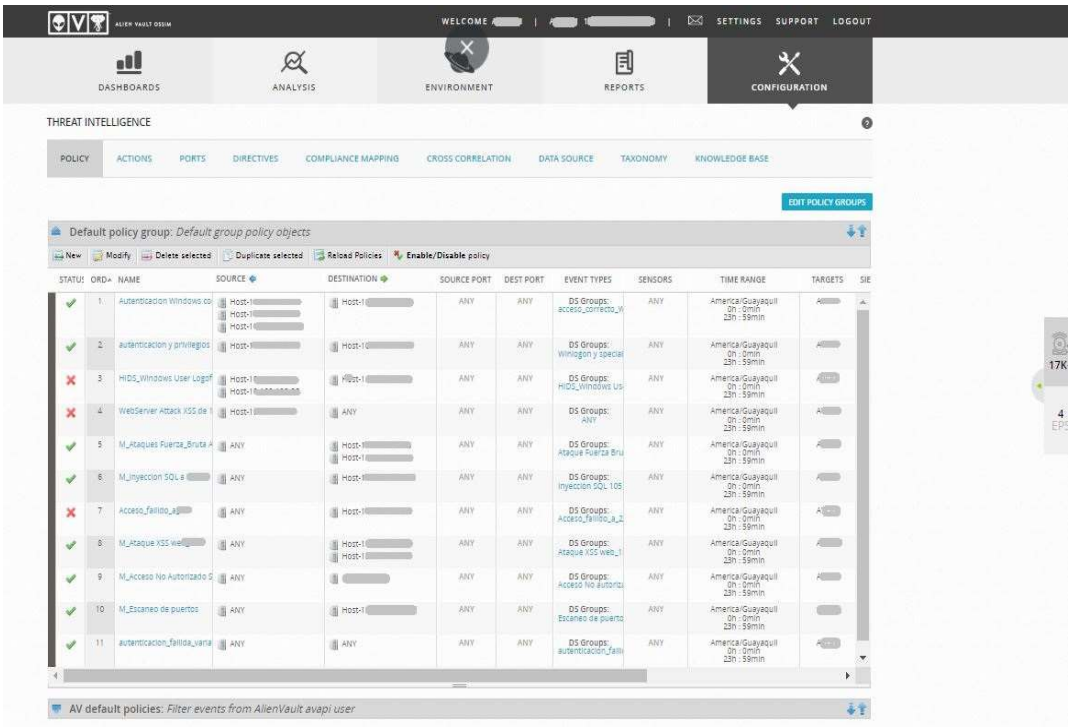


Figura 53. Tablero de Inteligencia de Amenazas

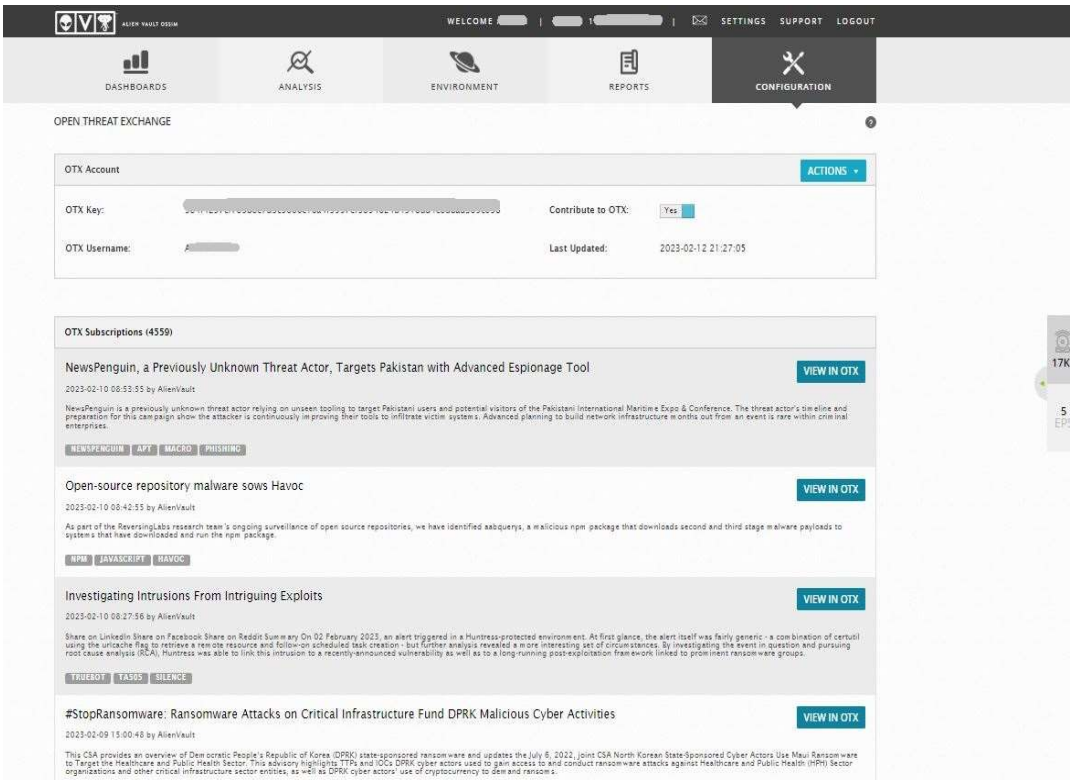


Figura 54. Tablero de OTX

6.9 Conclusiones y Recomendaciones

6.9.1 Conclusiones

Se aplicó las configuraciones iniciales en los dispositivos seleccionados de manera adecuada tanto con el uso de agentes y complementos integrados en la herramienta, así como en el uso de complementos elaborados de manera personalizada.

Las políticas y acciones aplicadas que permita verificar el funcionamiento de las mismas y que detecten y alerten ataques y vulnerabilidades se evidenciaron en los tiques generados, así como en el filtrado de eventos.

Se elaboró una guía de componentes del sistema, la misma que sirve de apoyo a los usuarios y administradores del sistema.

6.9.2 Recomendaciones

Se recomienda agregar más activos críticos al sistema OSSIM para obtener una mayor carga en el flujo de trabajo que permita evaluar el rendimiento del sistema.

En cuanto a configuración de políticas, directivas y reglas a aplicarse en los activos se recomienda incrementarlas para realizar mayores filtrados y lograr un mayor alcance en el uso de la herramienta.

Se recomienda tener un acceso más completo a la información de cada uno de los diferentes activos que forma parte de la red DMZ que permita lograr una configuración más afinada y se obtenga mejores resultados.

Simular un ambiente controlado en el cual se puedan realizar pruebas exhaustivas que permitan un mayor análisis y explotación de la presente herramienta.