UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Implementación de un sistema SIEM para mejorar la detección y respuesta a incidentes de seguridad en una institución financiera

AUTOR

Tenezaca Carpio, Eduardo Giovanny

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Cárdenas Cobo, Jesennia del Pilar

Santa Elena, Ecuador

Año 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
JESENNIA DEL PILAR CARDENAS COBO

Lic. Jesennia Cárdenas Cobo, Ph.D.
TUTOR

Firmado electrónicamente por:
SANG GUUN YOO .

Ing. Sang Guun Yoo, Ph.D
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Zambrano Martínez, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIO GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Eduardo Giovanny Tenezaca Carpio, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
JESENNIA DEL PILAR CARDENAS COBO

Lic. Jesennia del Pilar Cárdenas Cobo, Ph.D.

Santa Elena, 15 de diciembre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Eduardo Giovanny Tenezaca Carpio**

DECLARO QUE:

El trabajo de Titulación, Implementación de un sistema SIEM para mejorar la detección y respuesta a incidentes de seguridad en una institución financiera previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 15 de diciembre de 2024

EL AUTOR

EDUARDO GIOVANNY TENEZACA CARPIO

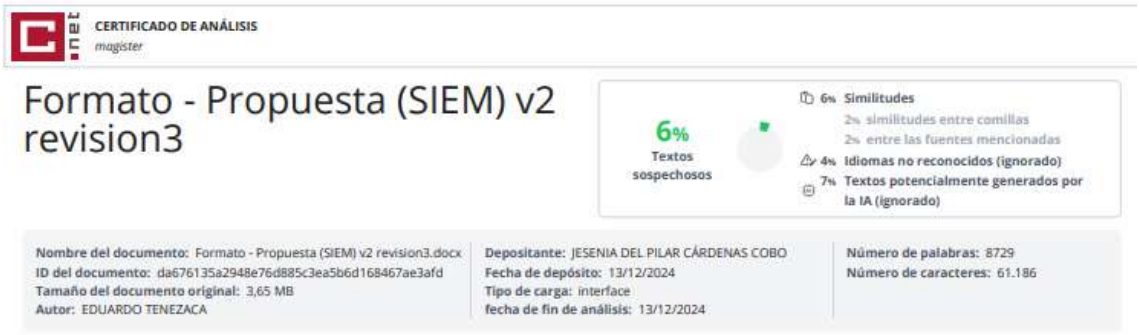
Digitally signed by EDUARDO GIOVANNY TENEZACA CARPIO

Eduardo Giovanny Tenezaca Carpio

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Implementación de un sistema SIEM para mejorar la detección y respuesta a incidentes de seguridad en una institución financiera, presentado por el estudiante, Eduardo Giovanny Tenezaca Carpio fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



CERTIFICADO DE ANÁLISIS
magister

Formato - Propuesta (SIEM) v2 revision3

6% Textos sospechosos

6% Similitudes
2% similitudes entre comillas
2% entre las fuentes mencionadas
4% Idiomas no reconocidos (ignorado)
7% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: Formato - Propuesta (SIEM) v2 revision3.docx
ID del documento: da676135a2948e76d885c3ea5b6d168467ae3afd
Tamaño del documento original: 3,65 MB
Autor: EDUARDO TENEZACA

Depositante: JESENIA DEL PILAR CÁRDENAS COBO
Fecha de depósito: 13/12/2024
Tipo de carga: interface
fecha de fin de análisis: 13/12/2024

Número de palabras: 8729
Número de caracteres: 61.186

TUTOR

Firmado electrónicamente por:
JESENNIA DEL PILAR CARDENAS COBO

Lic. Jesennia del Pilar Cárdenas Cobo Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **Eduardo Giovanny Tenezaca Carpio**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi propuesta metodológica y tecnológica avanzada con fines de difusión pública, además apruebo la reproducción de esta propuesta metodológica y tecnológica avanzada dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 15 de diciembre de 2024

EL AUTOR

EDUARDO GIOVANNY TENEZACA CARPIO

Digitally signed by EDUARDO GIOVANNY TENEZACA CARPIO

Eduardo Giovanny Tenezaca Carpio

AGRADECIMIENTO

Agradezco a Dios, que me ha brindado salud y me ha guiado para seguir cumpliendo las metas propuestas.

A mis docentes, en especial a la tutora Jesennia por su apoyo paciencia y dedicación, a mis amigos Alexandra, Leonardo, Peter, Jefferson, que de una u otra forma me ayudaron durante este proceso de formación académica.

Eduardo Giovanny, Tenezaca Carpio

DEDICATORIA

Este trabajo es dedicado para mis padres, hermanos, esposa e hijos que son mi motivación para alcanzar mis objetivos y mejorar cada día. Espero hacerlos sentir orgullosos.

Eduardo Giovanny, Tenezaca Carpio

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el siguiente proyecto de investigación se analizara e implementará un Sistema de Gestión de Eventos e Información (SIEM), mediante la evaluación técnica de una herramienta, que permita mejorar la detección y respuesta a Incidentes de seguridad en una institución Financiera mediante la monitorización de eventos y evaluación de vulnerabilidades de la infraestructura tecnológica y sistemas de información, obteniendo así una visión holística que permita la toma de decisiones y mitigar de forma proactiva las vulnerabilidades de una entidad financiera.

Como primer punto, tenemos el planteamiento de la propuesta tecnológica, en donde se orienta y visualiza los objetivos, así mismo, se manifiesta la necesidad de esta implementación y los beneficios suscitados al alcance de la propuesta. Como segundo punto, se presenta el marco teórico referencial, así como la revisión de literatura, desarrollo teórico conceptual, arquitectura, funciones y diseño de SIEM. Como tercer punto, se puede observar el contexto de la investigación e implementación del sistema, además del alcance y la investigación de la población y muestra, haciendo uso de técnicas e instrumentos de recolección de datos, levantamiento de información y procesamiento de los datos para modelar el análisis de vulnerabilidades en la institución financiera. Como cuarto punto, se presentan los resultados y discusiones inherentes al análisis de vulnerabilidades realizados, así como la configuración, la correlación de eventos, entre otros. De igual forma, se realiza un precedente de cómo se encontró y los resultados de la implementación del SIEM en la entidad financiera gracias a la toma de decisiones en base a la información recolectada.

Posterior a esto se presentan los resultados plasmados en las conclusiones y recomendaciones para finalmente visualizar la bibliografía y anexos.

Palabras claves: SIEM, Ciberseguridad, Incidentes.

ABSTRACT

In the following research project, an Event and Information Management System (SIEM) will be implemented, through the technical evaluation of a tool, which will improve the detection and response to security incidents in a financial institution through event monitoring and evaluation of vulnerabilities in the technological infrastructure and information systems, thus obtaining a holistic vision that allows decision-making and proactively mitigates the vulnerabilities of a financial entity.

As a first point, we have the approach of the technological proposal, where the objectives are oriented and visualized, likewise, the need for this implementation and the benefits raised within the scope of the proposal are manifested. As a second point, the theoretical framework is presented, as well as the literature review, conceptual theoretical development, architecture, functions and design of SIEM. As a third point, the context of the research and implementation of the system can be observed, in addition to the scope and investigation of the population and sample, making use of data collection techniques and instruments, information gathering and data processing to model. the analysis of vulnerabilities in the financial institution. As a fourth point, the results and discussions inherent to the vulnerability analysis carried out are presented, as well as the configuration, the correlation of events, among others. Likewise, a precedent is made of how it was found and the results of the implementation of the SIEM in the financial entity thanks to the decision making based on the information collected.

After this, the results reflected in the conclusions and recommendations are presented to finally view the bibliography and annexes.

Keywords: SIEM, Cybersecurity, Incidents.

INTRODUCCIÓN

Hoy en día las instituciones financieras se enfrentan a un incremento en los riesgos en la ciberseguridad. La protección de la información de los clientes en conjunto con la integridad y confidencialidad de los sistemas se ha transformado en objetivos estratégicos. Un elemento esencial para mejorar la estrategia de ciberseguridad es la implementación de tecnologías que puedan identificar de forma rápida y responder de forma eficiente a incidentes de seguridad. (Revista IT ahora, 2024)

De acuerdo con Gartner, para el año 2024, las compañías que implementen una estructura de ciberseguridad disminuirán el impacto financiero de los incidentes de seguridad individuales en una media del 90%. Estos sistemas permiten una mejor gestión de incidentes y una capacidad de respuesta más ágil, aspectos críticos para las cooperativas que manejan recursos limitados, pero deben mantener altos estándares de seguridad(Susan Moore & Gartner, 2022)

Los firewalls son una primera línea de defensa, pero no son suficientes para prevenir todos los tipos de ataques cibernéticos. Para identificar, analizar y responder de manera efectiva a amenazas más sofisticadas, es necesario contar con herramientas de detección y análisis avanzadas. La Gestión de Eventos e Información de Seguridad (SIEM), al correlacionar eventos de seguridad provenientes de múltiples fuentes, incluyendo el firewall, ofrecen una visión holística de la postura de seguridad de la organización, permitiendo detectar y responder a amenazas que podrían pasar desapercibidas por un firewall(Luis Ramírez Quevedo, 2024)

Los SIEM son herramientas que aportan a las organizaciones centralizar, correlacionar y analizar grandes volúmenes de datos de logs y eventos de seguridad en tiempo real. Esto mejora la detección temprana de amenazas y permite una respuesta más rápida(LogRhythm, 2024)

La implementación de un SIEM es un paso proactivo y estratégico para mejorar la detección y resolución de incidentes de seguridad, dando apoyo a la continuidad del negocio. Según el Informe de Amenazas de Ciberseguridad en América Latina de (Kaspersky, 2023), Ecuador ha visto un aumento significativo en incidentes de ciberseguridad, con un incremento del 24% en ataques dirigidos a instituciones financieras en el último año. Este contexto resalta la necesidad de fortalecer la detección y respuesta ante incidentes a través de la implementación de un sistema SIEM.

La Superintendencia de Economía Popular y Solidaria (SEPS) a través de la normativa SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 en su anexo 1 en la sección Controles tecnológicos menciona "*Las entidades, empresas y/o CONAFIPS de cada régimen, deberán diseñar, implementar y gestionar, la arquitectura segura para proteger los activos digitales en función de la particularidad tecnológica*" y en la sección Monitoreo y Detección menciona "*Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda y de acuerdo a la clasificación de activos, deberán implementar sistemas que mantengan registros de log correlacionados de la infraestructura critica, que permitan su detección, análisis y depuración*"

(Superintendencia de Economía Popular y Solidaria, 2022), la SEPS indica la necesidad de implementar sistemas que permitan registrar, correlacionar y analizar los logs de la infraestructura crítica. Un SIEM se presenta como una solución integral para cumplir con estos requerimientos, al centralizar y correlacionar los datos de seguridad provenientes de múltiples fuentes, facilitando la detección temprana de amenazas y la respuesta a incidentes.

Las cooperativas, al manejar información financiera y personal sensible son objetivos atractivos para ciberataques. La cooperativa de ahorro y crédito Lucha Campesina tiene aproximadamente 68.000 socios entre las 10 agencias, Cumandá, Bucay, Naranjito, Naranjal, Simón Bolívar, Baba, El Triunfo, La Troncal, Milagro y Vinces(referenciar), como institución financiera, se encuentra expuesta a diversos riesgos en su infraestructura tecnológica.

El objetivo de la presente propuesta es implementar un prototipo de SIEM en la Cooperativa Lucha Campesina con la finalidad de mejorar la postura de seguridad lo que permitirá detectar de manera proactiva amenazas, reducir el tiempo de respuesta a incidentes de seguridad. Este proyecto demostrará la viabilidad y los beneficios de implementar un SIEM en una institución financiera.

Planteamiento de la investigación

La dependencia de los sistemas tecnológicos en las instituciones financieras, y la creciente sofisticación de las amenazas cibernéticas, crean la necesidad de contar con herramientas robustas y eficientes para la detección y respuesta a incidentes de seguridad. El Sistema Gestión de Eventos e Información de Seguridad (SIEM) emergen como una solución integral para abordar esta problemática, ya que permite la centralización, correlación y análisis de grandes volúmenes de datos, facilitando la identificación de patrones de ataque y la mejora en los tiempos de detección incidentes.

La Cooperativa Lucha Campesina, se enfrenta al desafío de proteger sus sistemas y datos, La falta de visión unificada de los sistemas y eventos de seguridad dificultan la detección proactiva de incidentes y la respuesta oportuna.

Formulación del problema de investigación

¿Cuáles son las principales causas que dificultan la respuesta a incidentes en la Cooperativa de Ahorro y Crédito Lucha Campesina Ltda.?

Objetivo General:

Implementar un Sistema de Gestión de Eventos e Información (SIEM), mediante la evaluación técnica de una herramienta, que permita mejorar la detección y respuesta a Incidentes de seguridad en una Institución Financiera: Un Estudio de Caso en Cooperativa Lucha Campesina Ltda.

Objetivos Específicos:

- Analizar el estado de situación actual de la infraestructura tecnológica de la entidad financiera.
- Evaluar una solución SIEM que se ajuste a las necesidades de la entidad financiera.
- Implementar el sistema de seguridad centralizado y analizar información de correlación de eventos y alarmas para la toma de decisiones.

Planteamiento hipotético

El uso de un SIEM mejora la detección y respuesta a incidentes de seguridad en una institución Financiera.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1. Revisión de literatura

Indonesia, el artículo publicado por (Konstantinos Bezas & Foteini Filippidou, 2023) fue "*Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)"* cuyo objetivo era "*El estudio de sistemas SIEM basándose en características conocidas por la bibliografía y las mediciones experimentales realizadas por investigadores*." los investigadores utilizaron una metodología de revisión sistemática de la literatura concluyendo que "*El sistema Ossim parece ser el más investigado. Sus características lo convierten en el código abierto más completo que se ha estudiado e igual a muchos comerciales*"

España, el articulo realizado por (González-Granadillo, 2021) "*Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures*" el objetivo a cumplir "*revisar las herramientas de gestión de eventos e información de seguridad (comerciales y de código abierto) más utilizadas con el objetivo de identificar sus principales características, beneficios y limitaciones para detectar y reaccionar contra escenarios de ataque actuales*" los investigadores utilizaron una investigación

descriptiva sobre 42 soluciones SIEM en el mercado concluyendo que "*las condiciones son buenas para fomentar la inversión en mejorar y ampliar esta tecnología como componente clave no sólo para sistemas de control industrial con centros de operaciones de seguridad, sino también para proporcionar gestión de ciberseguridad a las PYMES con conocimientos y capacidades de seguridad*"

Ecuador, el trabajo investigativo de (Muñoz Álvarez, 2022) fue "*IMPLEMENTACIÓN DE UN GESTOR DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM) PARA LA PREVENCIÓN Y DETECCIÓN DE CIBER AMENAZAS EN UNA ENTIDAD GUBERNAMENTAL*" con el objetivo a cumplir "*Implementar un Sistema de Gestión de Eventos e Información (SIEM), utilizando la herramienta de código libre OSSIM AlienVault, para la prevención y detección de incidentes, amenazas y ataques de seguridad en la infraestructura tecnológica de una entidad gubernamental*", el investigador no menciona la metodología que utilizo, pero realizo un análisis, planificación, ejecución y pruebas concluyendo que: "*Todos los eventos registrados serán recopilados por OSSIM AlienVault y con ello, determinara si existe algún agente, código o ataque malicioso permitiendo tomar acciones correctivas o preventivas*"

Ecuador, la investigación realizada por (Agudelo Castro et al., 2022) fue "E*laboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft*" donde el objetivo principal fue "*Definir cinco casos de uso para la implementación de un SIEM que funciona a través de un SOC para las necesidades de ciberseguridad dentro de un ambiente de negocio del sector financiero*" se utilizó una metodología descriptiva, donde la fuente de datos utilizada fue "CyberArk Privileged Threat Analytics", concluyendo que "L*a definición correcta de un caso de uso desarrolla procesos de gestión de incidentes de ciberseguridad para mitigarlos, eliminarlos y prevenirlos*"

1.2. Desarrollo teórico y conceptual

SIEM

Un SIEM (Security Information and Event Management) es una estrategia orientada a la administración de eventos de seguridad informática que busca proporcionar a las empresas una respuesta rápida y efectiva para identificar y reaccionar ante posibles amenazas que afecten sus sistemas tecnológicos.(IBM, 2024)

Los SIEM fueron creados para brindar a las empresas una respuesta ágil y exacta para identificar y reaccionar ante cualquier amenaza a sus sistemas informáticos. (Admcloudservices, 2024). Adicional, reúnen toda la información en una base de datos centralizada para realizan un análisis exhaustivo, identificando tendencias y patrones de comportamiento que permitan distinguir actividades inusuales.

Una solución SIEM se compone de diversos módulos que permiten a los analistas de seguridad coordinar de manera efectiva la detección, investigación y respuesta ante incidentes de seguridad y actividades maliciosas.(Harper et al., 2010)

A continuación, se detalla de manera general la arquitectura de un SIEM.

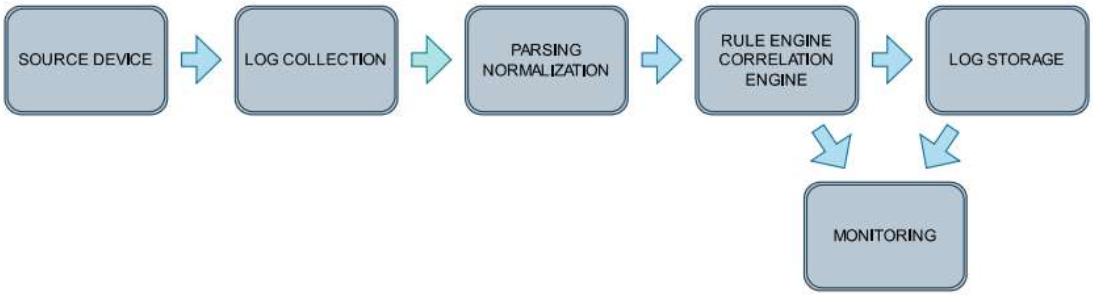


Ilustración 1 Arquitectura SIEM Elaboracion Propia

Arquitectura de un SIEM

Dispositivo fuente: realiza la captura de la información, recuperando registros que se almacenan y procesan en el SIEM. (Stellar Cyber, 2024)

Registro de Colección: realiza la obtención o recopilación de todos los registros de los dispositivos fuentes para transportarlos al SIEM.(Check Point, 2024)

Análisis / Normalización de Registros: realiza la asignación de un formato estándar de lectura de registros y generación de reglas del sistema para su uso en el SIEM.(Microsoft Learn Challenge, 2024)

Núcleo de Reglas / Núcleo de Correlación: el primero realiza la ampliación de la normalización de eventos para la activación de alertas en el SIEM; mientras que el núcleo de correlación realiza la comparación de todos los eventos normalizados de distintas fuentes de acuerdo con reglas creadas previamente.(Incibe, 2017)

Almacenamiento de Registros: favorece el trabajo en un único almacén de datos centralizado o distribuido, ayudando que la relación entre las diferentes funciones del SEM y las funciones forenses e informes del SIM sean acopladas, dependiendo de la cantidad de datos recogidos, y de la infraestructura de TIC.(Estela Campos, 2020)

Monitoreo: mediante una interfaz de consola y una interfaz web, se visualiza y analizan todos los datos almacenados en el SIEM, facilitando la gestión del sistema con una visión amplia e integral del entorno. (Baluja García et al., 2012)

Las funciones de un SIEM deben incluir:

Gestión de registros: agregan y centralizan registros de diversas fuentes, incluidos servidores, aplicaciones, dispositivos de red, y actividades de los usuarios. (García Merino, 2018)

Monitoreo en tiempo real: lo que permite a las instituciones financieras detectar eventos de seguridad a medida que ocurren y responder con prontitud a amenazas potenciales. (Morales Morera Randy, 2020)

Correlación de eventos de seguridad: utilizan algoritmos de correlación para analizar los eventos de seguridad, identificando anomalías que pudiesen derivar en incidentes de seguridad. (Red Hat, 2023)

Integración de inteligencia de amenazas: esta funcionalidad se conecta con fuentes de inteligencia de amenazas externas, las cuales proporcionan información actualizada sobre amenazas emergentes, vulnerabilidades y tácticas de ataque.(Kevin Bryan Costa Castillo, 2024)

Informes de cumplimiento: pueden utilizar informes generados por SIEM para demostrar el cumplimiento de los requisitos reglamentarios, los estándares de la industria y las políticas de seguridad internas.(Reddy Turpu, 2021)

Ciberseguridad

Se define como Ciberseguridad a un conjunto de acciones o directivas que una vez implementadas en un esquema informático, nos permite proteger la información de un sistema en general, así como también la infraestructura que salvaguarda dicha información. En otros criterios menos técnicos, la ciberseguridad tiene como definición la protección de datos espaciales y red interna garantizando la seguridad en la interacción entre personas. (Piñón et al., 2023)

En la actualidad los ataques cibernéticos tienen un crecimiento significativo, por lo que, la necesidad de adquirir medios para proteger la información consigue que las empresas busquen aplacar el impacto suscitado por un atacante, esto logra que se creen plataformas de ciberseguridad, capacitaciones, estándares, normativas, entre otros términos. (Sesmero, 2023)

Firewall

Es un sistema tecnológico permite prevenir ataques mediante una serie de reglas o directivas bloqueando acceso no permitido o autorizado a un determinado lugar en el ciberespacio(Ruiz Sala, 2024). Por ende, el firewall establece quien puede ingresar o tener acceso a cierto directorio o carpeta en la red interna de una entidad empresarial, así

mismo, si en algún momento un agresor cibernético logra vulnerar la seguridad de este dispositivo, este quedará expuesto en torno al agresor(Agualongo Domínguez, 2024).

Ataques cibernéticos

Los ataques informáticos son categorizados como acciones intencionales para comprometer la seguridad de los sistemas o redes internos de alguna empresa en específico. Con un ataque informático los atacantes pueden conseguir acceso, manipular, destruir, modificar o retener información, y la empresa quedar a expensas del atacante, ya que el objetivo final del atacante es el robo de información confidencial e importante(Choto Tuquerres, 2024). En este punto, la ciberseguridad juega un papel de suma importancia para la detección y protección de estos ataques, y sobre todo la notificación temprana de estas vulnerabilidades.(CALERO ESPINOZA, 2024)

Servidores

Se conocen como equipos tecnológicos interconectados que sirven para el almacenamiento de datos y distribución de información para su posterior uso a usuarios con acceso autorizado. En estos servidores se realiza el despliegue de aplicaciones y bases de datos acorde a la funcionalidad de este. Por lo tanto, son la primera línea de información que se van a intentar vulnerar y por lo que se debe realizar una correcta distribución de permisos.(Castañeda Cobeñas et al., 2023)

Tipos de ataques informáticos

- Malware: se define como un software malicioso que puede infectar un sistema informático y causar daño en los servidores. Algunos tipos de malware son, troyanos, gusanos y ransomware, que normalmente se los consideran virus.(Danilo et al., 2024)
- Phishing: Esto se realiza con el fin de suplantar la identidad de una fuente legítima para engañar a los usuarios y obtener información personal o financiera(Danilo et al., 2024)
- Denegación de servicios (DoS): Ataque informático que busca sobrecargar o saturar un sistema o red con tráfico para hacerlo inoperable(Danilo et al., 2024)
- SQL injection: inyección de un código SQL con fines de vulneración de bases de datos de la empresa(Danilo et al., 2024)
- Cross-site scripting (XSS): inyección de códigos javascript maliciosos en una página web para atacar a usuarios que la visitan (Danilo et al., 2024)
- Ataques de fuerza bruta: Intentos consecuentes o repetidos de vulneración de claves de seguridad (Danilo et al, 2024)

Marco Normativo

SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-02 En el anexo 1 menciona en la sección controles tecnológicos arquitectura segura "*Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán diseñar, implementar y gestiona, la arquitectura segura para proteger los activos digitales en función de la particularidad tecnológica*" (Superintendencia de Economía Popular y Solidaria, 2022)

LEY ORGÁNICA DE PROTECCIÓN DE DATOS La LOPD establece en el capítulo VI Seguridad de datos personales en el artículo 37 "*El responsable o encargado del tratamiento de datos personales, deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.*

Entre otras medidas, se podrán incluir las siguientes.

Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes" y en el capítulo XI sección 2ª, articulo 70 literal 4 Se considera infracciones graves del encargado de protección de datos "*No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales*" (Asamblea Nacional, 2021), es por ello que la implementación de un SIEM nos ayuda centralización y correlación de logs, detección en tiempo real facilitando la gestión de incidentes de seguridad, proporcionando información detallada sobre los eventos ocurridos.

CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

Como caso de estudio se escogió a la cooperativa de ahorro y crédito Lucha Campesina que se encuentra ubicada en la provincia de Chimborazo, la sede principal se encuentra cantón Cumandá de la misma provincia, tiene nueve sucursales en Bucay, Naranjito, Milagro, El Triunfo, Simón Bolívar, Naranjal en la provincia del Guayas, La Troncal en la provincia del Cañar y Baba, Vinces en la provincia de los Ríos. Aproximadamente tiene 63.187 socios entre las 10 agencias. (Lucha Campesina, 2024) con la autorización de gerente general de la cooperativa (ver anexo 1), se logró obtener logs de octubre y noviembre 2024.

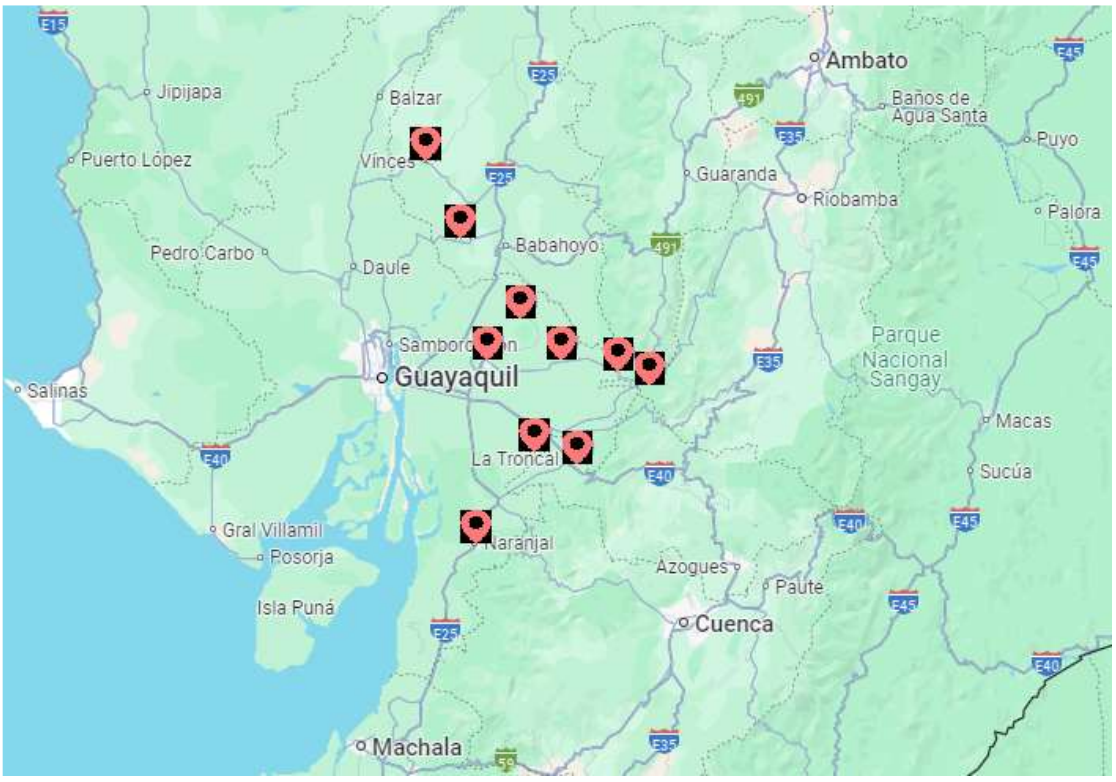


Ilustración 2 Ubicación Lucha Campesina (Elaboración propia)

2.2. Diseño y alcance de la investigación

El enfoque no experimental se utilizará en la presente investigación, se analizará una situación real sin alterar las variables involucradas. Para detallar los resultados obtenidos y el proceso de implementación del SIEM en la Cooperativa Lucha Campesina se seguirá un enfoque principalmente descriptivo. La combinación de la investigación no

experimental y la descriptiva permite obtener una compresión más detallada del impacto del SIEM en la mejora de la seguridad de la institución.

2.3. Tipo y métodos de investigación

Para obtener una comprensión integral del impacto de la implementación del SIEM en la Cooperativa Lucha Campesina Ltda., se empleará un enfoque de investigación cuantitativo. A través del análisis de la institución, definición de la mejor opción de SIEM, para su posterior instalación, configuración, implementación, monitoreo de eventos y tráfico de red, análisis de vulnerabilidades, plan de acción, análisis de vulnerabilidades-retest, finalmente la aprobación de pase a producción (comité de tecnología) de los datos recopilados, se identificarán tendencias en relación con la efectividad del SIEM en la detección y respuesta a incidentes.

2.4. Población y muestra

La población de este estudio está conformada por 727906 eventos de logs generados por los siguientes equipos: firewall, switch, directorio activo, servidor de aplicaciones y base de datos, de la Cooperativa de Ahorro y Crédito Lucha Campesina en el período comprendido entre [21 de octubre de 2024] y [15 de noviembre de 2024]. Lo que conforman un total de cuatro (4) equipos a los cuales se le realizará el análisis correspondiente para la detección de eventos. Estos logs, que actúan como un registro detallado de todas las actividades del sistema, nos proporcionan una fuente rica de datos para analizar patrones de uso, identificar posibles anomalías y evaluar el rendimiento general de la infraestructura.

2.5. Técnicas e instrumentos de recolección de datos

Para seleccionar el SIEM más adecuado para nuestras necesidades, se desarrolló una ficha técnica (ver Ilustración 5), que incluía criterios como: funcionalidad, escalabilidad, costo, reportes, monitorización de comportamiento. Esta ficha técnica fue utilizada para evaluar las diferentes opciones disponibles en el mercado y tomar una decisión informada. Además, se realizó una revisión sistemática de la literatura siguiendo las recomendaciones de Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA*)* para identificar las mejores prácticas en la selección de SIEM (ver Ilustración 4).

2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

El proceso de evaluación de la validez y confiabilidad de los instrumentos utilizados para recolectar información en este proyecto implicó una revisión bibliográfica de las reglas

de correlación y detección de eventos configuradas en el SIEM. Se evaluó la precisión de estas reglas al comparar los resultados obtenidos con incidentes de seguridad conocidos. La confiabilidad de los datos recopilados se verificó mediante la comparación con otras fuentes de información, como logs de sistemas operativos, aplicaciones y redes, asegurando así la integridad y consistencia de la información utilizada para la toma de decisiones en materia de seguridad.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

A pesar de que los sistemas y servidores de la cooperativa generan una gran cantidad de datos de logs, estos no están siendo aprovechados al máximo. La falta de análisis de los logs implica un desconocimiento de las actividades que ocurren en la red, lo que aumenta el riesgo de sufrir ataques cibernéticos sin detectarlos a tiempo.

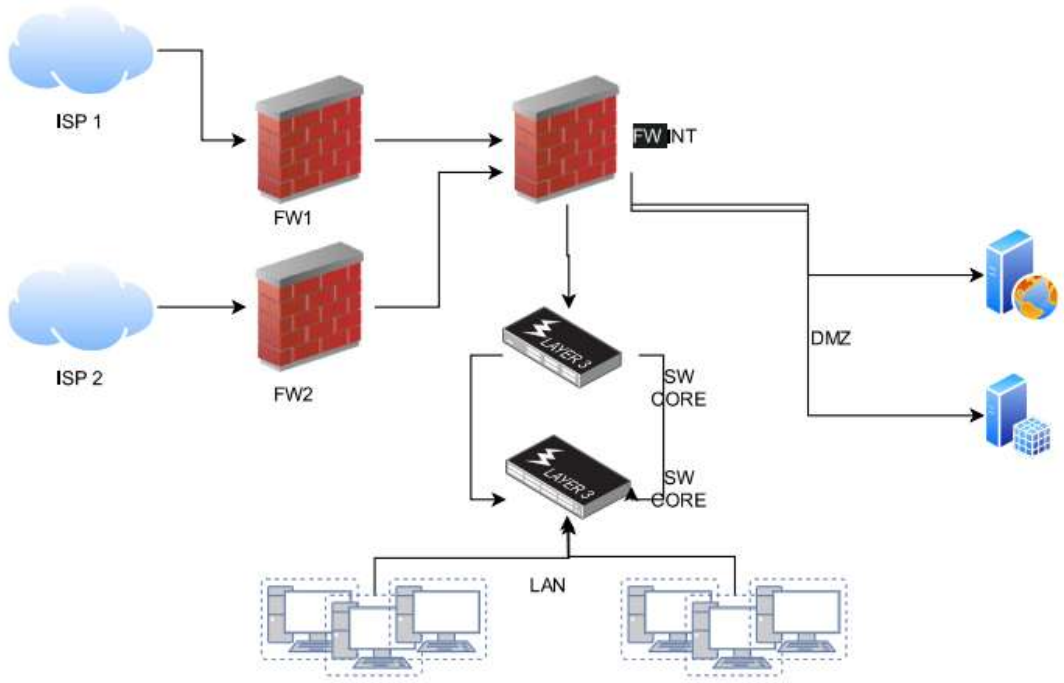


Ilustración 3 Diagrama actual de la red de la institución. Elaboración propia

La institución en su Data Center cuenta con 30 servidores entre ellos 12 servidores físicos, 18 servidores virtuales, 1 firewall, 5 switches, 4 servidores de almacenamiento en red. Los servidores prestan servicios como base de datos, aplicaciones, directorio activo, entre otros.

Debido a que los equipos son de producción y contienen información y procesos muy sensibles, luego de realizar el análisis con el personal a cargo, se establece aplicar la implementación y configuraciones en un grupo de equipos en un entorno controlado con el fin de no poner en riesgo la operatividad de todos los servicios que brinda esta área critica de la institución, se define un alcance basado en objetivos, por lo tanto, se trabajó con los equipos descritos a continuación en la tabla.

Tabla 1 Activos a monitorear

EQUIPO	Numero de equipos
Servidor de Bases de Datos	1
Servidor de Aplicaciones	1
Servidor Active Directory	1
Firewall	1
Switch	1
Servidor Linux	1
Total	**6**

Equipos que se encuentran en el centro de cómputo principal.

Configuración servidor virtual Active Directory

- Intel Xeon CPU E5-2660 v4
- System type 64 bits
- Procesador intel Xeon 2.00 GHz
- Memoria RAM 10.0 GB
- Disco sata de 100 GB
- Windows Server Standard 2022 Standard

Configuración servidor Base de datos

- Intel(R) Xeon(R) E-2336
- System type 64 bits
- Procesador intel Xeon 2.90 GHz
- Memoria RAM 32.0 GB
- Disco SSD de 1 TB
- Windows Server Standard 2022 Standard

Configuración servidor Aplicaciones

- Intel(R) Xeon(R) E-2336

- System type 64 bits
- Procesador intel Xeon 2.90 GHz
- Memoria RAM 32.0 GB
- Disco SSD de 1 TB
- Windows Server Standard 2019 Standard

Configuración Firewall

- Sophos XGS 3300
- ALMACENAMIENTO SSD SATA-III integrado, mín. 240 GB
- SFOS
- Puertos LAN 1-8 Velocidad 10/100/1000 Mbps

Configuración Sw Aruba

- Dual Core ARM® Coretex A9 @ 1016 MHz,
- DDR3 SDRAM 1 GB
- eMMCProcesador intel Xeon 2.20 GHz 4 GB

Equipos que se encuentran en el data center alterno en la ciudad de Guayaquil

Configuración servidor virtual Alien Vault

- Intel Xeon CPU E5-2660 v4
- System type 64 bits
- Procesador intel Xeon 2.00 GHz
- Memoria RAM 12.0 GB
- Disco sata de 500 GB
- alienvault 4.19.0-0.deb9.27-amd64

Configuración servidor virtual Linux

- Intel Xeon Silver 4214
- System type 64 bits
- Procesador intel Xeon 2.20 GHz
- Memoria RAM 8.0 GB
- Disco sata de 100 GB
- Ubuntu 24.04.1 LTS

Se identificaron 30 documentos en total, 11 de bases de datos y 19 de libros, documentos legales, tesis y páginas web gubernamentales. Fueron excluidos 4 por no estar a texto completo, 3 por duplicidad y 3 por no ajustarse al tema. La muestra fue de 18 documentos, de ellos identificados en bases de datos 8 distribuidos en: Researchgate n = 3; ; IEEE=2; IJCS n = 1; sensors n = 1. De los 10 obtenidos por otras vías se encuentran: 6 tesis, 2 libros y 2 normas los cuales fueron recuperados de páginas web gubernamentales y repositorios, como se representa en el flujograma de búsqueda de los documentos

incluidos el cual fue elaborado teniendo en cuenta las recomendaciones dadas por la Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) (Page et al., 2021). (Figura 3)

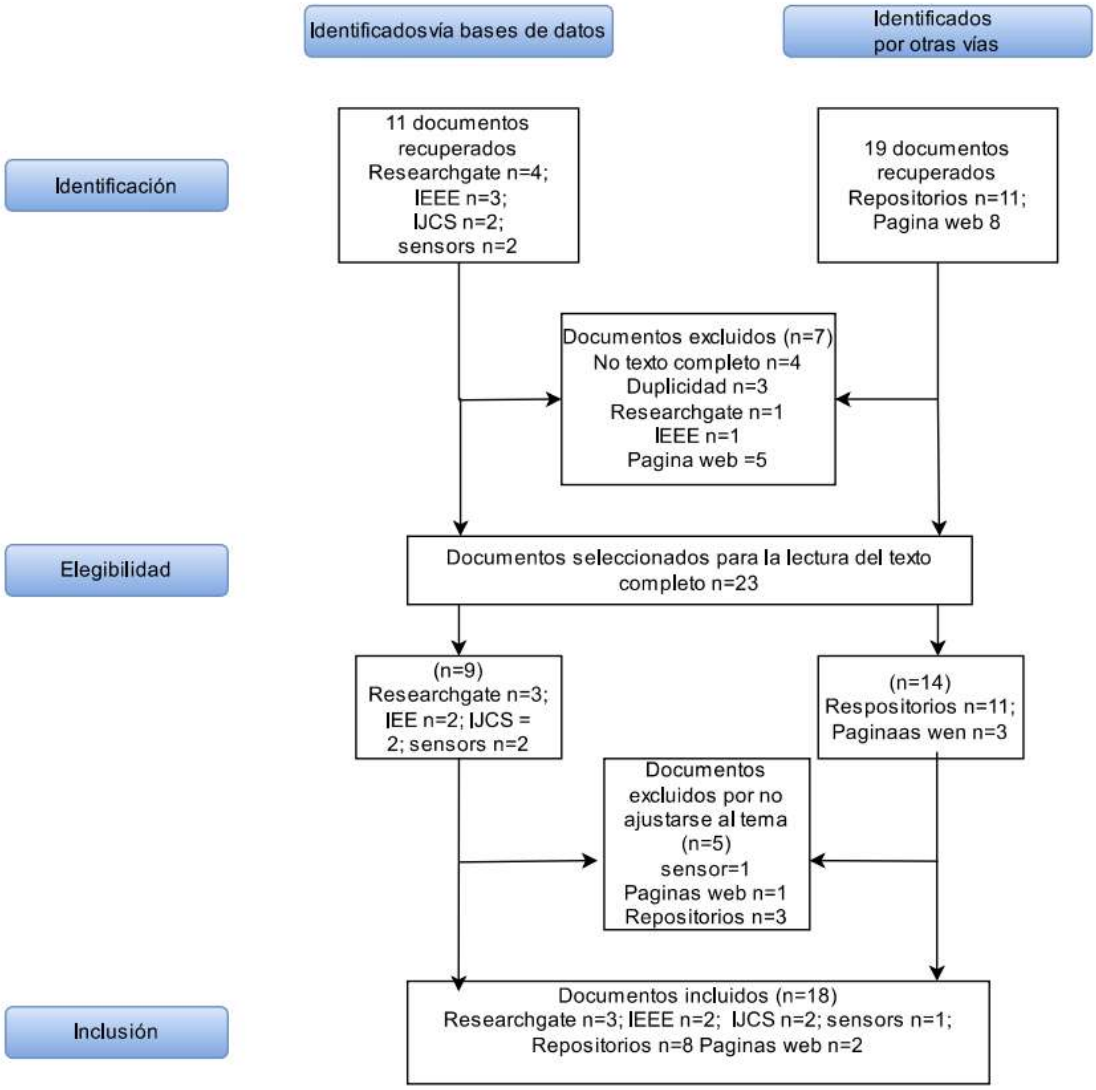


Ilustración 4 Flujo de evaluación del SIEM. (Elaboración propia)

Aunque todas las soluciones SIEM tienen como núcleo la recolección, almacenamiento y correlación de datos de eventos, OSSIM AlienVault se distingue por ofrecer un conjunto más amplio de características y funcionalidades, superando a muchas opciones comerciales y de código abierto disponibles en el mercado.

Para la evaluación se da cada característica SIEM basado en categorías como: alto (totalmente implementado), promedio (parcialmente implementado), bajo (no implementado).

Tabla 2 Categoría de las capacidades SIEM

Categoría	
Alto	
Promedio	
Bajo	

Los sistemas SIEM engloban un amplio espectro de capacidades, desde aspectos financieros y de desempeño hasta la gestión de grandes volúmenes de datos y la adaptación a entornos en constante evolución.

Desde este punto de vista la plataforma OSSIM AlienVault ofrece una solución de seguridad integral, intuitiva y asequible para organizaciones de todos los tamaños.

Capacidad	QRadar	LogRhythm	OSSIM AlienVault	Splunk	ArcSight	McAfee	SolarWinds	RSA
Almacenamiento								
Análisis de datos								
Análisis de riesgo								
Complejidad								
Escalabilidad								
Fuentes de datos								
Precio								
Procesamiento en tiempo real								
Reacción y reportes								
Reglas de correlación								
Rendimiento								
Resiliencia								
Seguridad								
Seguridad forense								
UBEA								
Visualización								
Volumen de datos								

Ilustración 5 Evaluación SIEM. (Gartner 2022)

Requisitos y acceso para implementación de OSSIM AlienVault

En el proceso de instalación es necesario unos requisitos básicos previo a la implementación.

- Dirección de correo para el envío de alertas
- Lista de subredes a monitorear
- Direcciones IP (3) para la implementación del servidor OSSIM (1), Sensor (1), Colector de eventos Linux (1).
- Credenciales o soporte para la configuración de los agentes HIDS
- Credenciales o asistencia para la habilitación de monitoreo syslog en el firewall
- Soporte o acceso a cuenta Sophos Central para configuración API integración.

Requerimientos.

La instalación se la realizara con las siguientes características

Configuración servidor virtual Alien Vault y Sensor

- Intel Xeon CPU E5-2660 v4
- System type 64 bits

- Procesador intel Xeon 2.00 GHz
- Memoria RAM 20.0 GB
- Disco sata de 500 GB
- alienvault 4.19.0-0.deb9.27-amd64

Configuración servidor virtual Linux

- Intel Xeon Silver 4214
- System type 64 bits
- Procesador intel Xeon 2.20 GHz
- Memoria RAM 8.0 GB
- Disco sata de 100 GB
- Ubuntu 24.04.1 LTS

La configuración para el servidor virtual se detalla especificando el nombre del servidor, Sistema Operativo Debian, Memoria 20 Gb y almacenamiento de 500 GB.

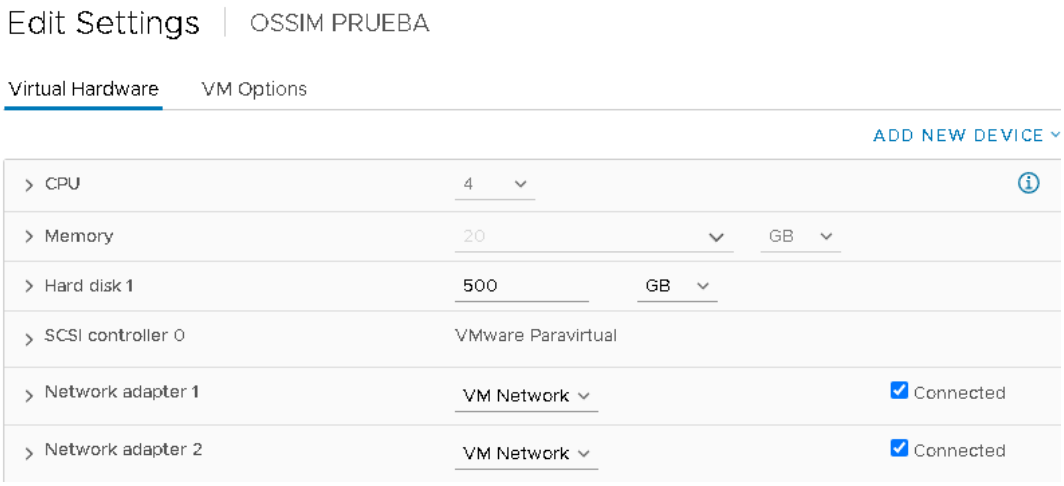


Ilustración 6 Configuración OSSIM AlienVault-Servidor (Elaboración Propia)

Métodos estadísticos utilizados por OSSIM Alien Vault.

OSSIM Alien Vault utiliza una serie de técnicas para identificar relaciones entre diferentes tipos de eventos:

Detector de patrones

Se nombra así a las aplicaciones capaz de escuchar el tráfico de red en busca de patrones que coincida con ataques conocidos o reglas, generando alertas de seguridad.(Puchades Olmos. Adrián & Peñalver Herrero, 2008)

Detector de anomalías

OSSIM Alien Vault integra detectores de patrones de open source como snort (NIDS, Network Intrusion Detection System), snare, osiris, HIDS (Host Intrusion Detection

System) instalados en los sistemas monitorizados de la red.(Puchades Olmos. Adrián & Peñalver Herrero, 2008)

Métodos de correlación.

Correlación lógica: Trabaja con las directivas de correlación, que especifican las condiciones que se deben cumplir para que un evento o una serie de eventos registrados en la base de datos puedan generar una alarma.

Correlación por inventario: Determina si un ataque en particular puede tener éxito en una determinada plataforma. Se emplea para descartar falsos positivos.

Correlación cruzada: Valida la información detectada por un sensor con los datos obtenidos por otros sensores de la red. Permite descartar falsos positivos o elevar la categoría de una alarma. (Manuel Madrid et al., 2015)

Tipos de Análisis Estadísticos

Análisis Descriptivo:

Se utiliza para resumir y describir las características básicas del tráfico de red. Incluye estadísticas como el volumen de tráfico, la cantidad de flujos, los protocolos más utilizados, y la duración de las conexiones.

Análisis de Tendencias:

Se centra en identificar patrones a lo largo del tiempo. Esto puede incluir el análisis de picos de tráfico, variaciones en el uso de ciertos protocolos o la aparición de nuevas direcciones IP (Estela Campos, 2020)

Análisis Comparativo:

Compara diferentes conjuntos de datos para identificar anomalías. Por ejemplo, comparar el tráfico de un día normal con el tráfico durante un ataque.(Luján Flores & Huancas Samillán, 2023)

Este tipo de análisis permite identificar y con ello responder rápidamente a posibles amenazas, optimizar la infraestructura de red y mejorar la política de seguridad de la organización.

3.1. Procedimiento

Se detalla el procedimiento desde la solicitud de autorización del proyecto, autorización, análisis de la institución, definición de los equipos a implementar el SIEM, definir el SIEM a utilizar, solicitud y aprobación de requisitos y accesos, instalación, configuración, definición de políticas, monitoreo, posibles errores, análisis y presentación de resultados de vulnerabilidades, toma de decisión, definición y ejecución de plan de acción, análisis y presentación de resultados post-plan de acción, aprobación pase a producción.

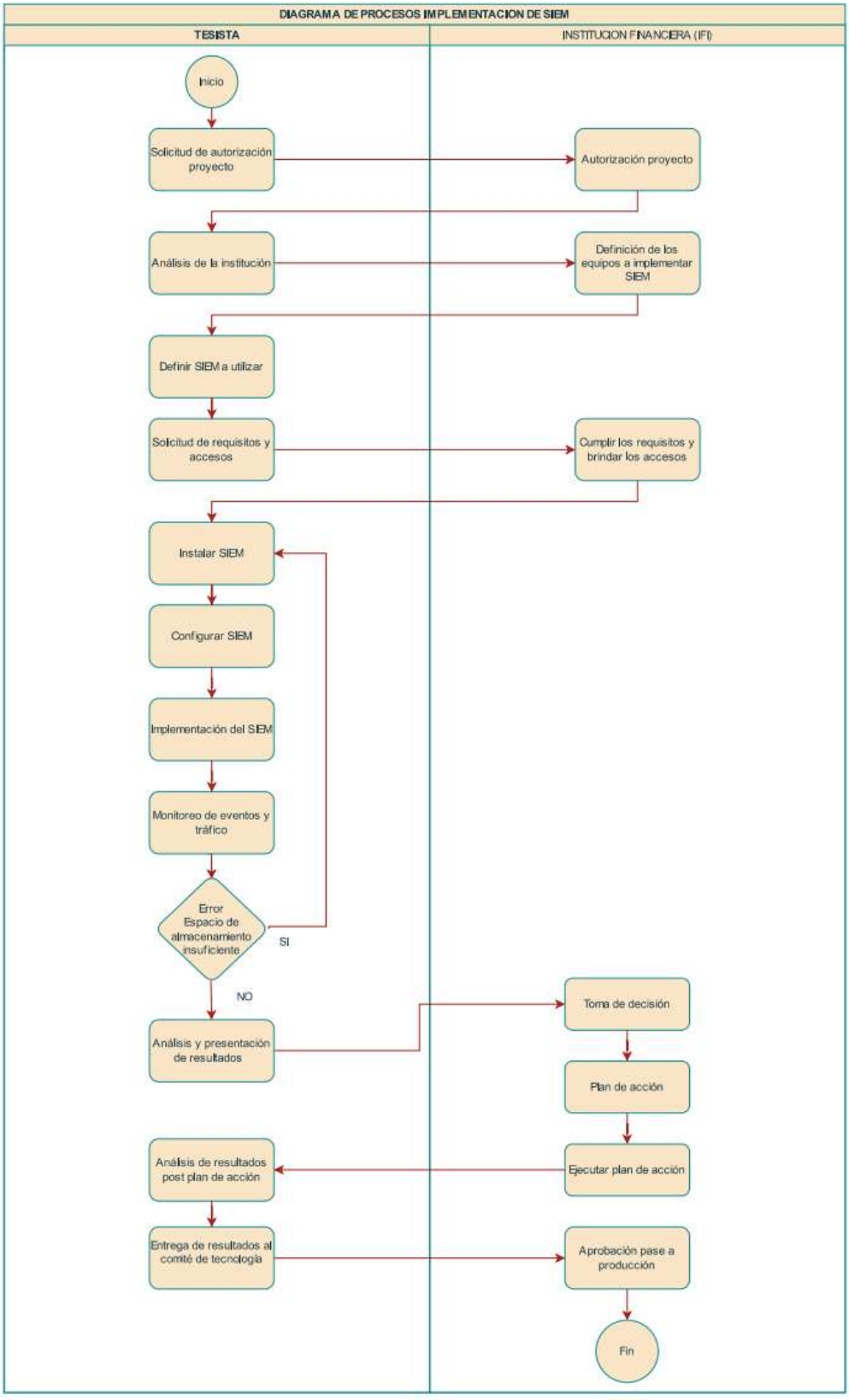


Ilustración 7 Procedimiento (Elaboración Propia)

3.2. Instalación SIEM Alien Vault OSSIM

Una vez seleccionado el sistema SIEM Alien Vault OSSIM se realiza la instalación paso a paso la cual va desde la selección de la imagen ISO hasta la pantalla inicial de login la cual podemos apreciar con más detalle en el (Anexo 3)

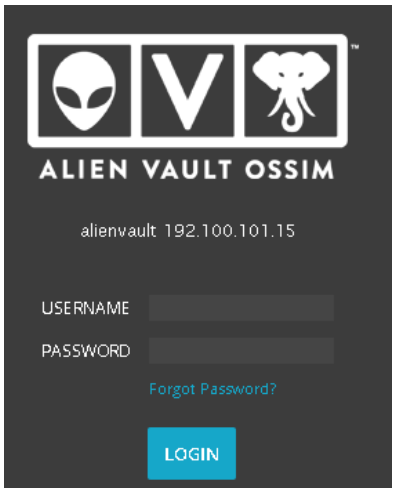


Ilustración 8 Configuración OSSIM Alien Vault - Pantalla Login (Elaboración Propia)

3.3. Configuración SIEM Alien Vault OSSIM

Al ingresar a la interfaz web de OSSIM AlienVault, se despliega una ventana de bienvenida para iniciar la configuración del servidor.

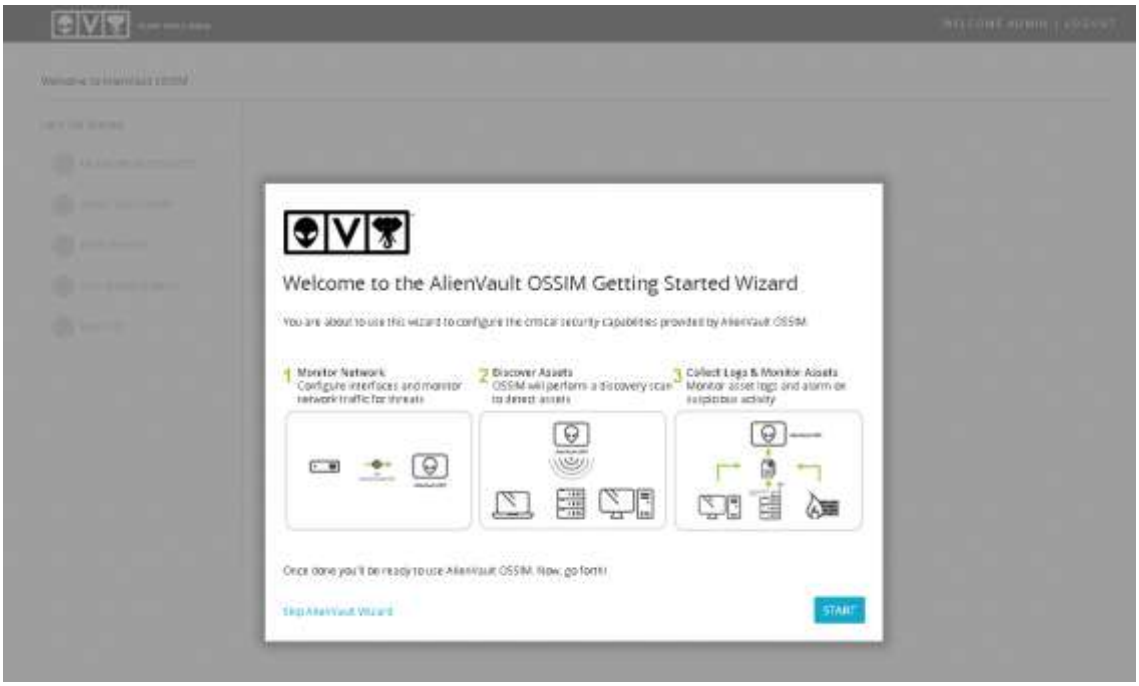


Ilustración 9 Configuración OSSIM AlienVault-Pantalla inicial de primeros pasos (Elaboración Propia)

Se muestra el asistente de configuración, se especifica las interfaces de red para su administración, recolección de log y escaneo.

Ilustración 10 Configuración OSSIM AlienVault - Configuración de interfaces de red (Elaboración Propia)

3.4. Implementación SIEM Alien Vault OSSIM

3.4.1 Equipos Windows

Se agrega los hosts que se va a implementar tanto en Windows como Linux

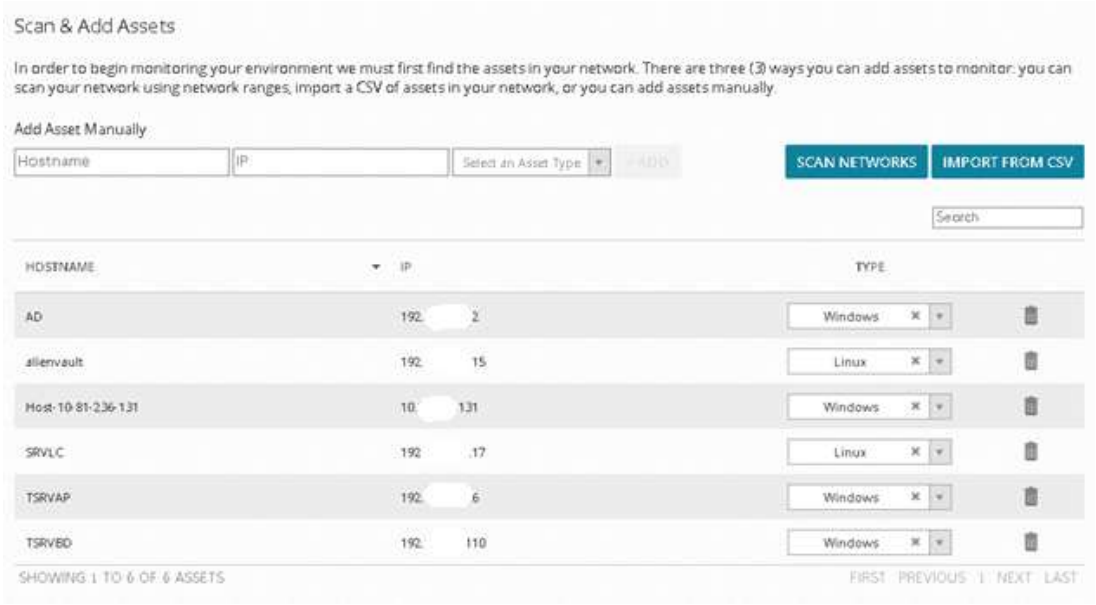


Ilustración 11 Configuración OSSIM AlienVault- Selección de hosts (Elaboración Propia)

Se agrega las credenciales para el despliegue del agente HIDS en los distintos servidores Windows.

Ilustración 12 Configuración OSSIM AlienVault - Ingreso de credenciales hosts windows (Elaboración Propia)

Se despliega automáticamente el agente en los 3 hosts seleccionados.

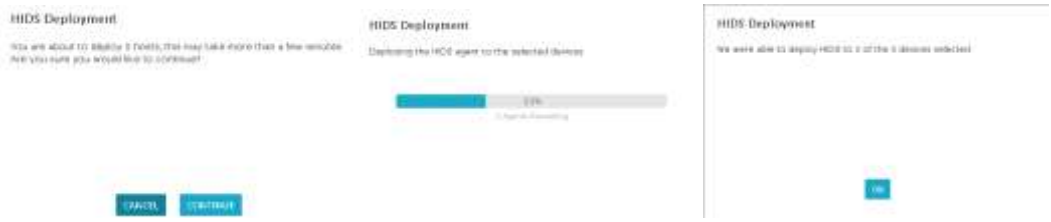


Ilustración 13 Configuración OSSIM AlienVault-Despliegue agente HIDS windows (Elaboración Propia)

3.4.2 Equipos Linux

Se realiza el mismo procedimiento para el servidor Linux especificando usuario y contraseña para el despliegue automático.

Ilustración 14 Configuración OSSIM AlienVault-Credenciales host Linux (Elaboración Propia)

Para la configuración del OTX, es necesario el registro de una cuenta que permitirá la integración del sistema detección de amenazas

Ilustración 15 Configuración OSSIM AlienVault-Configuracion de OTX (Elaboración Propia)

Al culminar el proceso de configuración, se muestra un mensaje de finalización de registro para intercambio

Ilustración 16 Configuración OSSIM AlienVault-Pantalla finalización asistente de despliegue (Elaboración Propia)

Se carga la interfaz web con los diferentes módulos de configuración.

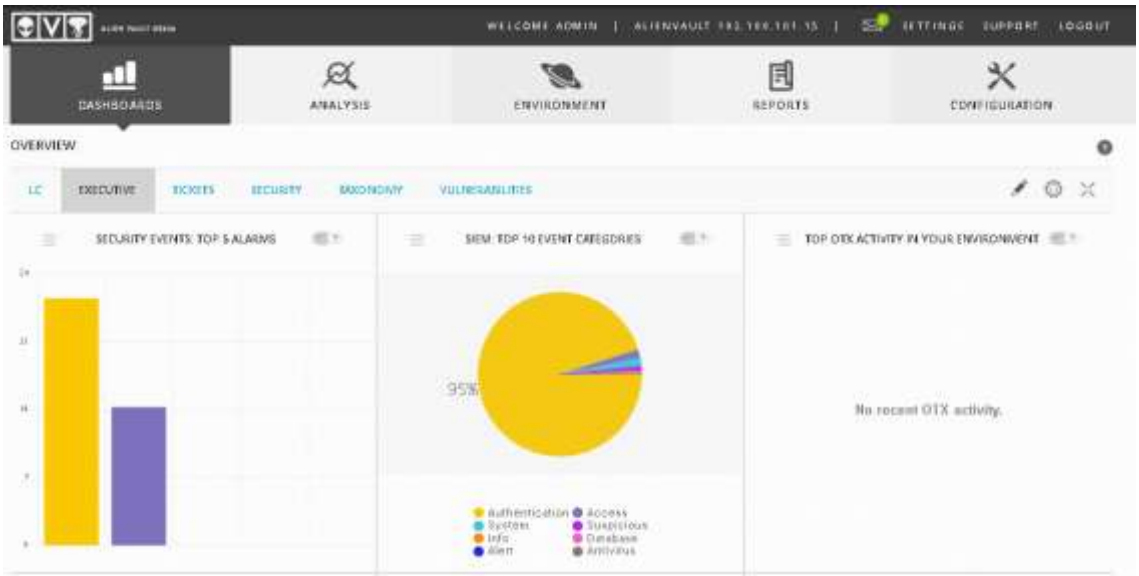


Ilustración 17 Configuración OSSIM AlienVault- Dashboard inicial (Elaboración Propia)

Se visualiza el estado del sistema y sus distintas configuraciones, el tiempo en línea, el uso de memoria, y almacenamiento, las interfaces habilitadas y demás estadísticas proporcionadas por la herramienta.

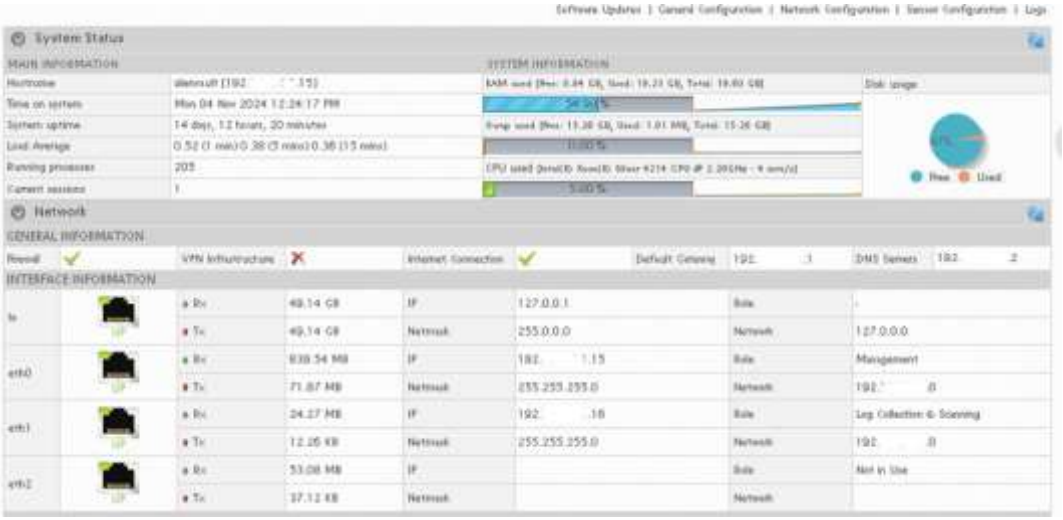


Ilustración 18 Configuración OSSIM AlienVault - Estado general del servidor (Elaboración Propia)

Se captura la recolección de un evento de seguridad en donde se ejecutó un comando en el host alienvault, así mismo le asigna el tipo, prioridad, y riesgo.

Ilustración 19 Configuración OSSIM AlienVault - Evento detectado (Elaboración Propia)

En la figura se observa el grafico de estadísticas de eventos a nivel de host HIDS (Sistema Detector de Intrusos Host) donde se agrupa eventos de autenticación y syslogs.

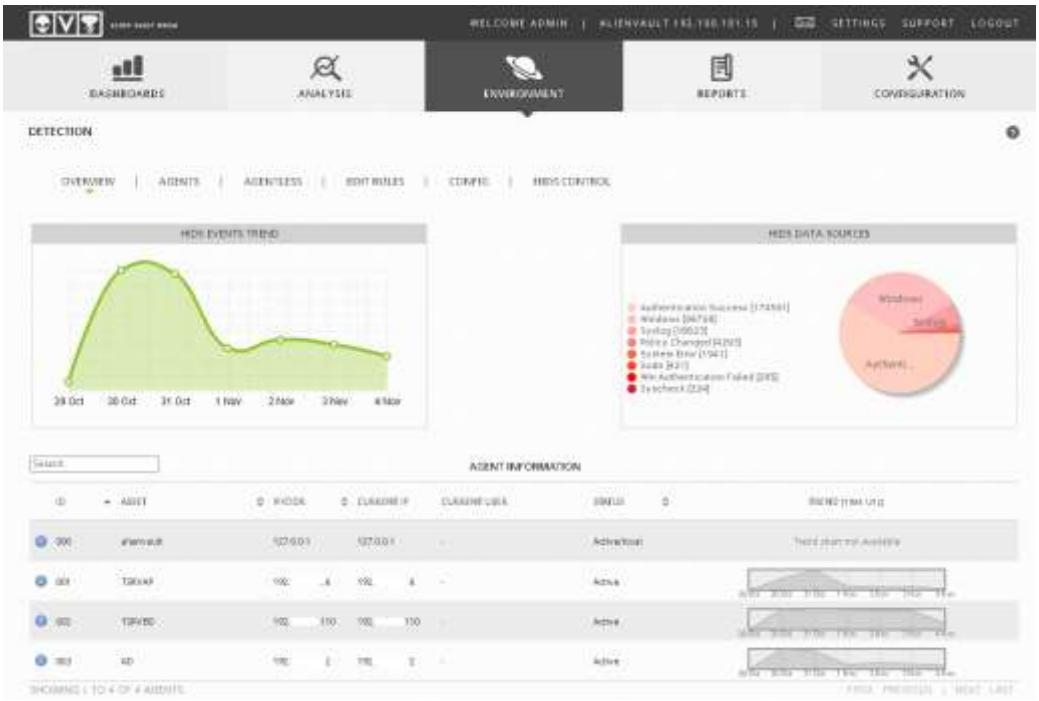


Ilustración 20 Configuración OSSIM AlienVault - Eventos capturados por el HIDS (Elaboración Propia)

En la ilustración 38 se muestra el monitoreo del tráfico de red nos permite observar el comportamiento de un host o una red, así como el tráfico generado de entrada y salida, así como los protocolos más usados en un rango de tiempo.

Ilustración 21 Configuración OSSIM AlienVault - Estadísticas Netflow (Elaboración Propia)

3.4.3. Sophos Central

Se realiza la instalación y configuración del sistema base del colector para los eventos producidos por Sophos Central.

```
root@srvclt:/home/etenezaca# uname -a
Linux srvclt 6.8.0-45-generic #45-Ubuntu SMP PREEMPT_DYNAMIC Fri Aug 30 12:02:04 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
```

Ilustración 22 Configuración Colector - Sistema Operativo (Elaboración Propia)

Se descarga el proyecto de github para la integración de Sophos Central con el SIEM con el comando wget.

```
root@srvclt:/home/etenezaca# wget https://github.com/sophos/Sophos-Central-SIEM-Integration/archive/refs/heads/master.zip
```

Ilustración 23 Configuración Colector - Descarga proyecto Sophos-Central-SIEM-Integration(Elaboración Propia)

Se realiza las configuraciones como client_id, client_secret, tenant_id, IP a la que se reporta, formato del archivo cef y el nombre de archivo.

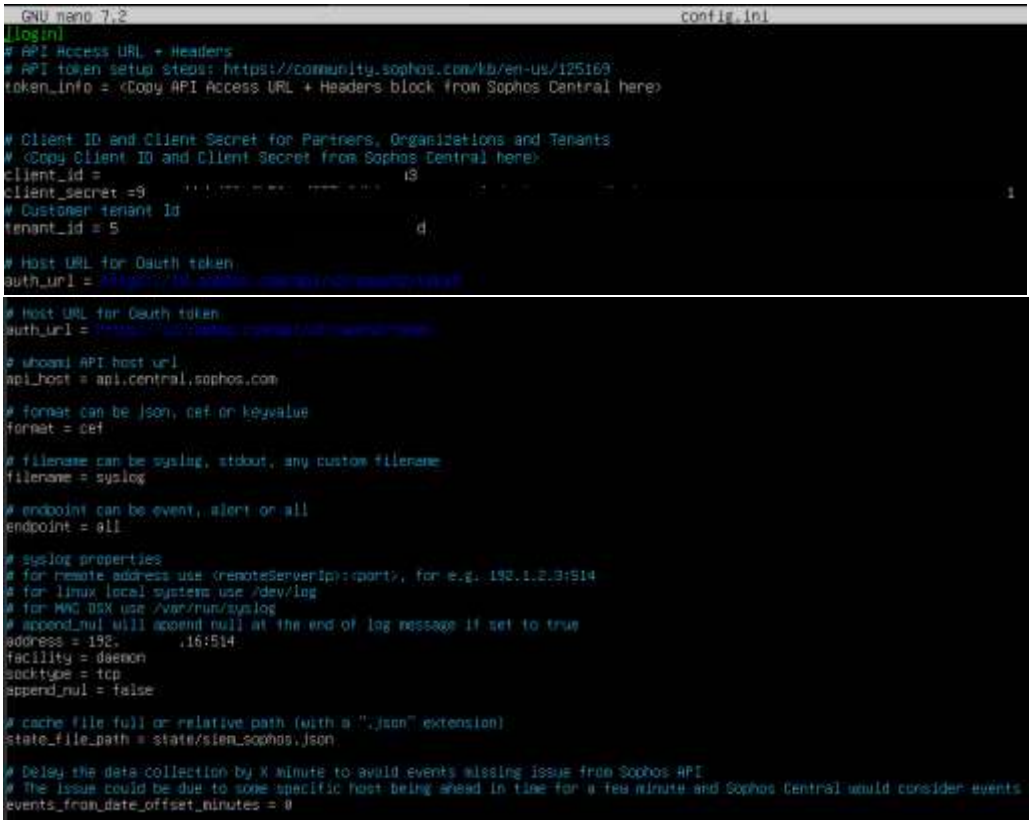


Ilustración 24 Configuración Colector - Configuración parámetros de conexión (Elaboración Propia)

Se verifica que los logs generados se envían correctamente hacia el receptor en el servidor OSSIM AlienVault.

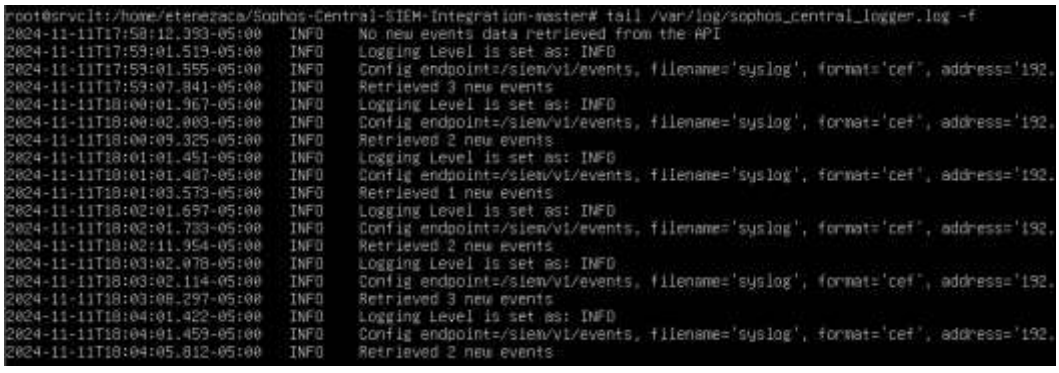


Ilustración 25 Configuración Colector -Revisión de envío de logs (Elaboración Propia)

Se configura el cron para que se ejecute cada minuto obteniendo nuevos eventos.

Ilustración 26 Configuración Colector - Configuración de Cron (Elaboración Propia)

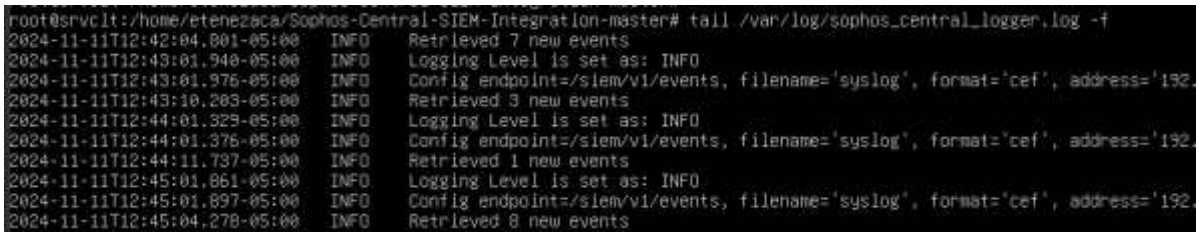


Ilustración 27 Configuración Colector - Revisión de logs de conexión (Elaboración Propia)

Se configura el Colector con el plugin adecuado para Sophos Central

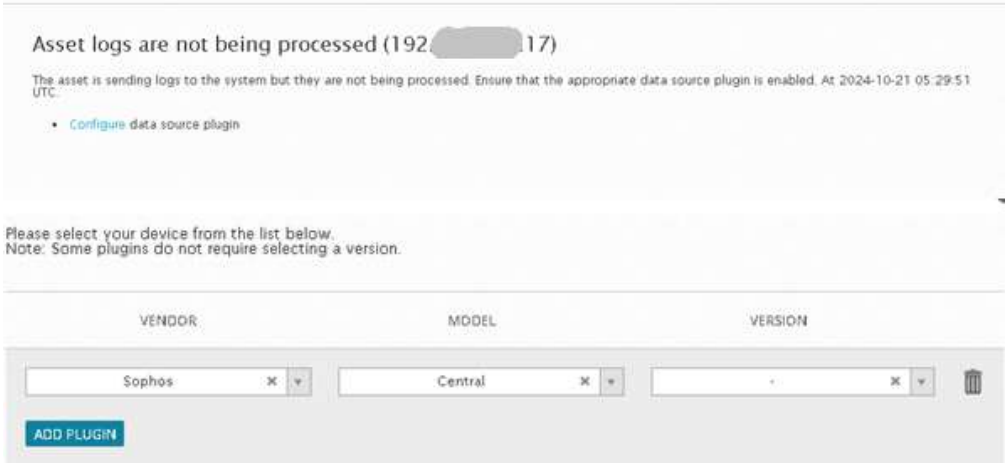


Ilustración 28 Configuración Plugin - Sophos Central (Elaboración Propia)

3.4.4. Equipos Red

Se realiza la configuración del switch Aruba para que envíe los eventos a la interfaz syslog.

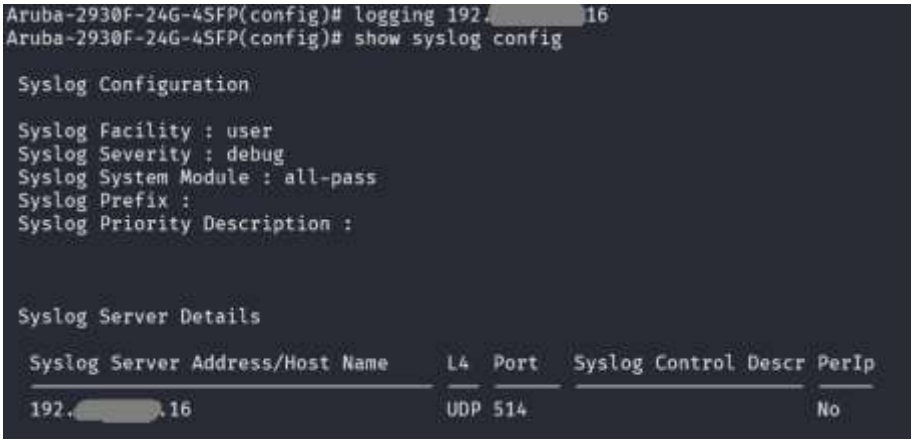


Ilustración 29 Configuración Switch - Configuración syslog (Elaboración Propia)

Se verifica que se envían los logs hacia el servidor OSSIM AlienVault.

Ilustración 30 Configuración Switch - Estadísticas logs enviados (Elaboración Propia)

3.5. Implementación de Políticas

3.5.1 Cuentas Habilitadas

Se realiza la configuración de data sources para la detección de cuentas habilitadas y deshabilitadas para ello se realizan las siguientes configuraciones.

Ilustración 31 Configuración Data Source - Cuentas Habilitadas (Elaboración Propia)

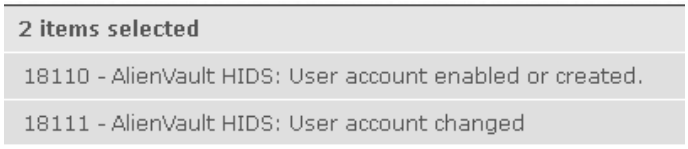


Ilustración 32 Configuración Data Source - Eventos Cuentas Habilitadas (Elaboración Propia)

Se realiza la configuración de la directiva para cuenta habilitada y para cuenta deshabilitada.

Ilustración 33 Configuración Directiva - Cuentas Habilitadas I (Elaboración Propia)

Ilustración 34 Configuración Directiva - Cuentas Habilitadas II (Elaboración Propia)

Finalmente se realiza la creación de la política.

Ilustración 35 Configuración Política - Cuentas Habilitadas (Elaboración Propia)

Se verifica que al darse el evento se envía el correo de notificación.

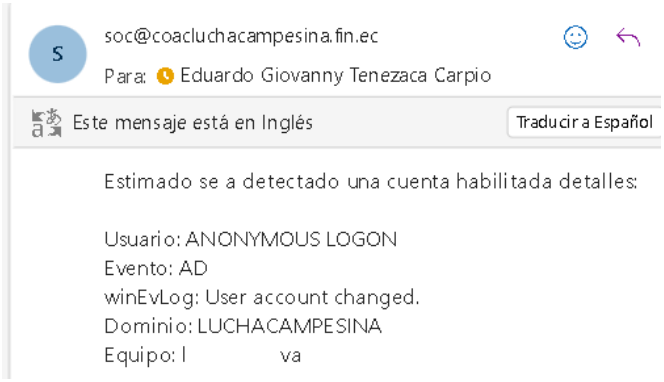


Ilustración 36 Configuración Envío Email - Cuentas Habilitadas (Elaboración Propia)

3.5.2 Cuenta Deshabilitada

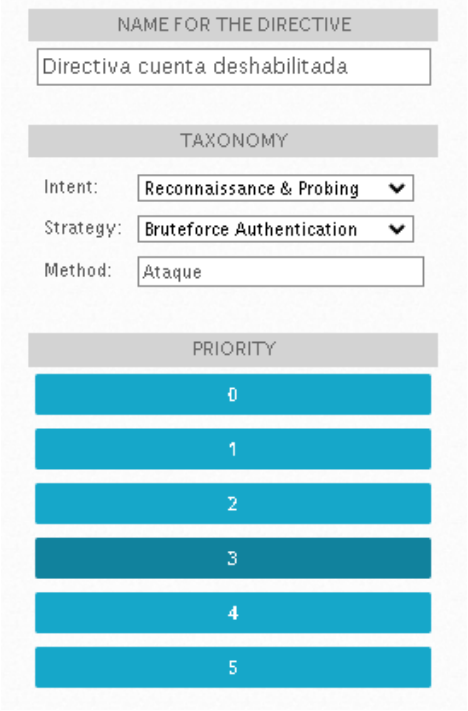


Ilustración 37 Configuración Directiva - Cuentas Deshabilitadas (Elaboración Propia)

Ilustración 38 Configuración Directiva - Cuentas Deshabilitadas II (Elaboración Propia)

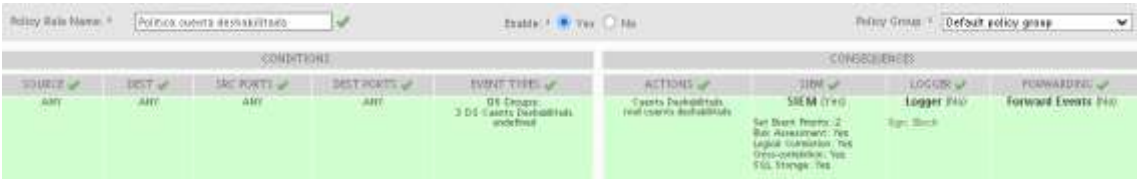


Ilustración 39 Configuración Política - Cuentas Deshabilitadas (Elaboración Propia)

Se verifica que al cumplirse la condición llega el mail de notificación.

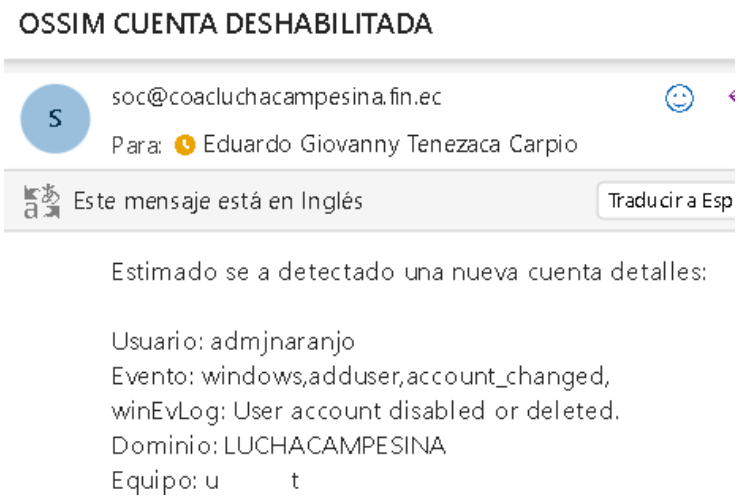


Ilustración 40 Configuración Envío Email - Cuentas Deshabilitadas (Elaboración Propia)

3.6. Monitoreo de eventos y tráfico

Se habilita el monitoreo en todos los activos agregados.

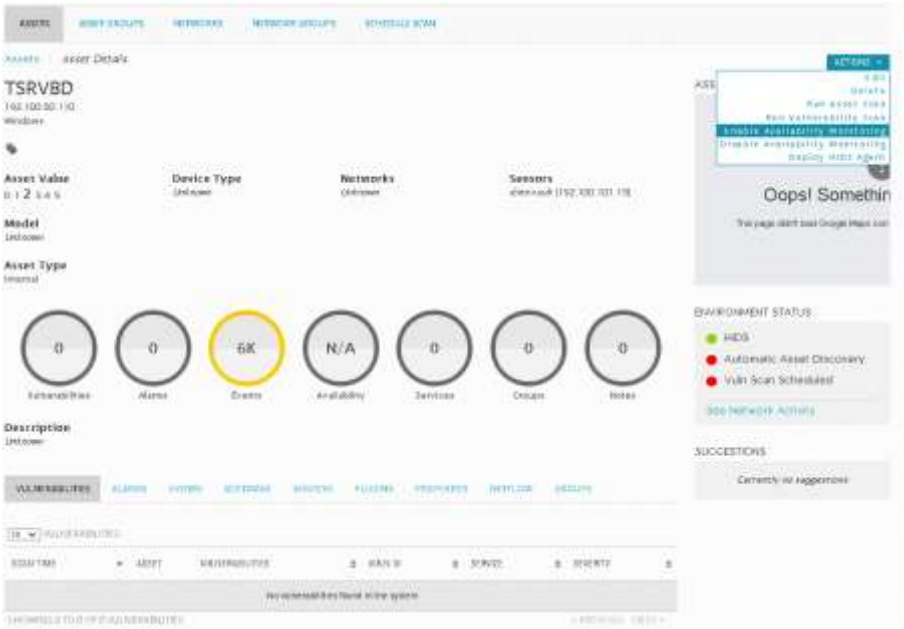


Ilustración 41 Configuración Monitoreo – Hosts (Elaboración Propia)

Se agrega los servicios para monitoreo

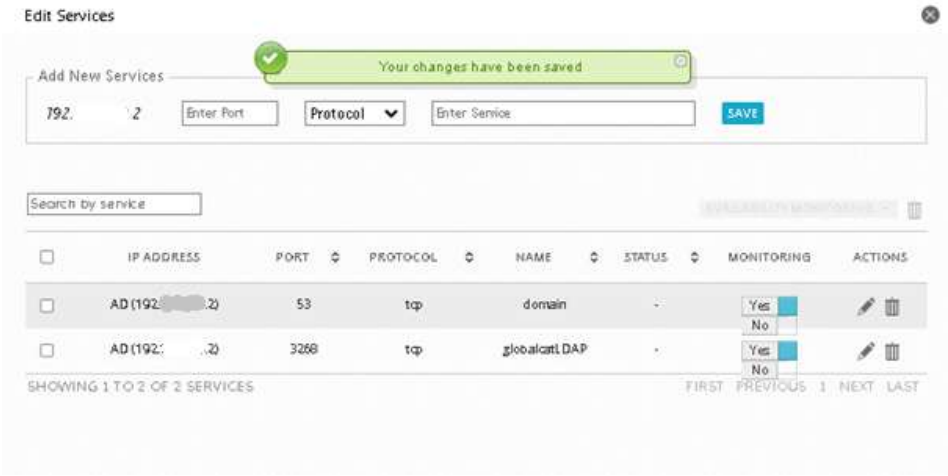


Ilustración 42 Configuración Monitoreo – Servicios (Elaboración Propia)

Se realiza la configuración del Netflow para recopilar información sobre el tráfico de red, protocolos y puertos usados.

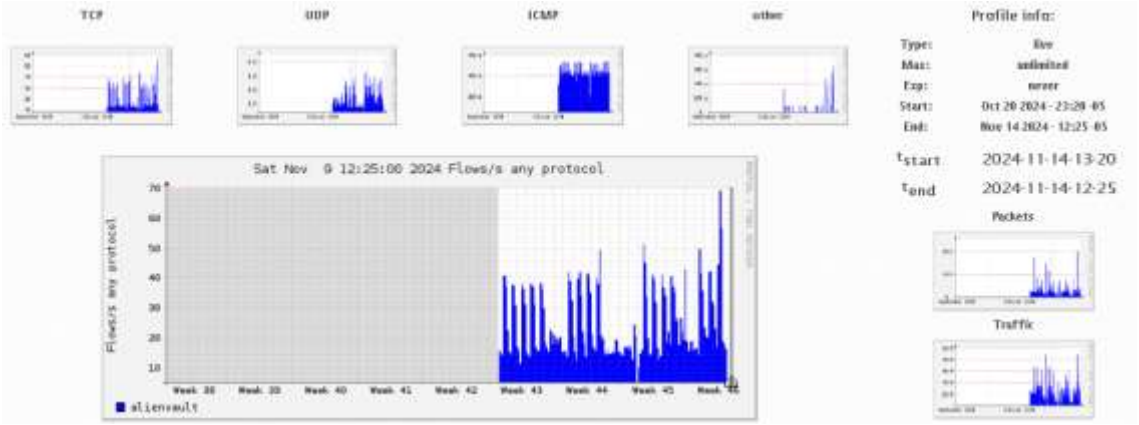


Ilustración 43 Configuración Netflow – Firewall (Elaboración Propia)

3.7. Análisis del estado actual

Al conjunto de eventos proporcionados por la herramienta AlienVault OSSIM, se verifica un total de 727906 eventos de múltiples datasources.

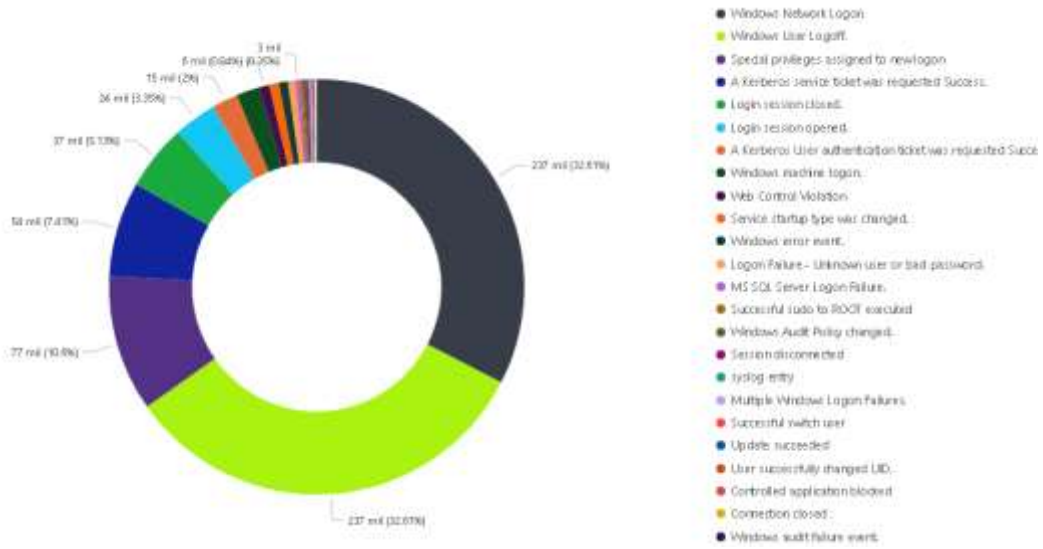


Ilustración 44 Data Sources por tipos de eventos (Elaboración Propia)

Evento	Total #	Unique Dst #	Unique Src #
"ET INFO WinHttp AutoProxy Request wpad.dat Possible BadTunnel"	24	3	1
A Kerberos service ticket was requested Success.	53920	1	194
A Kerberos User authentication ticket was requested Success.	14566	1	192
All Sophos services are running	1	1	1
Central management has been resumed	3	1	2
Central management has been suspended	3	1	2
Connection closed	271	1	1
Controlled application blocked	282	1	113
Generic Event	2	1	2
Login session closed.	37327	1	1
Login session opened.	24350	1	1
Login sucessful Accepted password	1	1	1
Logon Failure - Unknown user or bad password.	4065	4	9
MS SQL Server Logon Failure.	2549	1	15
Multiple Windows error events.	172	3	3
Multiple Windows Logon Failures.	925	4	14
Real time protection disabled	1	1	1
Reboot required after software update	7	1	5
Registry Entry Added to the System	125	3	3
Scan completed	46	1	43
Server listening	4	1	2
Server terminated	2	1	1
Service startup type was changed.	5475	3	3
Session disconnected	1330	1	1
Session reconnected/disconnected to winstation.	91	2	5
Special privileges assigned to new logon	77190	3	3
Successful sudo to ROOT executed	1660	1	1
Successful switch user	686	1	1
syslog entry	1166	1	4
Update Failure	4	1	3
Update succeeded	422	1	147
User account locked out (multiple login errors).	39	2	1
User successfully changed UID.	307	1	1
Web Control Violation	6118	1	176
Web server 400 error code.	173	1	4
Windows audit failure event.	178	4	2
Windows Audit Policy changed.	1532	1	1
Windows console logoff.	55	2	2
Windows Console Logon	75	3	3
Windows error event.	5093	3	3
Windows machine logon.	12907	3	3
Windows Network Logon	237361	3	203
Windows Successful Logon Unlock	38	3	5
Windows User Logoff.	237360	3	3

Ilustración 45 Lista de tipos de eventos (Elaboración Propia)

De la data analizada se verifica gran cantidad de eventos relacionados con inicio y cierre de sesión lo que demanda una alta actividad de usuarios en el sistema.

3.7.1. Revisión por data source Sophos-central.

Se verifica alto volumen de eventos “web control violation”, lo que sugiere actividad web no autorizada en endpoints, esto podría indicar intentos de acceso a sitios web bloqueados, descargas de archivos no permitidos, incluso actualización de servicios no permitidos.

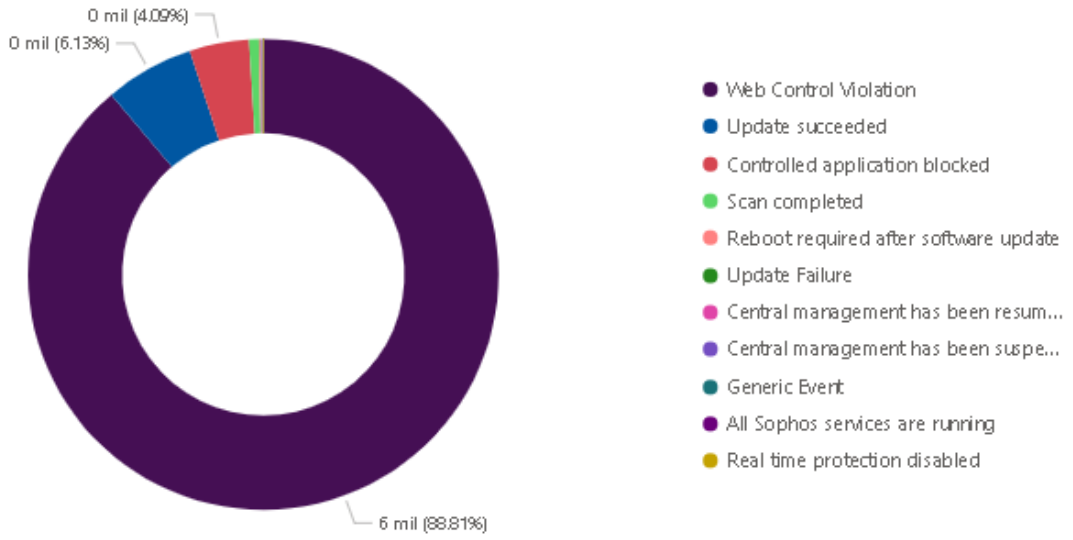


Ilustración 46 Data Sources Sophos Central por tipos de eventos (Elaboración Propia)

Evento	Total #	Unique Dst #	Unique Src #
All Sophos services are running	1	1	1
Central management has been resumed	3	1	2
Central management has been suspended	3	1	2
Controlled application blocked	282	1	113
Generic Event	2	1	2
Real time protection disabled	1	1	1
Reboot required after software update	7	1	5
Scan completed	46	1	43
Update Failure	4	1	3
Update succeeded	422	1	147
Web Control Violation	6118	1	176

Ilustración 47 Data Sources Sophos Central Lista de eventos (Elaboración Propia)

Para reducir significativamente los eventos de "Web Control Violation" se sugiere a la institución financiera establecer una política de uso de internet que incluya lineamientos claros sobre el acceso a sitios web, descargas, uso de dispositivos personales y prácticas de navegación segura

3.7.2. Revisión por data source AlienVault HIDS

Se visualiza eventos relacionados con inicios de sesión fallidos, (contraseñas incorrectas y usuarios desconocidos) de la investigación realizada se verifica que se debe a errores de usuarios, y al análisis de vulnerabilidades realizado.

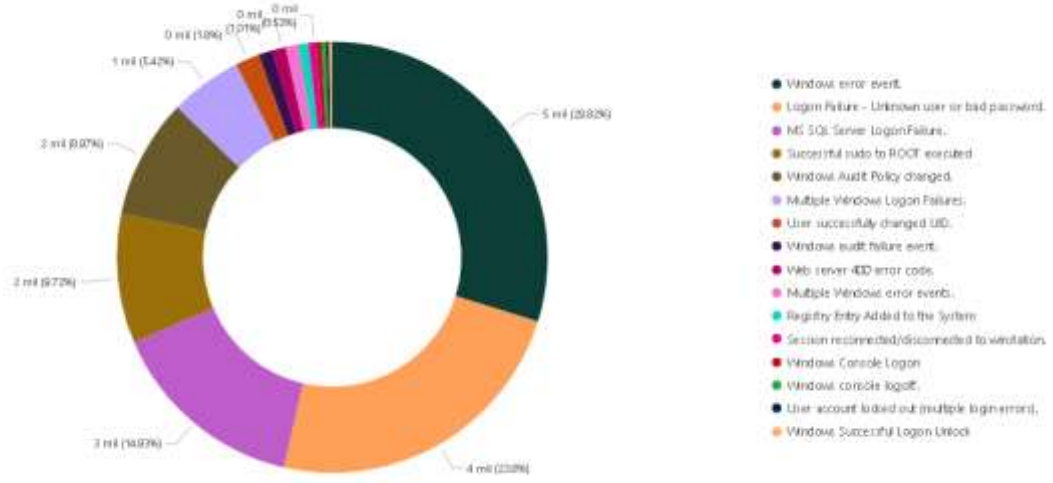


Ilustración 48 Data Sources AlienVault HIDS clasificado por tipos de eventos (Elaboración Propia)

Evento	Total #	Unique Dst #	Unique Src #
Windows Successful Logon Unlock	38	3	5
Windows error event.	5093	3	3
Windows Console Logon	75	3	3
Windows console logoff.	55	2	2
Windows Audit Policy changed.	1532	1	1
Windows audit failure event.	178	4	2
Web server 400 error code.	173	1	4
User successfully changed UID.	307	1	1
User account locked out (multiple login errors).	39	2	1
Successful sudo to ROOT executed	1660	1	1
Session reconnected/disconnected to winstation.	91	2	5
Registry Entry Added to the System	125	3	3
Multiple Windows Logon Failures.	925	4	14
Multiple Windows error events.	172	3	3
MS SQL Server Logon Failure.	2549	1	15
Logon Failure - Unknown user or bad password.	4065	4	9

Ilustración 49 Data Sources AlienVault HIDS - Lista de eventos (Elaboración Propia)

Eventos detectados como Falsos positivos después de la implementación de AlienVault OSSIM.

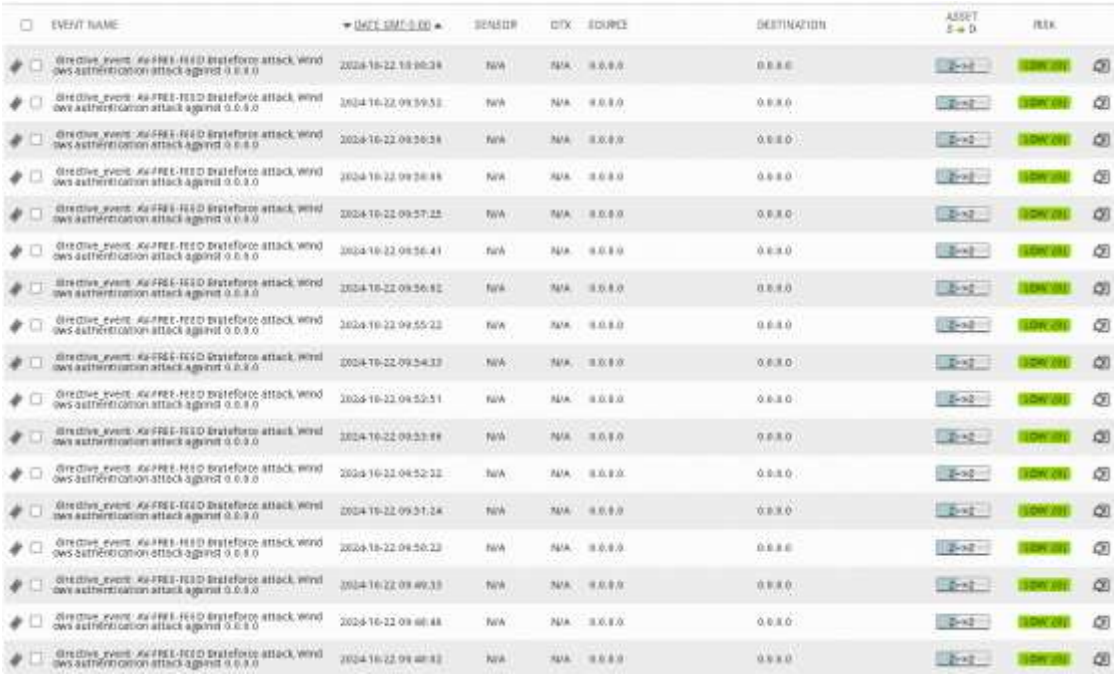


Ilustración 50 Eventos Generados - Falsos Positivos (Elaboración Propia)

Se revisa que la novedad se presenta por un servicio de reporting service mal configurado.

Ilustración 51 Eventos Generados – Servicio (Elaboración Propia)

Se desactiva el servicio, normalizando la novedad, luego de las acciones ya no se generan más alarmas

Ilustración 52 Eventos Generados – Alarmas Normalizadas (Elaboración Propia)

Se verifican las alarmas generadas por los intentos de autenticación y se cierran.

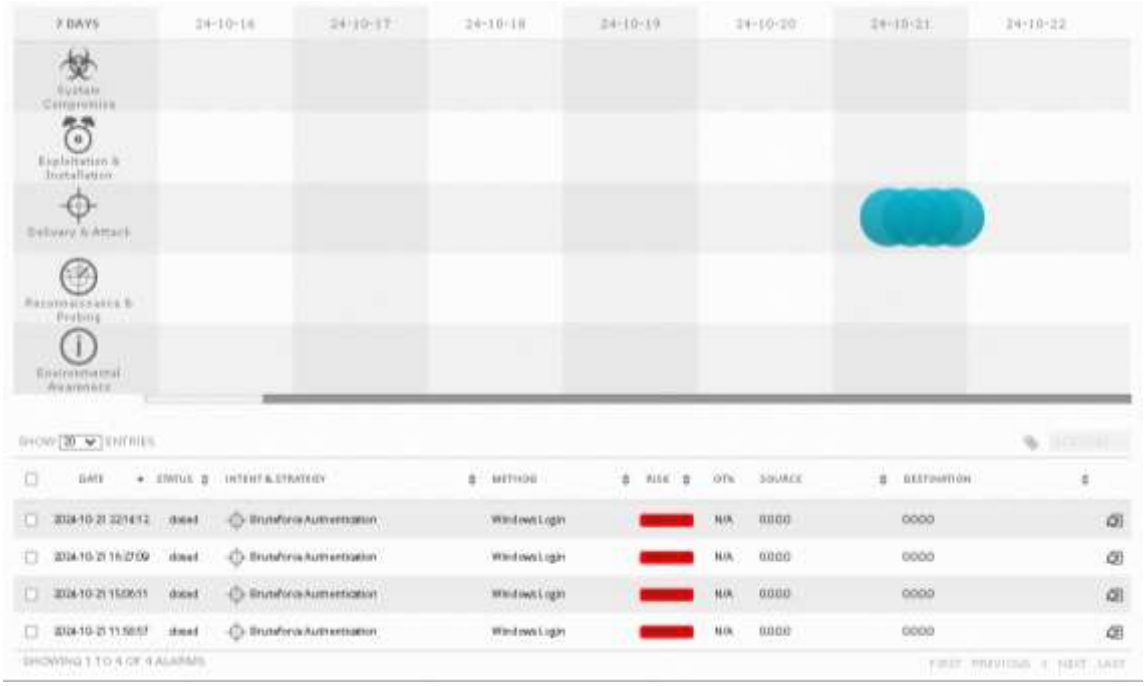


Ilustración 53 Eventos Generados - Alarmas Generadas (Elaboración Propia)

Para minimizar la generación de falsos positivos en la implementación de herramientas como Reporting Service, se sugiere a la institución financiera establecer una política o procedimiento formal de instalación de aplicaciones.

3.7.3. Top alarmas

Durante el periodo de monitoreo se visualiza que el sistema AlienVault OSSIM detectó las alertas relacionadas con intentos de ataques de fuerza bruta en autenticaciones Windows, SSH, lo que indica que los hosts estaban siendo sometidos a ataques automatizados donde se intentaba adivinar las contraseñas y un intento de infección de malware.

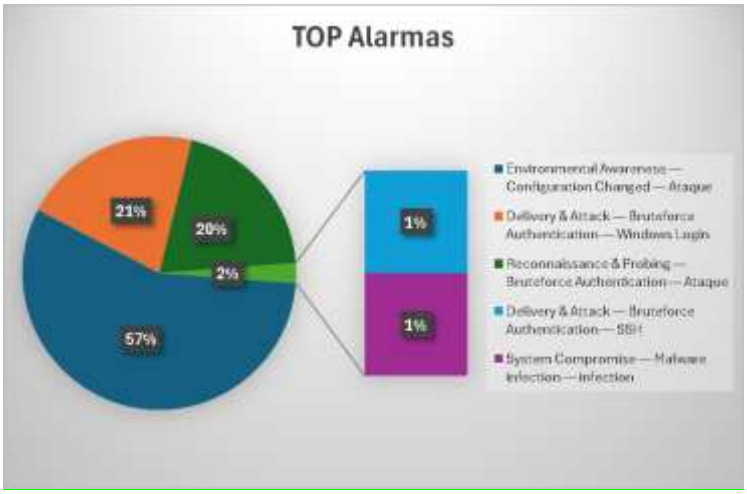


Ilustración 54 Alarmas - Tipos de Alarmas (Elaboración Propia)

TOP 10 ALARMS

ALARM	OCCURRENCES
Environmental Awareness — Configuration Changed — Ataque	47
Delivery & Attack — Bruteforce Authentication — Windows Login	18
Reconnaissance & Probing — Bruteforce Authentication — Ataque	17
Delivery & Attack — Bruteforce Authentication — SSH	1
System Compromise — Malware Infection — Infection	1

Ilustración 55 Alarmas - Lista de Alarmas (Elaboración Propia)

3.7.4. Tráfico generado Netflow

Durante el periodo de monitoreo se pudo observar que el consumo comprendido desde el 21de octubre hasta el 14 de noviembre de 2024, generó un tráfico total de 3.7 Tb, de los cuales 3.6 Tb es tráfico TCP, y 71.2Gb es UDP, 450.2 Mb de tráfico ICMP y 47.2 kb de otro tráfico.

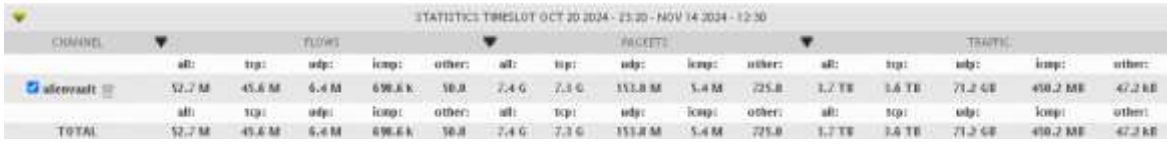


Ilustración 56 Netflow - Estadísticas desde 20/oct/2024 - 14/nov/2024 (Elaboración Propia)

Tráfico Total	
Protocolo	Cantidad
Todos	3.7 TB
TCP	3.6 TB
UDP	71.2 GB
ICMP	450.2 MB
OTROS	47.2 KB

Ilustración 57 Netflow - Lista de tipos de tráfico (Elaboración Propia)

A continuación, se detalla el Top 20 de origen con más tráfico, del análisis del top 20 de IP con más tráfico se puede apreciar que las x.x.x.201 concentran el mayor porcentaje del tráfico total, de lo conversado con el área de tecnología es tráfico normal generado por equipos de videovigilancia.

DATE FLOW SEEN GMT-5:00	DURATION	PROTO	IP ADDR	FLOWS(%)	PACKETS(%)	BYTES(%)	PPS	BPS	BPP
2024-10-20 17:07:26..000	2143471	any	x.x.2.201	210517(0.4)	463.2M(6.2)	522.9G(14.3)	216	2.0M	1128
2024-10-16 23:41:30..000	2465588	any	x.x.5.201	78129(0.1)	464.4M(6.2)	364.9G(10.0)	188	1.2M	785
2024-10-20 17:32:36..000	2142001	any	x.x.4.201	234597(0.4)	258.9M(3.5)	351.8G(9.6)	120	1.3M	1358
2024-10-20 23:33:16..000	2120475	any	x.x.3.201	1.3M(2.4)	326.4M(4.4)	175.5G(4.8)	153	661960	537
2024-10-18 14:25:00..000	2326170	any	x.x.50.190	768406(1.5)	281.4M(3.8)	150.0G(4.1)	120	515915	533
2024-10-21 00:04:02..000	2118629	any	x.x.6.201	406942(0.8)	238.3M(3.2)	118.0G(3.2)	112	445754	495
2024-10-19 19:02:51..000	2223124	any	x.x.9.201	854268(1.6)	251.5M(3.4)	115.6G(3.2)	113	416045	459
2024-10-20 17:17:12..000	2143047	any	x.x.10.201	1.0M(1.9)	183.5M(2.5)	109.2G(3.0)	85	407642	595
2024-10-20 20:05:43..000	2132944	any	x.x.4.202	786967(1.5)	99.2M(1.3)	96.1G(2.6)	46	360388	968
2024-10-19 19:20:24..000	2222047	any	x.x.7.201	815243(1.5)	189.1M(2.5)	86.9G(2.4)	85	312777	459
2024-10-21 00:03:59..000	2118632	any	x.x.8.201	779556(1.5)	145.7M(2.0)	76.4G(2.1)	68	288385	524
2024-10-20 20:08:45..000	2132762	any	x.x.100.211	834590(1.6)	128.4M(1.7)	62.4G(1.7)	60	234092	485
2024-10-20 20:09:03..000	2131547	any	x.x.6.202	320800(0.6)	59.9M(0.8)	61.6G(1.7)	28	231063	1027
2024-10-21 09:44:22..000	2035515	any	10.x.x.66	5.0M(9.4)	1.4G(18.7)	56.4G(1.5)	681	221478	40
2024-10-26 18:23:42..000	1572783	any	x.x.50.74	65995(0.1)	35.9M(0.5)	27.7G(0.8)	22	140728	771
2024-10-20 21:52:39..000	2117198	any	10.x.x.194	1.8M(3.4)	644.1M(8.7)	26.3G(0.7)	304	99386	40
2024-10-21 08:10:28..000	2089466	any	23.14.36.112	26862(0.1)	9.4M(0.1)	19.9G(0.5)	4	76086	2103
2024-10-21 00:03:43..000	2118247	any	8.243.200.75	17892(0.0)	11.2M(0.2)	19.5G(0.5)	5	73686	1738
2024-10-21 00:03:46..000	2118141	any	8.243.200.45	18082(0.0)	10.9M(0.1)	18.9G(0.5)	5	71556	1740
2024-10-20 23:39:11..000	2120143	any	192.229.211.108	433752(0.8)	12.8M(0.2)	18.9G(0.5)	6	71453	1482

Ilustración 58 Netflow - Top 20 Trafico (Elaboración Propia)

Se recomienda crear una subred exclusiva para las cámaras IP para aislarlas del resto de la red, se puede establecer políticas de acceso más granulares permitiendo que solo usuarios autorizados accedan a las cámaras.

3.7.5 Escaneo de vulnerabilidades

Se realiza el escaneo inicial de vulnerabilidades de los activos

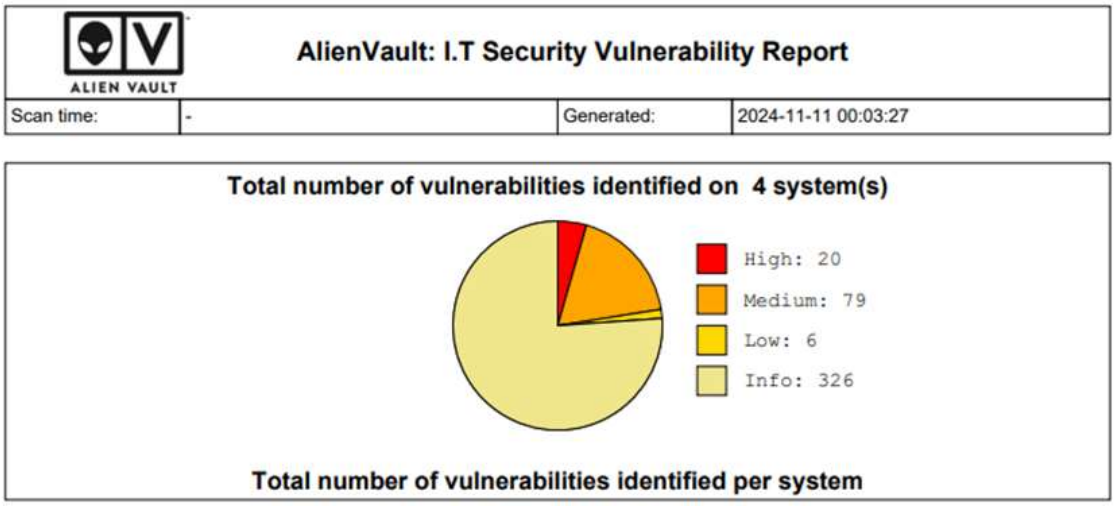


Ilustración 59 Análisis Vulnerabilidades - Estado Inicial (Elaboración Propia)

Se han detectado un total de 108 vulnerabilidades, 0 criticas, 20 altas, 80 medias, 8 bajas.

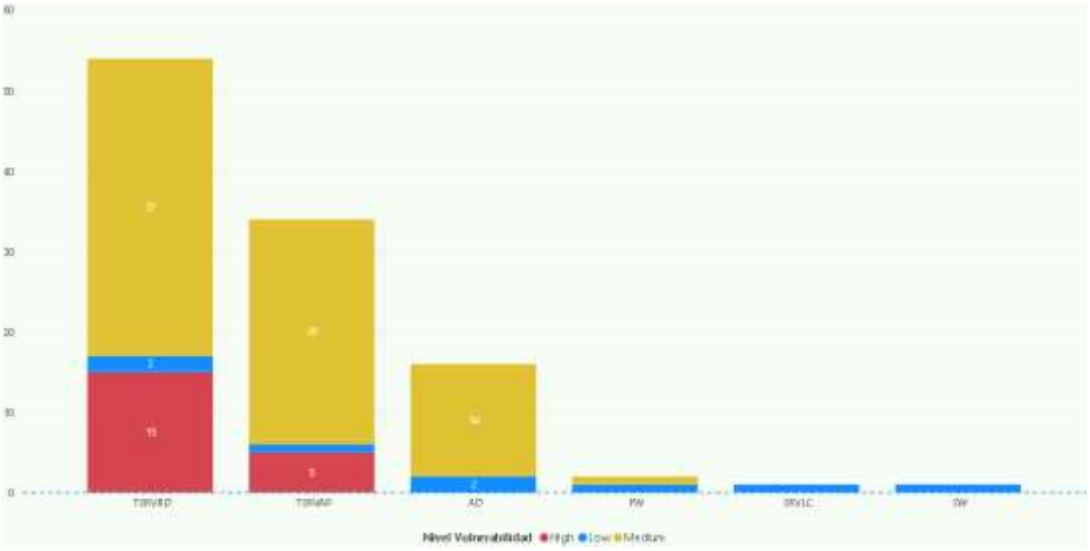


Ilustración 60 Análisis Vulnerabilidades - Vulnerabilidades Estado Inicial (Elaboración Propia)

Hostname	High	Low	Medium
TSRVBD	15	2	37
TSRVAP	5	1	28
AD		2	14
FW		1	1
SRVLC		1	
SW		1	

Ilustración 61 Análisis Vulnerabilidades – Vulnerabilidades Tabla (Elaboración Propia)

Se verifica que los host TSRVBD y TSRVAP presentan un número considerable de vulnerabilidades de riesgo alto y medio, esto sugiere que estos sistemas podrían ser objetivos prioritarios de ataques (ver Anexo 4).

3.7.6. Plan de acción.

Se revisa con el jefe de Tecnología y el Oficial de Seguridad de Información de la institución y se acuerda dar remediación inmediata en el presente proyecto piloto a las vulnerabilidades de riesgo alto (ver Anexo 5).

Para ello se identifica que las vulnerabilidades se deben a servicios desactualizados en estos ambientes, es por ello por lo que se trabaja en la actualización a la última versión disponible por fabricante.

3.7.7. Análisis Post Plan de Acción.

Se mitigaron el 40% del total de vulnerabilidades, de las 20 vulnerabilidades altas se mitigó el 100%, mientras que de las 80 vulnerabilidades medias se mitigó el 27.5% y de las 8 vulnerabilidades bajas se mitigó el 12.5 % (Ver Anexo 6).

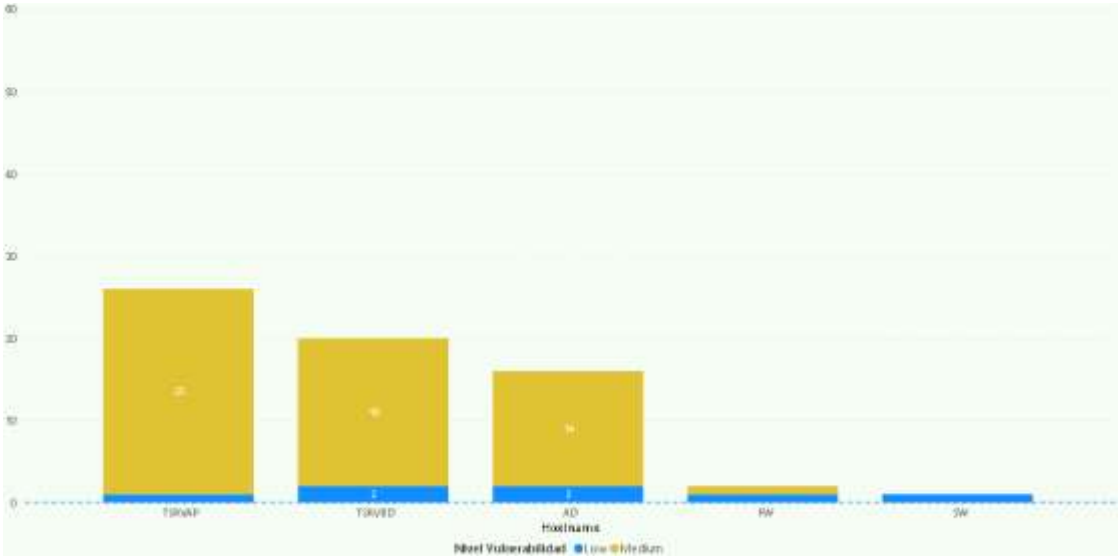


Ilustración 62 Vulnerabilidades - Post Plan de Acción (Elaboración Propia)

Hostname	Low	Medium
TSR\AP	1	25
TSR\BD	2	18
AD	2	14
FW	1	1
SW	1	

Ilustración 63 Lista de vulnerabilidades - Post Plan de Acción (Elaboración Propia)

3.7.8. Discusión

La presente investigación tenía como objetivo la implementación de un Sistema de Gestión de Eventos e Información (SIEM) en la Cooperativa Lucha Campesina Ltda., con el fin de mejorar la detección y respuesta a incidentes de seguridad. Los resultados de la presente investigación confirman la hipótesis propuesta: el uso de un SIEM mejora la detección y respuesta a incidentes de seguridad en una institución financiera, otorgando una herramienta robusta para la monitorización y análisis de la infraestructura tecnológica de la institución financiera.

Se detectaron varias vulnerabilidades críticas en el análisis del estado actual de la infraestructura las mismas que requerían atención inmediata es por ello qué se informó a la institución para realizar la respectiva mitigación. Estas vulnerabilidades no solo exponían a posibles riesgos de seguridad, sino que también limitaban su capacidad para responder a incidentes de manera eficaz. La evaluación de la solución SIEM demostró que con las características como la correlación de eventos más su capacidad de generación de alertas en tiempo real, se alineaban perfectamente con las necesidades identificadas en la fase inicial de la investigación.

Una vez implementado se observaron mejoras en la capacidad de detección de incidentes, así como en la rapidez de respuesta. Se concuerda con el autor Muñoz Álvarez que, el sistema OSSIM Alien Vault, durante el periodo de prueba se registraron múltiples eventos que fueron gestionados de manera más eficaz. Estos hechos están en concordancia con la literatura existente, que sugiere que la implementación y definición correcta de un SIEM puede transformar la postura de seguridad de una organización.

Es importante reconocer las limitaciones de este estudio. La implementación del SIEM estuvo sujeta a restricciones de tiempo y recursos, lo que podría haber afectado algunos de los resultados. En investigaciones futuras podrían enfocarse la integración de tecnologías emergentes en el campo de la ciberseguridad, además de la formación del personal en el manejo de esta herramienta.

En conclusión, la investigación respalda la hipótesis inicial que, la implementación de un SIEM mejora la detección y respuesta a incidentes de seguridad en una institución financiera, sino que también refuerza la importancia de un SIEM como una herramienta clave para mitigar vulnerabilidades en las instituciones financieras.

CONCLUSIONES

Se recomienda que las conclusiones deban ser redactadas en función de los objetivos tanto generales como específicos del trabajo de titulación.

- Una vez realizado el análisis de la infraestructura permitió agregar una herramienta para reforzar la gestión de seguridad, favoreciendo el monitoreo y detección de posibles anomalías en los diferentes servidores, equipos de comunicación y firewall, siendo capaz de incorporar la correlación de eventos en función del registro de logs.
- Los sistemas SIEM se han convertido en parte importante del sistema de defensa de una empresa para detectar un ataque y responder de forma inmediata. Las herramientas de código abierto satisfacen las necesidades de muchas organizaciones en crecimiento. Por ende, el Sistema SIEM AlienVault OSSIM presenta diversas ventajas de correlación y la documentación completa, analítica y comprensible, facilita su adopción por el usuario, siendo esta herramienta la más indicada para la implementación en la entidad financiera.
- La implementación de la solución SIEM combinado con el análisis de eventos y vulnerabilidades, ha fortalecido significativamente la postura de seguridad de la cooperativa. Por ende, la capacidad de correlacionar eventos y detectar anomalías en tiempo real nos ha permitido identificar, tomar decisiones y mitigar de manera proactiva las vulnerabilidades altas en un 100%, reduciendo significativamente el riesgo de incidentes cibernéticos.

RECOMENDACIONES

- La implementación del sistema de correlación de eventos e información (SIEM) nos da una visión holística de los activos (servidores) monitoreados, por ende, se recomienda agregar más equipos de la infraestructura tecnológica de la entidad financiera para que se realice un análisis global y así cubrir todos los equipos de la institución.
- Es aconsejable la asignación de personal al monitoreo de las alertas y tickets generados por la herramienta, así mismo, se exhorta a la capacitación continua del personal en el área de ciberseguridad y Linux para así aprovechar todas las funcionalidades de la herramienta AlienVault OSSIM.
- Se recomienda que, para publicar en ambiente de producción cualquier aplicativo, página web, servidor, equipo de red; realizar una evaluación de vulnerabilidades para determinar posibles brechas de seguridad. Mas aun, con esta implementación realizada en la entidad financiera, se podria implementar una política interna para que, antes de ser publicado cualquier sistema, deba ser analizado previamente por el SIEM, reduciendo eficazmente las vulnerabilidades.

REFERENCIAS

Admcloudservices. (2024). ¿Qué es el SEM? ¿qué es el SIM? y ¿qué es el SIEM? - ADM Cloud Services. *Https://Admcloudservices.Com/*. https://admcloudservices.com/sem-sim-siem/

Agualongo Domínguez, L. A. (2024). *DISEÑO DE UN SERVIDOR FIREWALL MEDIANTE USO DE HERRAMIENTAS OPEN SOURCE, PARA EL CENTRO DE SALUD SAN JOSÉ DE ANCÓN DE LA DIRECCIÓN DISTRITAL DE SALUD DE SANTA ELENA.* https://dspace.itb.edu.ec/handle/123456789/3400

Agudelo Castro, B. A., Álvarez Yépez, D. J., Andrade Valdez, J. A., Escobar Tucta, J. M., & Cortés López, A. (tutor). (2022). *Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft*. https://repositorio.uide.edu.ec/handle/37000/5610

Asamblea Nacional. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. www.lexis.com.ec

Baluja García, W., Caro Reina, C. C., & Cancio Bello, F. A. (2012). OSSIM, una alternativa para la integración de la gestión de seguridad en la red. *Telem@tica (La Habana)*, *11*(1), 11–19. http://revistatelematica.cujae.edu.cu/index.php/tele/article/view/12/7

CALERO ESPINOZA, K. J. (2024). *Los ataques informáticos y su incidencia en la seguridad de los servidores con sistemas operativos open source en la Universidad Técnica de Babahoyo*.

Castañeda Cobeñas, B., Luis Br Castro Venegas, J., Genaro, O., Gamboa, A., & David, E. (2023). *Hardening y patching para la Seguridad informática de la infraestructura de servidores de Profuturo*.

Check Point. (2024). *¿Qué es SIEM (Gestión de eventos e información de seguridad)? - Software Check Point*. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/

Choto Tuquerres, A. F. (2024). *Análisis informático forense en juegos de video en línea y sus implicaciones con delitos informáticos*. https://repositorio.puce.edu.ec/handle/123456789/41022

Danilo, W., Salguero, S., Manuel, J., Alfaro, M., Abraham, J., Corado, G., Alberto, C., Ramos, R., & Cotto Argueta, J. A. (2024). *Análisis cognitivo de la respuesta de estudiantes de la Universidad del Valle de Guatemala frente a ataques informáticos y sus respectivas medidas de protección para fortalecer la educación en seguridad informática*.

Estela Campos, M. A. (2020). Implementación de un security information and event management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera. *Universidad Tecnológica Del Perú*. http://repositorio.utp.edu.pe/handle/20.500.12867/3375

García Merino, J. (2018). *Ventajas e implementación de un sistema SIEM*. https://openaccess.uoc.edu/handle/10609/81425

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors 2021, Vol. 21, Page 4759*, *21*(14), 4759. https://doi.org/10.3390/S21144759

Harper, A., VanDyke, S., Blask, C., Harris, S., & Miller, D. (2010). *Security Information and Event Management (SIEM) Implementation*. McGraw-Hill Osborne Media. https://doi.org/10.1036/9780071701082

IBM. (2024). *¿Qué es SIEM? | IBM*. https://www.ibm.com/es-es/topics/siem

Incibe. (2017). *Diseño y Configuración de IPS, IDS y SIEM en Sistemas de Control Industrial*. http://www.incibe.es.

Kaspersky. (2023, August). *Panorama en América Latina 2023 | Blog oficial de Kaspersky*. https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/?srsltid=AfmBOorUZPNrpGCS-mFdvIn4vQo7OZtgHw-3SDKFTK-I6E-tWm92TBfO

Kevin Bryan Costa Castillo. (2024). *IMPLEMENTACIÓN DE UN SIEM PARA LA DEFENSA ACTIVA ANTE INTRUSIONES EN LA RED*.

Konstantinos Bezas, & Foteini Filippidou. (2023). *Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)*. http://ijcs.net/ijcs/index.php/ijcs/article/view/3182/118

LogRhythm. (2024). *Aprende que es SIEM y cómo funciona | LogRhythm*. https://logrhythm.com/blog/que-es-siem-y-como-funciona/

Lucha Campesina. (2024). *Lucha Campesina*. https://luchacampesina.fin.ec/

Luis Ramírez Quevedo. (2024). *Tecnologías de defensa frente a inteligencia de amenazas y ciberataques*. https://revistas.itecsur.edu.ec/index.php/inndev/article/view/94/66

Luján Flores, T. L., & Huancas Samillán, V. E. (2023). *Gestión de la Seguridad de la Información de la Infraestructura de Red Datos de la Minera Shahuindo Mediante Ossim y Cobit*. http://repositorio.unprg.edu.pe/handle/20.500.12893/12543

Manuel Madrid, J., Eduardo, L., & Eduardo Múnera Salazar, L. (2015). *Implementación y mejora de la consola de seguridad informática OSSIM en el entorno colombiano*. https://www.researchgate.net/publication/242593393

Microsoft Learn Challenge. (2024). *Descripción de la normalización de la base de datos - Microsoft 365 Apps | Microsoft Learn*. https://learn.microsoft.com/es-es/office/troubleshoot/access/database-normalization-description

Morales Morera Randy. (2020). *Casos de uso resilientes SIEM*.

Muñoz Alvarez, L. A. D. (2022). *Implementación de un gestor de información y eventos de seguridad (SIEM) para la prevención y detección de ciber amenazas en una entidad gubernamental*. http://localhost:8080/xmlui/handle/123456789/4865

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología*, *74*(9), 790–799. https://doi.org/10.1136/bmj.n71

Piñón, L. C., Sapién, A. L., Gutiérrez, M. del C., Piñón, L. C., Sapién, A. L., & Gutiérrez, M. del C. (2023). Capacitación en ciberseguridad en una empresa mexicana. *Información Tecnológica*, *34*(6), 43–52. https://doi.org/10.4067/S0718-07642023000600043

Puchades Olmos. Adrián, & Peñalver Herrero, L. (2008). *Sistema de gestión de la información Open Source*.

Red Hat. (2023). *Gestión de la información y los eventos de seguridad (SIEM)*. https://www.redhat.com/es/topics/security/what-is-SIEM

Reddy Turpu, R. (2021). ENHANCING CLOUD SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) FOR BANKS. In *Article in INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY AND MANAGEMENT INFORMATION SYSTEMS*. https://iaeme.com/Home/journal/IJITMIS

Revista IT ahora. (2024, June 24). *Ciberseguridad financiera: Protegiendo el futuro de la banca ecuatoriana – IT ahora*. https://itahora.com/2024/06/04/ciberseguridad-financiera-protegiendo-el-futuro-de-la-banca-ecuatoriana/

Ruiz Sala, F. (2024). *Caracterización de un Firewall Perimetral implementado mediante software libre OpenBSD y CentOS MAESTRO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN*.

Sesmero, J. (2023). ¡Cómo resolver el dilema de talento en ciberseguridad en tu empresa! *Revista SIC: Ciberseguridad, Seguridad de La Información y Privacidad, ISSN 1136-0623, Vol. 32, Nº. 154 (Abril 2023), 2023 (Ejemplar Dedicado a: CISOs, La Encrucijada Regulatoria), Págs. 122-124*, *32*(154), 122–124. https://dialnet.unirioja.es/servlet/articulo?codigo=8912822&info=resumen&idioma=SPA

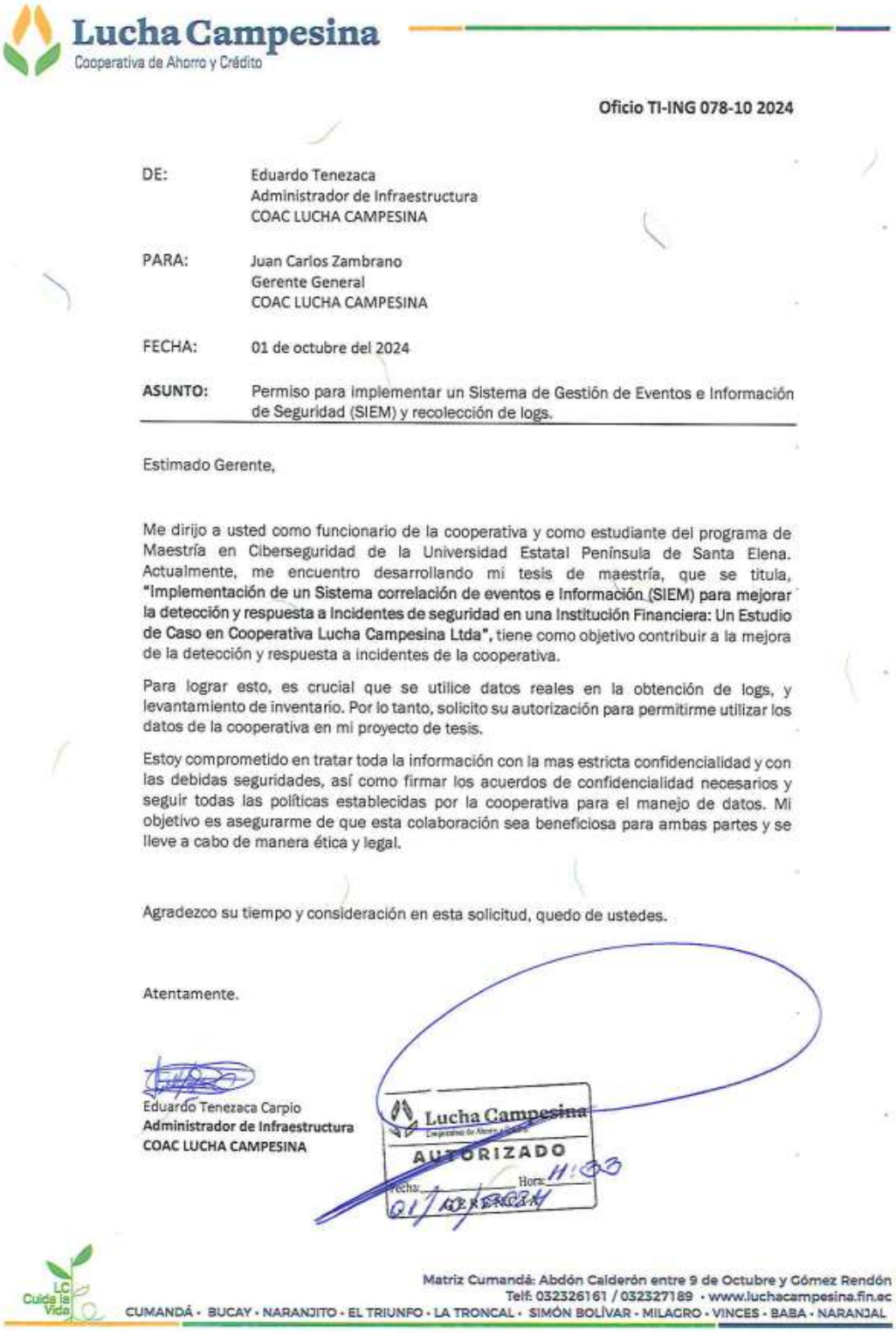
Stellar Cyber. (2024). *Registro SIEM: descripción general y mejores prácticas*. https://stellarcyber.ai/es/learn/siem-logging-overview-best-practices/

Superintendencia de Economía Popular y Solidaria. (2022). *SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002*. https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Susan Moore, & Gartner. (2022, April). *Las tendencias en ciberseguridad de Gartner para 2022*. https://www.gartner.es/es/articulos/las-7-principales-tendencias-en-ciberseguridad-para-2022

ANEXOS

Anexo 1: Autorización



Lucha Campesina
Cooperativa de Ahorro y Crédito

Oficio TI-ING 078-10 2024

DE: Eduardo Tenezaca
Administrador de Infraestructura
COAC LUCHA CAMPESINA

PARA: Juan Carlos Zambrano
Gerente General
COAC LUCHA CAMPESINA

FECHA: 01 de octubre del 2024

ASUNTO: Permiso para implementar un Sistema de Gestión de Eventos e Información de Seguridad (SIEM) y recolección de logs.

Estimado Gerente,

Me dirijo a usted como funcionario de la cooperativa y como estudiante del programa de Maestría en Ciberseguridad de la Universidad Estatal Península de Santa Elena. Actualmente, me encuentro desarrollando mi tesis de maestría, que se titula, **"Implementación de un Sistema correlación de eventos e Información (SIEM) para mejorar la detección y respuesta a Incidentes de seguridad en una Institución Financiera: Un Estudio de Caso en Cooperativa Lucha Campesina Ltda"**, tiene como objetivo contribuir a la mejora de la detección y respuesta a incidentes de la cooperativa.

Para lograr esto, es crucial que se utilice datos reales en la obtención de logs, y levantamiento de inventario. Por lo tanto, solicito su autorización para permitirme utilizar los datos de la cooperativa en mi proyecto de tesis.

Estoy comprometido en tratar toda la información con la mas estricta confidencialidad y con las debidas seguridades, así como firmar los acuerdos de confidencialidad necesarios y seguir todas las políticas establecidas por la cooperativa para el manejo de datos. Mi objetivo es asegurarme de que esta colaboración sea beneficiosa para ambas partes y se lleve a cabo de manera ética y legal.

Agradezco su tiempo y consideración en esta solicitud, quedo de ustedes.

Atentamente.

Eduardo Tenezaca Carpio
Administrador de Infraestructura
COAC LUCHA CAMPESINA

Lucha Campesina
AUTORIZADO
Fecha: 01/ OCTUBRE/24
Hora: 11:03

LC Cuida la Vida

Matriz Cumandá: Abdón Calderón entre 9 de Octubre y Gómez Rendón
Telf: 032326161 / 032327189 · www.luchacampesina.fin.ec
CUMANDÁ · BUCAY · NARANJITO · EL TRIUNFO · LA TRONCAL · SIMÓN BOLÍVAR · MILAGRO · VINCES · BABA · NARANJAL

Ilustración 64 Solicitud de implementación de proyecto SIEM (Elaboración Propia)

Anexo 2: Matriz de Consistencia

MATRIZ DE CONSISTENCIA									
CAUSA	PROBLEMA	**OBJETIVO GENERAL**	**HIPOTESIS**	**VARIABLE DEPENDIENTE**	**VARIABLE INDEPENDIENTE**	**INSTRUMENTO**	**PREGUNTA**	**TIPO DE VARIABLE**	**RESPONSIBLE**
La inexistencia de un siem Desconocimiento de los siem existentes	Dificultad para dar respuestas a incidentes	Analizar los SIEM, a través de métricas de seguridad para mejorar las respuestas a incidentes de seguridad en la institución	La inexistencia de un SIEM dificulta la respuesta a incidentes	Respuesta a incidentes	SIEM	Analisis de logs	Poseen unSIEM	Cuantitativa	OSI, TI, Equipos
		OBJETIVOS ESPECIFICOS							
Infraestructura no adecuadad	Dificultad para dar respuestas a incidentes	Analizar el estado actual de la infraestructura	como es la infraestructura que tiene la empresa	Respuesta a incidentes	Infraestructura	Ficha observacional	Como es la infraestructura de la empresa	Cuantitativa	Equipos
Desconocimiento de los SIEMs existentes	Dificultad para dar respuestas a incidentes	Evaluar las caracteristicas y funcionalidades de los SIEM	cuales son los SIEM en el mercado	Respuesta a incidentes	SIEM	software SIEM	Cuales son los SIEM en el mercado	Cuantitativa	Estudiante
Poco análisis de logs	Dificultad para dar respuestas a incidentes	Implementar el SIEM y analizar la informacion de correlacion de eventos y alarmas.	Cuales herramientas me permiten hacer deteccion de logs	Respuesta a incidentes	Logs	Registros	Cuantas veces en el mes se analiza los logs?	Cuantitativa	OSI, TI

Ilustración 65 Matriz de Consistencia (Elaboración Propia)

Anexo 3: Historial de implementación

Instalación SIEM (Alien Vault OSSIM)

Se agrega el ISO para el boot y continuar con la instalación.

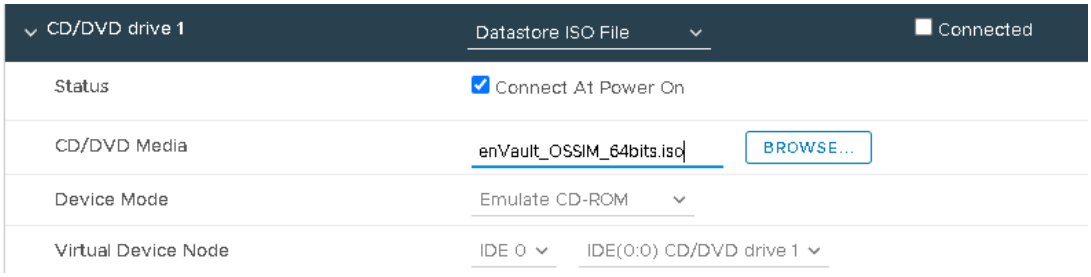


Ilustración 66 Configuración OSSIM AlienVault-Imagen ISO (Elaboración Propia)

Una vez encendida del servidor virtual lo primero que encontramos son dos opciones para instalar server OSSIM (Install AlienVault OSSIM 5.8.11 64 Bits) o un sensor (Install AlienVault Sensor 5.8.11 64 Bits), elegimos en nuestro caso instalar el OSSIM.

Ilustración 67 Configuración OSSIM AlienVault-Pantalla inicial (Elaboración Propia)

Después de la selección tenemos un apartado para elegir el idioma en nuestro caso el español

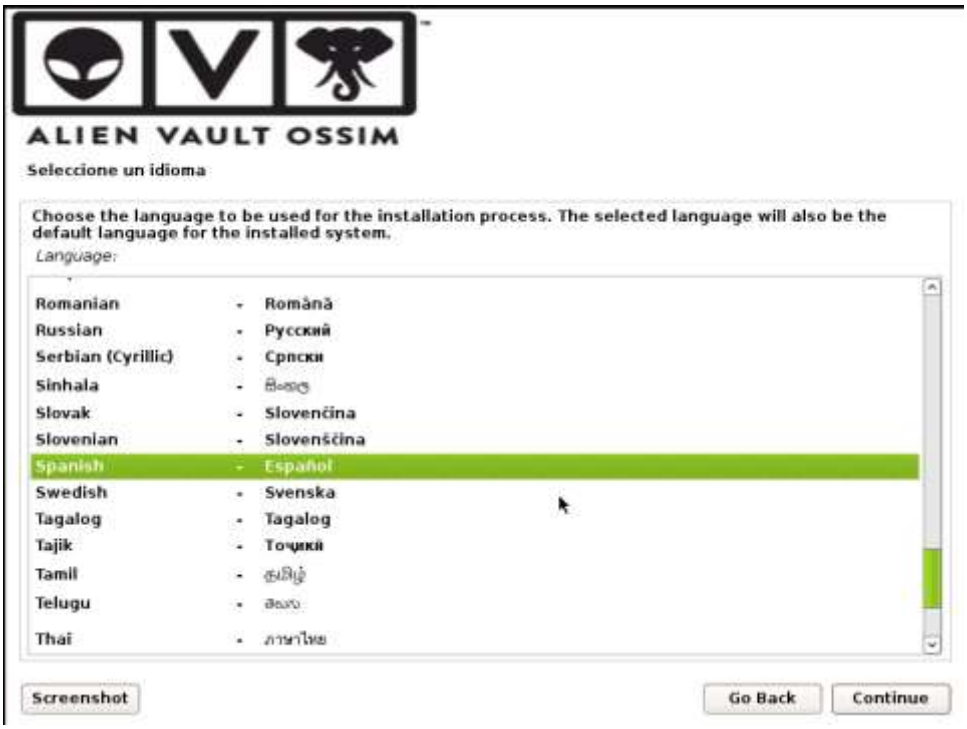


Ilustración 68 Configuración OSSIM AlienVault-Selección de Idioma (Elaboración Propia)

Se despliega la opción de elegir la ubicación en nuestro caso Ecuador.

Ilustración 69 Configuración OSSIM AlienVault-Selección de ubicación (Elaboración Propia)

Nos solicita que se configure la distribución del teclado en nuestro caso Ingles estadounidense

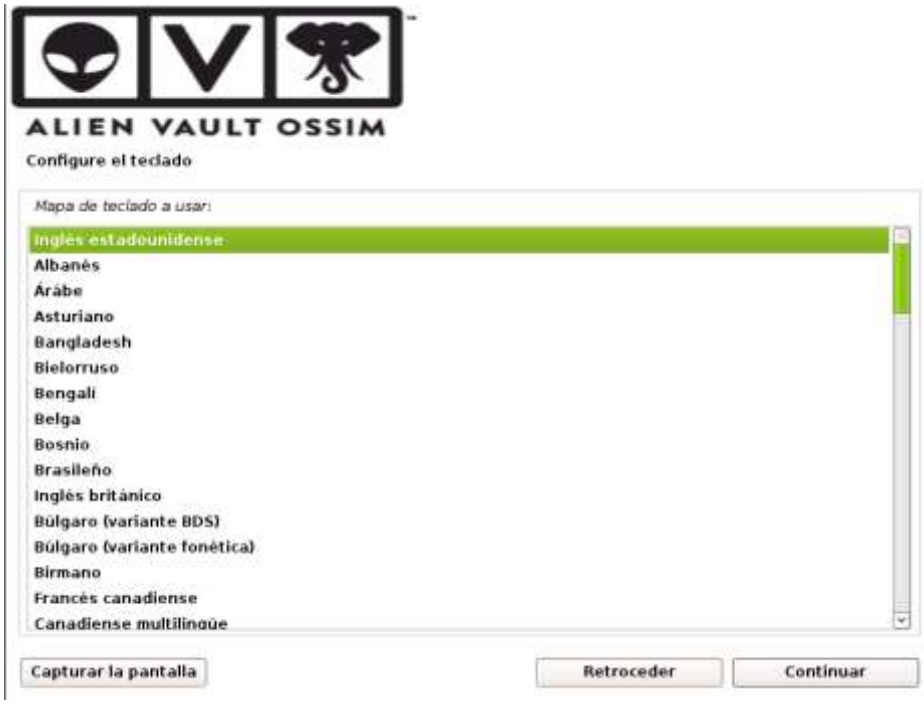


Ilustración 70 Configuración OSSIM AlienVault-Selección dedistribución teclado (Elaboración Propia)

Continuando con el despliegue, inicia con los procesos de instalación y análisis de la imagen.

Ilustración 71 Configuración OSSIM AlienVault-Proceso de Instalación (Elaboración Propia)

Continúa descargando componentes adicionales requeridos para su correcta ejecución.

Ilustración 72 Configuración OSSIM AlienVault-Proceso de descarga paquetes adicionales (Elaboración Propia)

En la siguiente ventana se realiza la configuración de la dirección IP de OSSIM AlienVault.

Ilustración 73 Configuración OSSIM AlienVault-Configuración IP (Elaboración Propia)

Se especifica la máscara correspondiente a la red configurada.

Ilustración 74 Configuración OSSIM AlienVault-Configuración mascara de red (Elaboración Propia)

Se realiza la configuración de la dirección IP para el Gateway (puerta de enlace) que tendrá el servidor.

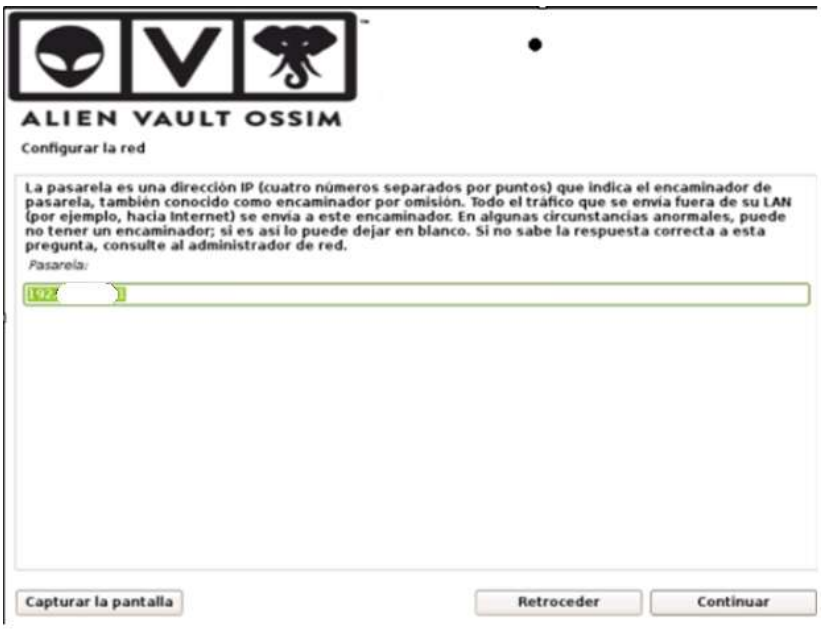


Ilustración 75 Configuración OSSIM AlienVault-Configuración Gateway (Elaboración Propia)

Se realiza la configuración de la IP correspondiente DNS para la resolución de nombres de dominio.

Ilustración 76 Configuración OSSIM AlienVault-Configuración DNS (Elaboración Propia)

En el apartado se realiza la configuración de la contraseña de usuario super usuario

Ilustración 77 Configuración OSSIM AlienVault-Configuración contraseña root (Elaboración Propia)

Se realiza la configuración de la zona horaria

Ilustración 78 Configuración OSSIM AlienVault-Configuración zona horaria (Elaboración Propia)

Luego de indicar los parámetros anteriores se inicia la instalación del sistema OSSIM AlienVault en el disco del servidor.

Ilustración 79 Configuración OSSIM AlienVault-Instalación sistema base II (Elaboración Propia)

Una vez terminada la fase de instalación, se reinicia automáticamente y muestra la siguiente pantalla.

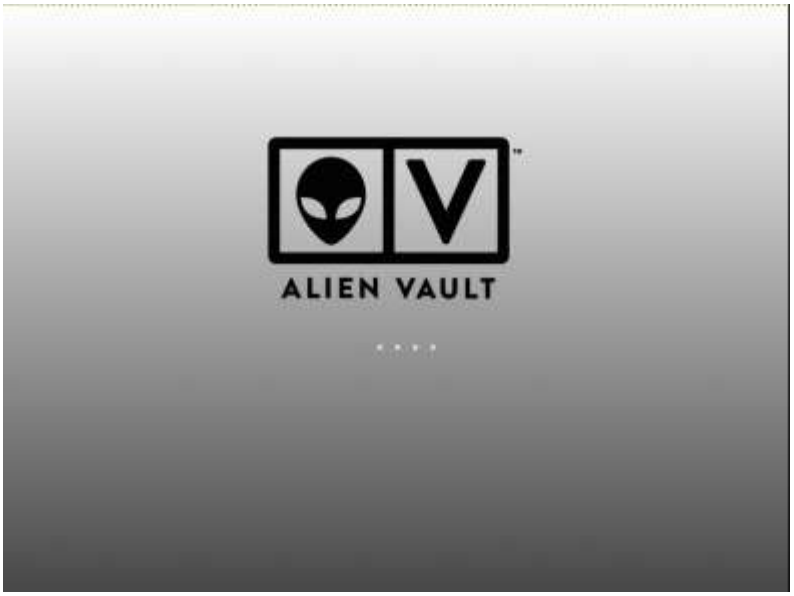


Ilustración 80 Configuración OSSIM AlienVault-Pantalla Inicial sistema base (Elaboración Propia)

Luego nos muestra esta consola para acceder al sistema

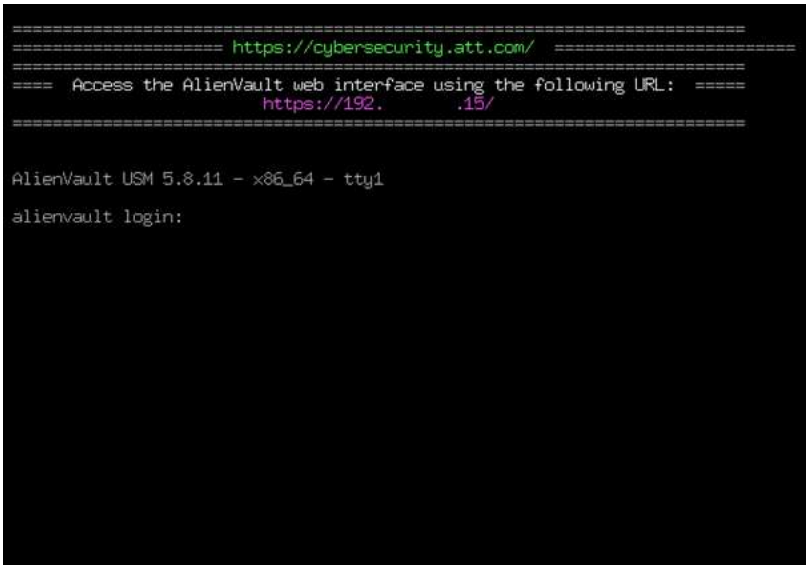


Ilustración 81 Configuración OSSIM AlienVault-Consola Inicial (Elaboración Propia)

Se ingresan las credenciales configuradas, posterior se despliega el siguiente menú con varias opciones de configuración disponibles.

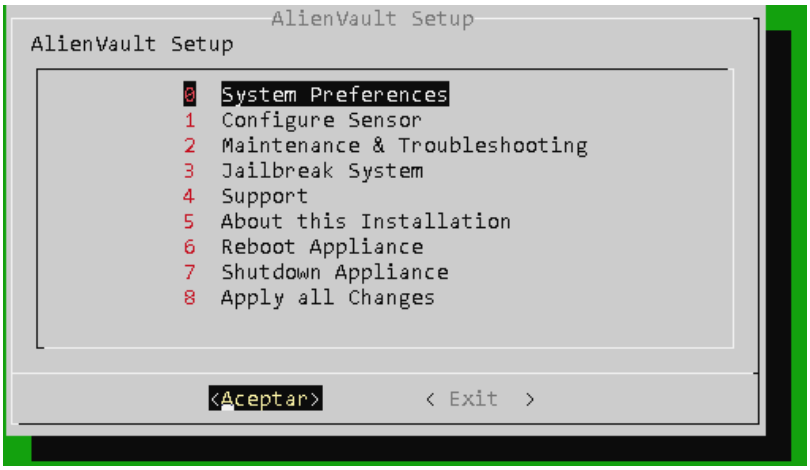


Ilustración 82 Configuración OSSIM AlienVault- Menú (Elaboración Propia)

Para acceder a la interfaz web, se digita en un navegador la IP configurada para el servidor AlienVault. La cual nos mostrará la siguiente pantalla de bienvenida.

En los siguientes campos, nos pide llenar el nombre completo, crear una contraseña por defecto robusta, configurar un email, el nombre de la compañía.

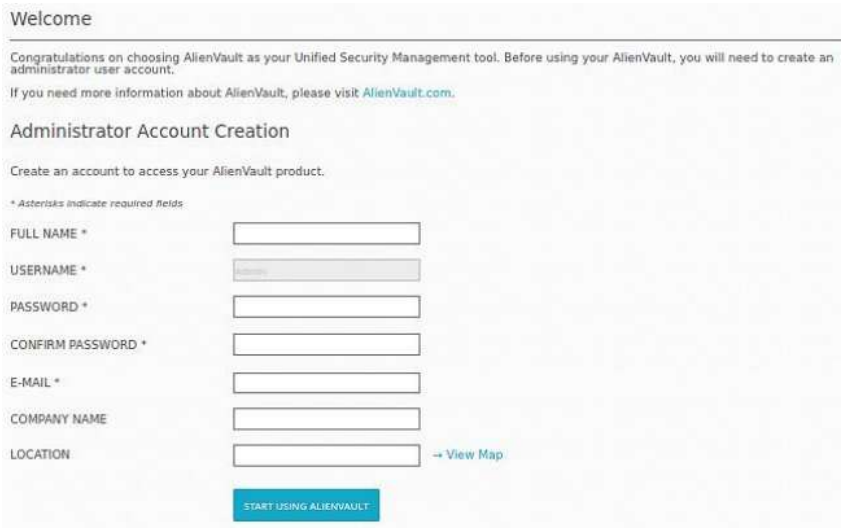


Ilustración 83 Configuración OSSIM AlienVault-Creación de usuario admin (Elaboración Propia)

Luego de ello se muestra la interfaz de login, se ingresa las credenciales configuradas admin y la contraseña, con ello se finaliza la instalación.

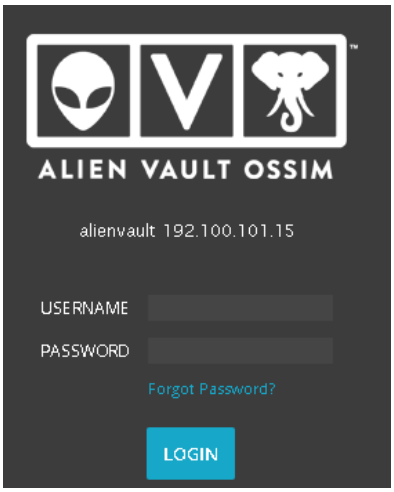


Ilustración 84 Configuración OSSIM AlienVault- Pantalla de ingreso (Elaboración Propia)

Anexo 4: Informe Vulnerabilidades Estado Inicial

Ilustración 85 Informe Vulnerabilidades Estado Inicial parte 1 (Elaboración Propia)

Lucha Campesina
Cooperativa de Ahorro y Crédito

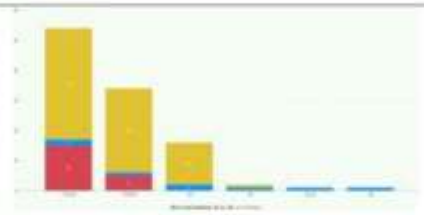
www.luchacampesina.fin.ec

INFORME TILC-ING--001	INFORME VULNERABILIDADES	TECNOLOGIA

OBJETIVO DEL ESTUDIO:	Ejecutar un análisis de vulnerabilidades sobre el ecosistema definido en el alcance del proyecto de tesis en la Cooperativa Lucha Campesina para identificar, recomendar acciones.	FECHA:
SOLICITADO POR:	Ing. Jesennia Cárdenas Cobo, MAE	11/2024
ELABORADO POR:	Ing. Eduardo Tenezaca Carpio	HORA: 10H00

ASUNTO:	Informe de vulnerabilidades servidores desarrollo
ALCANCE:	El alcance de este informe considera las pruebas de seguridad sobre los siguientes grupos de dispositivos, según acuerdo con el cliente: SERVIDORES Nombre / IP TSRVAP / 192.x.x.6 TSRVBD / 192.x.x110 TSRVLC / 192.x.x.17 AD / 192.x.x.2 EQUIPO DE RED Nombre / IP SW / 192.x.x.12 FIREWALL Nombre / IP FW / 10.x.x.1
DETALLE/CUERPO/CONTENIDO:	
Ejecución: Se realizaron las pruebas de seguridad de los activos descritos en el alcance, donde se validó el cumplimiento de mejores prácticas de seguridad en cuanto al blindaje de la infraestructura tecnológica en servidores, equipo de red, y firewall. **Total, de vulnerabilidades Identificadas.**	

Ilustración 86 Informe Vulnerabilidades Estado Inicial parte 2 (Elaboración Propia)

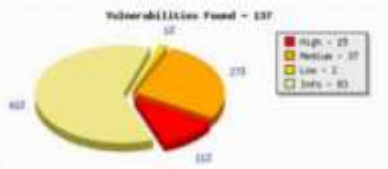


Hostname	High	Low	Medium
TSRVBD	15	2	37
TSRVAP	5	1	28
AD		2	14
RVV		1	1
SRVLC		1	
DVV		1	

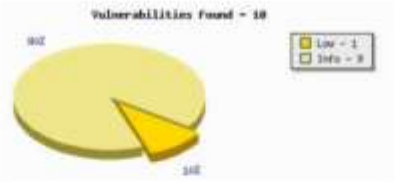
Vulnerabilidades identificadas en Servidores.

En el servidor TSRVAP se detectaron 34 vulnerabilidades siendo 0 criticas, 5 altas, 28 medias, 1 baja.

En el servidor TSRVBD se detectaron 54 vulnerabilidades, 0 criticas, 15 altas, 37 medias, 2 bajas.

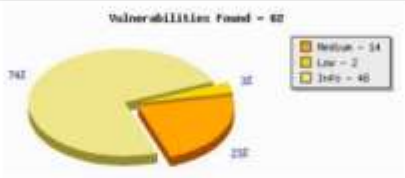


En el servidor colector Linux SRVLC se detectaron un total de 1 vulnerabilidades, 0 criticas, 0 altas, 0 medias, 1 baja.



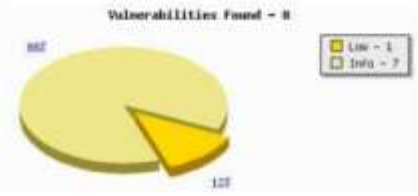
En el servidor AD se detectaron 16 vulnerabilidades de las cuales 0 criticas, 0 altas, 14 medias, 2 bajas.

Ilustración 87 Informe Vulnerabilidades Estado Inicial parte 3 (Elaboración Propia)



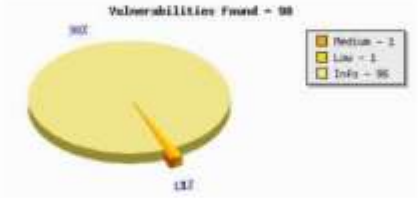
Vulnerabilidades identificadas Equipo de Red.

En el switch se detectaron un total de 1 vulnerabilidades, 0 criticas, 0 altas, 0 medias, 1 baja.



Vulnerabilidades identificadas Equipo de firewall.

En el firewall se detectaron un total de 2 vulnerabilidades, 0 criticas, 0 altas, 1 media, 1 baja.



CONCLUSIONES:	• Se identificaron un total de 108 vulnerabilidades, 0 criticas, 20 altas, 80 medias, y 8 bajas. • Es importante tener en cuenta que el cierre de las vulnerabilidades identificadas mitigaria en gran medida los riesgos de sufrir ciberataques en la Cooperativa. • El número de vulnerabilidades está directamente relacionado con la superficie de análisis, es decir, que se analizaron varios frentes, como servidores, dispositivos de red y firewall.
RECOMENDACIONES:	• Elaborar un plan de cierre de vulnerabilidades para lo identificado, dando prioridad a las vulnerabilidades de riesgo alto y medio respectivamente • Realizar este tipo de análisis de manera recurrente para identificar posibles riesgos de seguridad.

RESPONSABILIDADES	NOMBRES / CARGOS	FIRMAS
ELABORADO POR:	EDUARDO TENEZACA/ ESTUDIANTE UPSE	

Ilustración 88 Informe Vulnerabilidades Estado Inicial parte 4 (Elaboración Propia)

Anexo 5: Plan de Acción

Ilustración 89 Plan de Acción (Elaboración Propia)

Anexo 6: Informe Vulnerabilidades Post Plan de Acción

Ilustración 90 Informe Vulnerabilidades Post Plan de Acción Parte 1 (Elaboración Propia)

Lucha Campesina
Cooperativa de Ahorro y Crédito

www.luchacampesina.fin.ec

INFORME TILC-ING--001	INFORME VULNERABILIDADES RETEST	TECNOLOGIA

OBJETIVO DEL ESTUDIO:	Ejecutar la comprobación de cierre de vulnerabilidades críticas sobre el ecosistema definido en el alcance del proyecto de tesis en la Cooperativa Lucha Campesina.	FECHA:
SOLICITADO POR:	Ing. Jesennia Cárdenas Cobo, MAE	11/2024
ELABORADO POR:	Ing. Eduardo Tenezaca Carpio	HORA: 10H00

ASUNTO:	Informe de vulnerabilidades servidores desarrollo Restest
ALCANCE:	El alcance de este informe considera las pruebas de seguridad sobre los siguientes grupos de dispositivos, según acuerdo con el cliente: SERVIDORES Nombre | IP TSRVAP | 192.x.x.6 TSRVBD | 192.x.x110 TSRVLC | 192.x.x.17 AD | 192.x.x.2 EQUIPO DE RED Nombre | IP SW | 192.x.x.12 FIREWALL Nombre | IP FW | 10.x.x.1

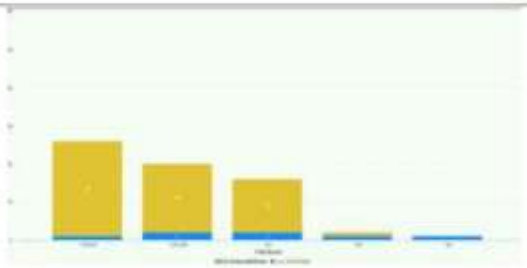
DETALLE/CUERPO/CONTENIDO:

Ejecución:

Se realizaron las pruebas de seguridad de los activos descritos en el alcance, donde se validó el cumplimiento de mejores prácticas de seguridad en cuanto al blindaje de la infraestructura tecnológica en servidores identificados con criticidad alta de acuerdo con lo acordado con el Oficial de Seguridad de la Información y el jefe de Tecnología.

Total de vulnerabilidades identificadas.

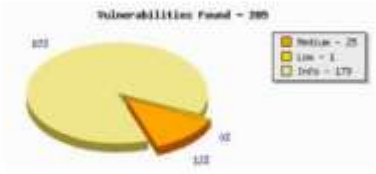
Ilustración 91 Informe Vulnerabilidades Post Plan de Acción Parte 2 (Elaboración Propia)



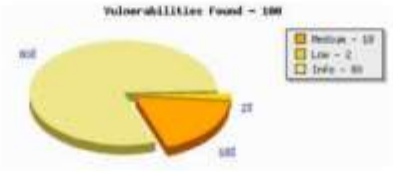
Hostname	Low	Medium
TSRVAP	1	25
TSRVBD	2	18
AD	2	14
FW	1	1
SW	1	

Vulnerabilidades identificadas en Servidores.

En el servidor TSRVAP se detectaron 26 vulnerabilidades siendo 0 criticas, 0 altas, 25 medias, 1 baja.



En el servidor TSRVBD se detectaron 20 vulnerabilidades, 0 criticas, 0 altas, 18 medias, 2 bajas.



CONCLUSIONES:	• Se mitigaron el 40% del total de vulnerabilidades, de las 20 vulnerabilidades altas se mitigó el 100%, mientras que de las 80 vulnerabilidades medias se mitigó el 27.5% y de las 8 vulnerabilidades bajas se mitigó el 12.5 %.	
RESPONSABILIDADES	NOMBRES / CARGOS	FIRMAS
ELABORADO POR:	EDUARDO TENEZACA/ ESTUDIANTE UPSE	

Ilustración 92 Informe Vulnerabilidades Post Plan de Acción Parte 3 (Elaboración Propia)

Anexo 7: Aprobación de paso a producción por Comité de Tecnología.

Cumandá 19 de noviembre del 2024

Certificación

La Suscrito secretaria del Comité de Tecnología de Información de la Cooperativa de Ahorro y Crédito **"LUCHA CAMPESINA LTDA",** en sesión realizada el martes 19 de noviembre del 2024 a las 16:00 pm y luego de analizar el desarrollo del Orden del día, mediante Acta **N° 026 RESOLUCIONES N°026, numeral 6,** aprobó con 04 votos a favor 0 votos en contra, la siguiente resolución detallada a continuación:

6.- Aprobar la implementación en producción del Sistema Correlación de Eventos e Información (SIEM), el cual se incorporará a los activos de tecnología fortaleciendo la seguridad y gestión de servicios.

Es todo cuanto puedo certificar en honor a la verdad.
LO CERTIFICO. –

Atentamente,

MARIA ALEXANDRA BONE JIMENEZ
Firmado digitalmente por MARIA ALEXANDRA BONE JIMENEZ
Fecha: 2024.12.02 22:14:23 -05'00'

SECRETARIA
COMITÉ DE TECNOLOGIA DE INFORMACION
LUCHA CAMPESINA

Ilustración 93 Aprobación de paso a producción por Comité de Tecnología (Elaboración Propia)