Diseño esquema de detección de amenazas con software wazuh en las empresas Pymes en Bogotá Zona Centro

Hernando Yamit Almanza Pumarejo

Asesor

Hernando José Peña Hidalgo

Universidad Nacional Abierta Y A Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería - ECBTI

Especialización En Seguridad Informática

2025

Agradecimientos

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

Resumen

Con la virtualización de parte del sector laboral y la digitalización de la información en los últimos años, especialmente a raíz de la pandemia, se ha observado un aumento significativo de ciberataques dirigidos a organizaciones de todo tipo.

Las PYMES de Bogotá, debido a su reducido personal y recursos financieros limitados, suelen carecer de una infraestructura tecnológica robusta que les permita detectar amenazas como malware, phishing y ransomware en una etapa temprana. Estos ataques son cada vez más comunes y sofisticados. Por lo tanto, es crucial implementar un sistema de detección de intrusiones para garantizar la protección y disponibilidad de los datos de la empresa, proporcionando alertas tempranas sobre comportamientos anómalos en la red que puedan indicar posibles amenazas.

Este documento presenta un marco para dicha implementación, diseñado específicamente para pequeñas organizaciones, que garantiza la monitorización de su información y activos digitales para proteger sus datos.

Palabras clave: Ciberseguridad, ISO 27001, Malware, PYMES, SIEM

Abstract

Due to the virtualization of part of the labor sector as well as the digitization of information in recent years with the trigger of the pandemic, there has been a large increase in cyberattacks directed at organizations of all types.

Pymes in Bogotá, due to their nature of small staff and assets, do not have a robust technological infrastructure that allows them to identify early all the threats of Malware, Pishing, Ransomware, which these attacks are becoming more common every day and with their sophistication. For this reason, it is of vital importance to protect and keep the information of these companies available to have an intrusion detection system so that it alerts in an early manner abnormal behavior of the network that may contain any type of threat.

This document will have the scheme of said implementation especially aimed at small organizations in which they can count that their information and digital assets are monitored to help guarantee and safeguard the information.

Keywords: Cybersecurity, ISO 27001, Malware, PYMES, SIEM

Tabla de Contenido

Pág.

Lista de Tablas

Lista de Figuras

Lista de Apéndice

Introducción

La presente monografía describe la creación y estructuración del esquema de detección de intrusos del software libre Wazuh que permitirá a las empresas pymes en Bogotá contar con una potente herramienta de software libre que se adapte a las necesidades de la organización.

Con el aumento de la información en medios digitales las organizaciones Pymes se encuentran especialmente vulnerables a los ciberataques tan comunes actualmente, el diseño de la estrategia de detección y protección de intrusos abarca la selección de la metodología y estándar que mejor se adecue a las necesidades y que esté vigente en el marco legal en Colombia, así mismo se comparan las mejores soluciones de Ciberseguridad del mercado en cuanto a su licenciamiento como ventajas y desventajas que mejor se adecue al ambiente de las Pymes.

De una solución para SOC y marco de seguridad se procederá a diseñar la estrategia que permitirá dar respuesta de manera oportuna a gran número de amenazas que pueda presentar las organizaciones en Bogotá.

Definición del Problema

Antecedentes del Problema

Colombia es uno de los países de América Latina que más ataques recibió por malware tipo ransomware durante el año 2022. Según el informe "*Cyber Threat Report 2023*" de la empresa SonicWall, este tipo de amenazas se incrementó considerablemente en la región, evidenciando la baja capacidad de muchas organizaciones colombianas para detectar, prevenir y responder ante ciberataques (SonicWall, 2023).

Una de las razones de dichos aumentos de ciberataques se debe que a los delincuentes aprovechan las vulnerabilidades en las prácticas de trabajo hibridas de las organizaciones así que da a entender que el principal punto de ataque es el correo electrónico de los usuarios a través de Phishing lo que permite ejecutar el Malware o sustraerle la información si no es detectado a tiempo o el usuario no cuenta con la experticia para detectar un mail falso.

El panorama de ciberataques en Colombia durante el año 2023 fue preocupante. Según el diario la Republica informo al menos 27 organizaciones fueron víctimas de algún tipo de robo de información, siendo el hurto de credenciales de acceso a plataformas de correo electrónico uno de los principales objetivos. De las entidades afectadas, 17 pertenecían al sector gubernamental y a instituciones de educación superior, lo cual evidencia la vulnerabilidad de sectores estratégicos frente a amenazas cibernéticas (La República, citado en RENATA, 2023).

Por lo anterior, es cada vez más prioritario que las compañías de todos los sectores presten mayor atención a la seguridad de la información con medidas preventivas contra los ciberataques.

Formulación del Problema

En el contexto de un incremento significativo de ciberataques en Colombia, especialmente vinculados al ransomware y al phishing, las pequeñas y medianas empresas (PyMEs) en Bogotá enfrentan una vulnerabilidad creciente. Este panorama evidencia debilidades en sus capacidades de prevención y respuesta frente a amenazas cibernéticas, como lo indica el Informe de Amenazas Cibernéticas 2023 publicado por SonicWall (SonicWall, 2023).

Uno de los principales desafíos radica en la seguridad de la información, particularmente en la detección y protección contra intrusos en el entorno digital. Las prácticas de trabajo híbridas, comunes en muchas organizaciones, brindan una superficie de ataque propicia para los delincuentes cibernéticos, especialmente a través de correos electrónicos de phishing.

El problema se agrava por la falta de experticia en la detección de correos electrónicos falsos por parte de los usuarios, lo que facilita la ejecución de malware o el robo de información sensible. Además, el informe de SonicWall señala que las organizaciones colombianas, especialmente en el sector gubernamental y educativo, están experimentando robos de información, destacando la vulnerabilidad de las credenciales de acceso a plataformas de correo electrónico.

En este contexto, surge la necesidad crítica de implementar estrategias efectivas de detección de intrusos que se adapten a las necesidades específicas de las organizaciones pymes en Bogotá. Es esencial una solución para un SIEM adecuado y establecer un marco de seguridad robusto que permita responder de manera oportuna y eficiente a las amenazas cibernéticas emergentes.

La limitación del trabajo está en las organizaciones Pymes en Bogotá y está centrada en la red de datos de dichas organizaciones por lo cual se seleccionará entre los principales IPS/IDS de

software libre que permita no solo la detección sino la prevención de cualquier comportamiento anómalo en la red por lo cual se desplegará los diferentes componentes del SIEM amparado con la Iso 27001.

Por lo tanto, el problema central a abordar es: ¿Cómo implementar un sistema de detección y prevención de intrusos en la red de datos de las empresas Pymes en Bogotá, mediante herramientas de software libre?

Justificación

Con el aumento de la moderación de los procesos de organización que cada vez más tienen toda su información en medios digitales y con la Pandemia del 2020 que obligo a muchas compañías a realizas sus procesos de manera remota abrió la puerta a los criminales se especializaran en explotar todas las vulnerabilidades que presentan las redes y servicios de informática de las pequeñas organizaciones en Bogotá y al ser hoy en día la información digital el mayor bien de las empresas es de vital importancia su protección y aseguramiento, como se evidencio anteriormente la amenaza más común a la que se enfrentan las organizaciones es el secuestro de información por medio de Ransomware el cual va encriptando la información que le tiene accesible para luego pedir un rescate, al conocer este procedimiento es imprescindible detectar este intruso en la red antes que sea demasiado tarde es por ello de vital importancia contar con una herramienta de detección y monitoreo en tiempo real que sea capaz de detectar no solo la descarga y ejecución del Malware a través de sus detección de intrusos así como entender comportamientos anómalos dentro de la red como la encriptación de sus archivos.

Con el sistema de detección de intrusos basado en host de código abierto Wazuh es posible escanear y monitorear los sistemas en búsqueda de malware, rootkits y anomalías sospechosas, es capaz de detectar archivos y procesos ocultos así como todo el monitoreo y escucha de la red interna, con dichas características es posible detectar de manera temprana un ataque a través de Malware a la red donde se tenga implementado esta solución lo cual lo hace una herramienta imprescindible para el panorama de ciberseguridad de Bogotá en la actualidad para las pequeñas empresas.

Objetivos

Objetivo General

Diseñar una estrategia para la detección y prevención de intrusiones mediante el uso de herramientas de software libre para fortalecer las capacidades de ciberseguridad en las Pymes de Bogotá

Objetivos Específicos

Desarrollar el estado del arte de la tendencia actual de los IDS/IPS, a partir de una revisión de soluciones tecnológicas y sus capacidades que permita reconocer las herramientas que pueden utilizarse en el aseguramiento de la información.

Analizar las metodologías y marcos para la detección y contención de intrusiones mediante una comparación de sus capacidades y métodos para el establecimiento de un mapa de ruta aplicable a las pymes en Bogotá.

Proponer una solución para la detección de amenazas mediante la adopción de herramientas tecnológicas que fortalezcan la seguridad de la información.

Determinar metodologías normatividad, herramientas de detección y prevención de intrusos con el fin de mejorar la capacidad de respuesta de ciber amenazas de las pymes en Bogotá.

Marco Referencial

Desde que la información de las organizaciones se convirtieron un pilar fundamental para la continuidad de negocio se evidencio la necesidad de proteger dichos activos digitales contra cualquier tipo de ataque que atente con la integridad, disponibilidad y estado de la información, por lo cual se tiene la publicación de IEEE del 2009 ya se observaba el incremento de hackers y malwares por lo que se requiere evitar que la información de equipos del gobiernos puedan verse afectadas, con las soluciones SIEM para la detección de intrusos en tiempo real a nivel de red utilizando la tecnología de conteo CBFs (Counting Bloom Filters).

Con la sofisticación de los ataques también ha ido evolucionando las medidas de detección que tienen los sistemas de monitoreo para detectar a tiempos las amenazas que pueden incidir en comprometer la estructura de la red así como de su información por lo cual las herramientas SIEM como informa Elsevier con su publicación “A global security architecture for intrusion detection on computer networks” el cual puede detectar ataques simultáneos en varios sitios y redes lo que proyecto una vista global de la seguridad de la red.

El monitoreo y detección de intrusos debe buscar y analizar un enorme tráfico dentro de la red, es por ello por lo que los SIEM esencialmente cuenta con un abanico de herramientas que puede hacer esta tarea más simple lo que permite contar con un mayor aumento de encontrar amenazas o falsos positivos que pueden poner en riesgo la integridad de la seguridad de la red.

Marco Conceptual

SOC

El centro de operaciones de seguridad se refiere a todo el personal, herramientas de hardware y software y procesos de ciberseguridad que trabajando en conjunto son los responsables de la seguridad de la información de una organización, también se puede definir como una plataforma que se encarga de toda la supervisión y administración de la seguridad del sistema de información a través de herramientas de captura, correlación de eventos e intervención remota.

SIEM

(Security Information Event Management) la información sobre seguridad y gestión de eventos es una solución de seguridad que permite a las organizaciones a reconocer posibles amenazas y vulnerabilidad de seguridad antes que puedan causar alguna alteración de la información, permite visualizar las anomalías en el comportamiento del usuario y tuliza inteligencia artificial para automatizar muchos de los procesos manuales asociados con la detección de amenazas.

IDS

Un sistema de detección de intrusos es una herramienta de supervisión que detecta actividades sospechosas y genera alertas tempranas sobre el incidente, por medio de estas alertas el administrador de la herramienta de ciberseguridad investiga el problema y toma las medidas necesarias para corregir dicha alerta o amenaza.

IPS

Es un sistema de previsión de intrusos que permite alertas a los administradores de la seguridad informática tomar medidas antes que el intruso ingresa a la red o tome control de algún

activo informático mediante el despliegue de software y controles con reglas de identificación de comportamiento anómalo y base de datos conocidas de software malicioso.

Endpoint Security

Es un sistema central de seguridad que permite mitigar riesgo de amenazas evitando que dichas infecciones se propaguen por la red, su modo de acción más común en la instalación de un software en cada dispositivo de la red que está monitoreando y realizando análisis tanto a los archivos como a la navegación puertos y demás y si detecta algún archivo malicioso o actividad anómala bloquee el dispositivo para evitar su propagación en la red.

Threat Intelligence

Son los conocimientos que se obtienen mediante análisis de datos, base de datos de amenazas que permite detectar, reconocer y prevenir las amenazas.

Incident Response

Es el conjunto de acciones que una organización lleva a cabo para identificar, gestionar y recuperarse de una amenaza de ciberseguridad, es posible programar el actuar de manera automática mediante una amenaza por medio de controles previamente establecidos y configurados para una correcta respuesta que logre detectar y bloquear la amenaza.

Marco Histórico

Desde que las redes de las organizaciones se han vuelto cada vez más publicas hacia el internet a surgido a la par la necesidad de proteger, asegurar, monitorear dicha red junto con su información, por lo cual desde el 2009 se han desarrollado hardware de Network Intrusion Detection (NID) acompañado del método de conteo CBFs (Counting Bloom FIlters) permitía analizar información con una mayor velocidad en la detección de amenazas, con la llegada de los SIEM en el 2005 han venido aumentando su importancia e incidencia en la seguridad informática.

Antecedentes

Con la seguridad informática y avance del uso de los SIEM se encuentra muchos autores que han venido contribuyendo a la mejoría de estas plataformas para proteger la información lo que permite entender todo su funcionamiento.

Debido al aumento de los ataques informáticos se tienen muchos antecedentes de los peligros que se enfrentan las organizaciones por no contar con sistemas de monitoreo de intrusos, así como varios trabajos de implementación en distintas organizaciones en Bogotá de SIEM que permiten mantener la seguridad de la red.

Marco Científico o Tecnológico

Se describen los componentes de los SIEM que se utilizaran para detectar intrusos en tiempo real en la red de pruebas:

Intrusion detection: este agente del software libre Wazuh monitorea el sistema en busca de malware y anomalías.

Log Data Analysis: este componente lee la operación del sistema y aplicaciones por medio de logs, que ayudan a encontrar cualquier actividad que incida en la seguridad de la red.

File Integrity Monitoring: identifica cualquier cambio sospechoso que se presente en la red y puede leer y modificar archivos en búsqueda de anomalías asociadas a malwares.

Vulnerability Detection: con este componente permite enviar información al servidor y subirla mediante logs para compararlas en las bases de datos para identificar las amenazas.

Marco Legal

El gobierno colombiano emitió el decreto 338 que establece los lineamientos generales para la gobernanza de seguridad digital.

- Ley 1273 de 2009 se cree el bien jurídico de la protección de la información y de los datos.

Establece delitos y sanciones relacionados con sistemas informáticos, datos personales, software malicioso y otros.

Preserva los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- Conpes 3701 se establece los lineamientos de política para la ciberseguridad en Colombia.

Busca generar los lineamientos de política en ciberseguridad orientados a desarrollar una estrategia nacional que ayude a minimizar el incremento de las amenazas informáticas que afectan significativamente al país, así mismo recoge los antecedentes nacionales e internaciones, como la normatividad del país en torno al tema.

Análisis del Estado del Arte de los IPS/IDS y su Aplicabilidad en la Protección de la Información

En la era digital actual donde tecnologías como la computación en la nube y el internet de las cosas (IoT) se integran en diversas industrias, la ciberseguridad se ha convertido en una prioridad crítica para las organizaciones. Los sistemas de detección y prevención de intrusos, conocidos como IDS (Intrusion Detection Systems) e IPS (Intrusion Prevention Systems), desempeñan un papel clave en la protección contra ataques cibernéticos. En especial, las pequeñas y medianas empresas (PYMES) de Bogotá, que suelen contar con presupuestos limitados, se ven obligadas a implementar soluciones eficaces y de bajo costo para proteger sus redes e infraestructuras. Este trabajo se centra en el diseño de una estrategia integral que incluya la implementación de IDS/IPS en un Centro de Operaciones de Seguridad (SOC), considerando los desafíos y oportunidades que plantea la ciberseguridad actual en entornos corporativos modernos. La importancia de un SIEM con monitoreo en tiempo real y personal especializado en fundamental para gestionar incidencias y proteger de manera efectiva la infraestructura empresarial.

Revisión de los IDS/IPS en la Ciberseguridad Actual

En un mundo cada vez más interconectado, donde la computación en la nube y el Internet de las cosas (IoT) están impulsando la unión de las tecnologías y hardware acompañando a la revolución industrial, la seguridad cibernética se ha convertido en un desafío crítico para las organizaciones. Los Sistemas de Detección de Intrusos (IDS) y los Sistemas de Prevención de Intrusos (IPS) juegan un papel fundamental en la protección de las redes y sistemas de información contra las crecientes amenazas cibernéticas, especialmente para entorno corporativos con poco presupuesto como las Pymes en Bogotá.

Al consultar los autores en los relacionado a SIEM se encuentran puntos en común de cómo abordar esta problemática para contar con la mejor protección de todo tipo de malware o accesos no permitidos a su infraestructura.

Evolución de la Seguridad

La introducción de tecnologías como la computación en la nube y el IoT ha cambiado el panorama de la seguridad cibernética. Sin embargo, a pesar de los avances en la infraestructura y la conectividad, los paradigmas de seguridad no han evolucionado al mismo ritmo. La mayoría de las organizaciones aún dependen de un enfoque de seguridad perimetral, lo que genera desafíos en términos de autenticación, confidencialidad, integridad y disponibilidad de datos, ahora con un Endpoint en los dispositivos no es suficiente que asegure la protección de la infraestructura, es necesario contar una solución integral que ataque todos los frentes comunes de los ciberataques iniciando con un Soc con personal capacitado y especializado en la detección de amenazas, dicho Soc debe contar con un monitoreo en tiempo real que permita gestionar todas las posibles incidencias de seguridad acorde con los estándares actuales.

Importancia de las Soluciones IDS/IPS

El autor Erdal Ozkaya en Cybersecurity: The Beginner's Guide : A Comprehensive Guide to Getting Started in Cybersecurity y Marcos Rodrigues en Design and Implementation of a Low-Cost Low Interaction IDS/IPS System Using Virtual HoneypotApproach recalcan la importancia en que las organizaciones entiendan e inviertan tanto en recursos humanos, capacitaciones hardware y software que permita una protección perimetral robusta por medio de un IDS/IPS y un SIEM que permita gestionar de forma centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad.

Desafíos y requisitos actuales

Las infraestructuras modernas son cada más complejas lo que aumenta la superficie de ataque por lo cual se requiere unas medidas de seguridad junto con un marco de trabajo adaptable y flexible a las necesidades y legislación particular.

Marcos de Ciberseguridad

Existe un esfuerzo significativo por parte de diversas organizaciones internacionales, universidades y entidades para establecer marcos de ciberseguridad como ISO o NIST son adaptados por las organizaciones en la evaluación de riesgos para sistemas industriales. La gestión de identidad y acceso y las capacidades de acceso del usuario son esenciales en marcos de ciberseguridad distribuidos porque confirman la legitimidad de las cosas materiales y lógicas incluidas en la construcción, así como la autorización para acceder a servicios e infraestructuras diseminados y desplegados en diversas organizaciones.

En la siguiente imagen se puede apreciar los distintos frameworks y estándares de Ciberseguridad y con sus principales características y sus fases.

Figura 1

Frameworks y Estándares en la Cyberseguridad

Nota. Recuperado de: newcontrol.com.pe

Seguridad en la Nube y Virtualización

Con el aumento de las implementaciones en la nube y la virtualización, la investigación se centra en el desarrollo de soluciones IDS/IPS específicas para entornos virtuales y en la nube. Esto incluye la detección de amenazas en máquinas virtuales, contenedores y servicios en la nube, así como la protección de la infraestructura de red virtualizada.

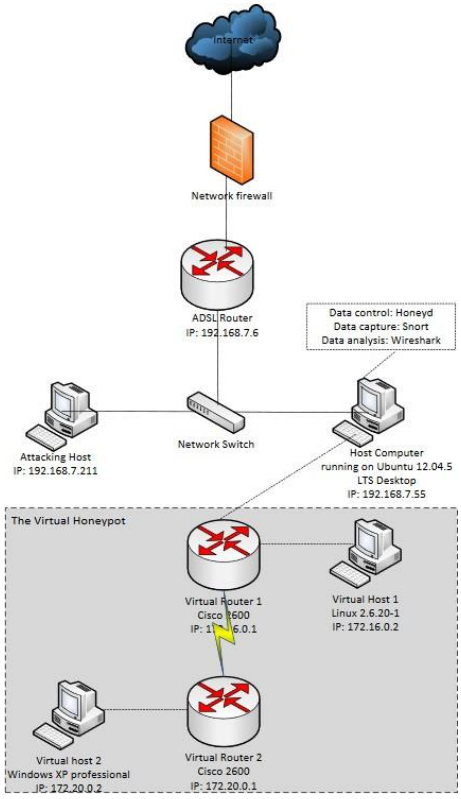
Por lo cual en las organizaciones es indispensable conocer su entorno e infraestructura para tener claro su alcance, así como la documentación sobre las potenciales amenazas a las que podrían enfrentarse y los activos críticos que requieren protegerse. La selección de la herramienta IDS/IPS para ser implementada la cual se debe adaptar a las necesidades particulares, así como al marco de trabajo para garantizar una acción eficaz, más adelante se realizará un análisis de los distintos software libre de protección y monitoreo.

La arquitectura de la solución es una decisión muy importante ya que determine en donde colocar los sensores IDS/IPS como será su integración y la comunicación con el SIEM, la mayoría de los autores recomienda el inicio de la seguridad perimetral después del Modem del operador para controlar todo el tráfico entrante los autores Olamilekan Shobayo y Marcos Rodrigues en su trabajo Design and Implementation of a Low-Cost Low Interaction IDS/IPS System Using Virtual HoneypotApproach propone la topología del firewall después de la conexión a internet y el Honeypot que para nuestro caso particular seria el SIEM y por su bajo costo es perfecto para las Pymes en Bogotá.

En la imagen se observa un esquema de protección de una red por medio de un Honeypot.

Figura 2

Esquema de Protección con Honeypot



Nota. Recuperado de: journals.covenantuniversity.edu.ng

Los Sistemas de Detección de Intrusos (IDS) y los Sistemas de Prevención de Intrusos (IPS) son esenciales para la seguridad de las redes y sistemas de información, especialmente en el contexto de las PYMES en Bogotá que operan con presupuestos limitados. La implementación de un Centro de Operaciones de Seguridad (SOC) que incluya IDS/IPS y un SIEM (Security Information and Event Management) es crucial para la protección contra amenazas cibernéticas. La seguridad cibernética no ha evolucionado al mismo ritmo que las tecnologías como la computación en la nube y el Internet de las Cosas (IoT). Las organizaciones todavía dependen en gran medida de la seguridad perimetral, lo cual presenta desafíos significativos en términos de

autenticación, confidencialidad, integridad y disponibilidad de datos por lo cual el SIEM será fundamental en la ayuda de la detección de amenazas por medio del análisis de datos capturados en la red en busca de anomalías.

Por lo cual no es suficiente con asegurar solo los endpoints (dispositivos finales). Es necesario implementar una solución integral que aborde todas las posibles amenazas cibernéticas. Esto incluye contar con personal capacitado y especializado en la detección de amenazas, y un monitoreo en tiempo real para gestionar las incidencias de seguridad de acuerdo con los estándares y controles predefinidos, con la evolución de las redes empresariales que cada vez más organizaciones tienen su información digital e involucran sus procesos la automatización con la revolución industrial aumento la implementación en la nube y la virtualización por lo cual es crucial desarrollar soluciones IDS/IPS específicas para estos entornos. Esto incluye la detección de amenazas en máquinas virtuales, contenedores y servicios en la nube.

las infraestructuras modernas son cada vez más complejas, lo que aumenta la superficie de ataque. Se requiere un marco de trabajo adaptable y flexible, así como medidas de seguridad específicas para estas infraestructuras, es decir, la solución debe tener la capacidad de epatarse a las necesidades de la organización donde se requiera implementar.

La arquitectura de la solución es una decisión crítica. La colocación de los sensores IDS/IPS y su integración y comunicación con el SIEM son aspectos fundamentales. La mayoría de los autores recomienda la seguridad perimetral iniciando después del módem del operador para controlar todo el tráfico entrante y debe contar con la adopción de marcos de ciberseguridad como los proporcionados por ISO y NIST es esencial para la evaluación de riesgos y la gestión

de identidad y acceso en sistemas industriales. Estos marcos ayudan a confirmar la legitimidad y la autorización de acceso a servicios e infraestructuras.

En un entorno tecnológico en constante evolución, la ciberseguridad debe adaptarse rápidamente para proteger a las organizaciones de amenazas cada vez más sofisticadas. La implementación de SOC que integren IDS/IPS y SIEM es esencial para una defensa robusta, especialmente para PYMES con recursos limitados. Los avances en la computación en la nube y el IoT requieren soluciones específicas y adaptables que aborden la complejidad de las infraestructuras modernas. La adopción de marcos de ciberseguridad reconocidos y la construcción de una arquitectura de seguridad sólida son pasos cruciales para garantizar la protección de los datos y sistemas de información en este nuevo panorama digital. A medida que las empresas continúan su transición hacia entornos en la. Nube y virtualizados, resulta crucial desarrollar y ajustar continuamente las estrategias de seguridad. Solo mediante una arquitectura de seguridad bien diseñada y una gestión proactiva de los riesgos será posible salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas en el nuevo panorama digital.

Análisis de las Metodologías y Marcos de Trabajo en la Implementación de los SIEM

En el contexto de la seguridad informática, los sistemas de detección y prevención de intrusos juegan un papel fundamental en la protección de las redes y sistemas de información de una organización. A medida que las amenazas cibernéticas continúan evolucionando, es crucial contar con herramientas efectivas que permitan identificar, responder y mitigar actividades sospechosas o maliciosas

Objetivos: El objetivo principal de un IDS es proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos de una organización. Esto implica identificar y responder a actividades no autorizadas o anómalas que podrían representar una amenaza para la seguridad.

Datos de entrada: Un IDS recopila datos de diversas fuentes, como registros de eventos del sistema, registros de red, registros de aplicaciones y registros de bases de datos. Estos datos proporcionan información sobre el tráfico de red, el comportamiento del sistema y las actividades de los usuarios.

Análisis de eventos: Los datos recopilados son analizados para identificar eventos que puedan indicar un comportamiento sospechoso o malicioso. Esto se puede lograr mediante técnicas como la correlación de eventos, el análisis de anomalías y el uso de firmas o patrones conocidos de ataques.

Reglas y firmas: Un IDS utiliza reglas y firmas predefinidas para comparar los eventos analizados con patrones conocidos de ataques o comportamiento malicioso. Estas reglas pueden ser desarrolladas internamente o proporcionadas por fuentes externas, como proveedores de seguridad.

Detección y alerta: Si se encuentra una coincidencia entre los eventos analizados y una regla o firma, el IDS genera una alerta para notificar a los administradores del sistema sobre la actividad sospechosa. Estas alertas pueden ser visualizadas en un panel de control o enviadas por correo electrónico, mensajes de texto u otros medios de comunicación.

Respuesta y mitigación: Una vez que se genera una alerta, los administradores del sistema deben tomar medidas para investigar y responder al incidente. Esto puede implicar el bloqueo de direcciones IP, el cambio de contraseñas, la desconexión de usuarios o la implementación de otras medidas de mitigación.

Un sistema de protección de intrusos (IPS, por sus siglas en inglés) se centra en prevenir y bloquear actividades maliciosas o no autorizadas en una red o sistema.

Objetivos: El objetivo principal de un IPS es proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos de una organización. Se enfoca en evitar que las intrusiones o ataques tengan éxito y bloquear el acceso no autorizado a los recursos de la red.

Políticas de seguridad: Un IPS se basa en políticas de seguridad bien definidas que establecen reglas y directrices para proteger los sistemas. Estas políticas deben ser coherentes con los objetivos de seguridad de la organización y deben abordar aspectos como la identificación de amenazas, el control de acceso y la prevención de ataques específicos.

Detección y prevención: Un IPS combina capacidades de detección y prevención para identificar y bloquear actividades maliciosas. Utiliza técnicas como la inspección profunda de paquetes (DPI), el análisis de anomalías, la detección de firmas y la correlación de eventos para identificar patrones de ataques conocidos o comportamientos anómalos.

Actualizaciones y bases de datos de amenazas: Un IPS se mantiene actualizado con las últimas bases de datos de amenazas y firmas de ataques conocidos. Estas actualizaciones permiten al sistema reconocer y bloquear nuevas variantes de ataques y técnicas utilizadas por los intrusos.

Acciones de mitigación: Cuando se detecta una actividad sospechosa o maliciosa, un IPS toma medidas de mitigación inmediatas para bloquear la amenaza. Esto puede incluir la generación de alertas, el bloqueo de direcciones IP, la terminación de conexiones, el cierre de puertos o cualquier otra acción definida en las políticas de seguridad.

Monitorización y registro: Un IPS registra y monitoriza continuamente el tráfico de red y las actividades del sistema. Esto permite la recolección de datos para el análisis posterior, la

identificación de patrones de ataques y la generación de informes de seguridad para su revisión y análisis.

Integración con otros sistemas de seguridad: Un IPS se integra con otros sistemas de seguridad, como firewalls, sistemas de detección de intrusos (IDS), sistemas de gestión de eventos y registros de seguridad (SIEM) y sistemas de prevención de pérdida de datos (DLP). Esta integración permite una respuesta coordinada y una mayor eficacia en la protección de la red y los sistemas.

Evaluación y mejora continua: Es esencial evaluar y mejorar constantemente el desempeño del IPS. Esto puede implicar pruebas de penetración, evaluaciones de vulnerabilidades, análisis de registros y la implementación de actualizaciones y parches de seguridad. La retroalimentación y la retroalimentación de los incidentes de seguridad también contribuyen a la mejora continua del sistema.

Detección y Respuesta a Incidentes: El SIEM debe ser capaz de detectar y responder rápidamente a incidentes de seguridad. Esto incluye:

Identificación de Amenazas: Utilizar herramientas de análisis y correlación de datos para identificar patrones de comportamiento que indiquen la presencia de amenazas.

Análisis de Incidentes: Evaluar la gravedad y el impacto de los incidentes detectados.

Respuesta Inmediata: Implementar medidas de contención, erradicación y recuperación para minimizar el impacto del incidente.

Gestión de Logs y Análisis Forense: La recopilación y el análisis de logs son fundamentales para la detección de amenazas y el análisis forense post-incidente. Los logs proporcionan un registro detallado de todas las actividades en la red, lo cual es crucial para:

Investigación de Incidentes: Determinar cómo ocurrió un incidente y qué medidas deben tomarse para prevenir futuros eventos similares.

Cumplimiento Normativo: Asegurar que la organización cumpla con las regulaciones y estándares de seguridad como se encuentra en su página web de documentación (Wazuh, n.d.) como PCI DSS el cual es el estándar para pagos con tarjeta de crédito HIPAA es la ley en los Estados Unidos que establece estándares para proteger la información médica sensible y NIST 800-53 que son los conjuntos de controles de seguridad y privacidad desarrolladores por el Instituto Nacional de Estándares y Tecnología (NIST).

La inteligencia de amenazas permite al SIEM anticiparse a los ataques mediante el análisis de información sobre amenazas emergentes. Esto incluye:

Recolección de Datos: Obtener información de diversas fuentes sobre amenazas conocidas y nuevas.

Análisis Predictivo: Utilizar modelos predictivos y análisis de tendencias para identificar posibles vectores de ataque.

Compartición de Información: Colaborar con otras organizaciones y entidades para compartir datos de inteligencia de amenazas.

Formación y Concienciación

La formación continua del personal de seguridad y la concienciación de los empleados sobre buenas prácticas de ciberseguridad son componentes críticos de un SIEM efectivo. Esto incluye:

Entrenamiento Regular: Capacitar al personal en las últimas técnicas y herramientas de seguridad.

Simulacros de Incidentes: Realizar ejercicios de simulación para preparar al equipo ante posibles escenarios de ataque.

Campañas de Concienciación: Informar a todos los empleados sobre las mejores prácticas de seguridad y cómo identificar posibles amenazas.

Los sistemas de detección y prevención de intrusos (IDS e IPS) son componentes esenciales en la estrategia de seguridad de cualquier organización. Su capacidad para identificar y responder a actividades sospechosas o maliciosas es crucial para mantener la integridad, confidencialidad y disponibilidad de los datos. A través de la recopilación y análisis de datos, la utilización de reglas y firmas, y la implementación de políticas de seguridad bien definidas, los IDS e IPS pueden detectar y bloquear amenazas de manera efectiva.

La integración de los IDS e IPS con otros sistemas de seguridad, como firewalls y sistemas de gestión de eventos de seguridad (SIEM), permite una respuesta coordinada y mejora la protección global de la red. Además, la actualización constante de bases de datos de amenazas y la evaluación continua del desempeño del IPS mediante pruebas de penetración y análisis de vulnerabilidades son prácticas esenciales para mantenerse al día con las nuevas amenazas y mejorar continuamente la eficacia del sistema. Los IDS/IPS proporcionan una capa adicional de defensa que es vital en el panorama de seguridad cibernética actual. Implementar y mantener estos sistemas de manera efectiva puede marcar la diferencia entre una red segura y una comprometida, destacando su importancia en cualquier estrategia de ciberseguridad.

Las metodologías SIEM se centran en una serie de procesos y tecnologías que trabajan en conjunto para proporcionar una defensa integral contra las amenazas cibernéticas. Estas metodologías incluyen el monitoreo continuo, la detección y respuesta a incidentes, la gestión de vulnerabilidades, la inteligencia de amenazas, la automatización y orquestación, y la formación

continua, los SIEM como encargados de proteger y asegurar la información de las organizaciones por lo cual deben contar con metodologías y normativas con las cuales tener los lineamientos para alcanzar los objetivos propuestos, las metodologías y normas más utilizadas en los SIEM son:

Metodología MITRE ATT&CK: El MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es un marco de trabajo utilizado para describir y categorizar las tácticas y técnicas utilizadas por los atacantes. Los SIEM pueden utilizar esta metodología para comprender mejor las tácticas que pueden ser empleadas contra su organización y desarrollar contramedidas efectivas.

Metodología de detección y respuesta de seguridad (EDR): La metodología EDR se centra en la detección temprana, la respuesta y la mitigación de amenazas avanzadas. Los SIEM pueden utilizar herramientas EDR para recolectar y analizar datos en tiempo real de los sistemas y redes, con el fin de identificar comportamientos maliciosos y responder rápidamente.

Norma ISO 27001: La norma ISO 27001 establece los requisitos para implementar un sistema de gestión de seguridad de la información (SGSI) en una organización. Los SIEM pueden seguir esta norma para establecer políticas, procedimientos y controles de seguridad eficaces, y garantizar la confidencialidad, integridad y disponibilidad de la información.

Norma NIST SP 800-61: El NIST SP 800-61 es un documento de referencia del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, que describe las mejores prácticas para gestionar y responder a incidentes de seguridad. Los SOC pueden utilizar esta norma para establecer un proceso de respuesta a incidentes eficaz, desde la detección y notificación inicial hasta la recuperación y el aprendizaje posterior al incidente.

Metodología SIEM (Security Information and Event Management): Los sistemas SIEM se utilizan para recopilar, analizar y correlacionar registros de eventos y datos de seguridad en tiempo real. Los SOC pueden implementar una metodología SIEM para monitorear y detectar actividades sospechosas o maliciosas en la infraestructura de la organización.

La importancia de que los Centros de Operaciones de Seguridad (SOC) adopten metodologías y normativas específicas para proteger y asegurar la información de las organizaciones de manera efectiva. La implementación de marcos de trabajo como MITRE ATT&CK, la metodología de detección y respuesta de seguridad (EDR), y la utilización de sistemas de gestión de seguridad de la información basados en normas como ISO 27001 y NIST SP 800-61, son fundamentales para desarrollar contramedidas eficaces y garantizar la confidencialidad, integridad y disponibilidad de la información. Además, la metodología SIEM es crucial para la recopilación, análisis y correlación de datos de seguridad en tiempo real, permitiendo a los SIEM detectar y responder rápidamente a actividades sospechosas o maliciosas. En conjunto, estas metodologías y normativas proporcionan un marco integral y robusto para la gestión de la seguridad, permitiendo a los SIEM enfrentar las amenazas cibernéticas de manera proactiva y eficaz.

Para implementar un SIEM efectivo, es necesario seguir una serie de pasos que aseguren la integración y funcionamiento adecuado de todas las metodologías mencionadas:

Evaluación de Necesidades y Requisitos: Identificar las necesidades específicas de la organización y los requisitos de seguridad.

Diseño de la Arquitectura SOC: Definir la arquitectura del SOC, incluyendo la colocación de sensores IDS/IPS y la integración con sistemas SIEM.

Selección de Herramientas y Tecnologías: Elegir las herramientas y tecnologías adecuadas que cumplan con los requisitos de la organización.

Capacitación del Personal: Formar al personal en el uso de herramientas y en la implementación de procedimientos de seguridad.

Implementación y Configuración: Implementar y configurar las herramientas y tecnologías seleccionadas.

Monitoreo y Ajustes Continuos: Realizar monitoreo continuo y ajustes necesarios para optimizar la operación del SIEM.

Selección de Metodologías

La implementación de la norma ISO 27001 en un Centro de Operaciones de Seguridad (SOC) es esencial para fortalecer la seguridad de la información y garantizar la protección de los activos de la organización. Este proceso requiere un compromiso firme por parte de la alta dirección, la definición clara del alcance del sistema de gestión de seguridad de la información (SGSI), y la realización de evaluaciones de riesgos detalladas. El desarrollo de políticas y procedimientos específicos, la implementación de controles de seguridad adecuados, y la realización de pruebas y auditorías internas son pasos críticos para asegurar la conformidad con la norma. La certificación externa y el mantenimiento de un ciclo de mejora continua también son fundamentales para mantener la eficacia del SGSI del SOC.

La implementación de la norma ISO 27001 en un Centro de Operaciones de Seguridad (SOC) puede ayudar a fortalecer la seguridad de la información y garantizar la protección de los activos de la organización por lo cual la importancia de contar con lo siguiente:

Compromiso de la alta dirección: Es fundamental que la alta dirección de la organización respalde y se comprometa con la implementación de la norma ISO 27001 en el SOC. Deben asignar los recursos necesarios y designar a un responsable del proyecto.

Establecimiento del alcance: Definir el alcance del sistema de gestión de seguridad de la información (SGSI) del SOC. Esto incluye identificar los activos de información relevantes, los procesos involucrados y los límites del SOC.

Realización de una evaluación de riesgos: Realizar una evaluación de riesgos para identificar las amenazas y vulnerabilidades que pueden afectar la seguridad de la información en el SOC. Esto implica identificar los activos críticos, evaluar las amenazas potenciales y determinar los riesgos asociados.

Desarrollo de políticas y procedimientos: Crear políticas y procedimientos de seguridad de la información específicos para el SOC. Estos deben abordar aspectos como el acceso físico y lógico, la gestión de incidentes, la protección de datos, la monitorización y la respuesta a eventos de seguridad.

Implementación de controles de seguridad: Establecer controles de seguridad de acuerdo con los requisitos de la ISO 27001. Esto puede incluir controles técnicos (como firewalls, sistemas de detección de intrusiones, cifrado), controles organizativos (como políticas y procedimientos) y controles físicos (como sistemas de acceso restringido).

Realización de pruebas y auditorías internas: Realizar pruebas y auditorías internas periódicas para evaluar la eficacia de los controles implementados y asegurarse de que se cumplen los requisitos de la norma ISO 27001.

Certificación externa: Si se desea obtener la certificación ISO 27001, se debe contratar a un organismo de certificación externo que realice una auditoría y emita la certificación oficial.

Mantenimiento y mejora continua: El proceso de implementación de la ISO 27001 es un ciclo continuo. Es importante mantener y mejorar continuamente el SGSI del SOC, revisar regularmente los controles, realizar evaluaciones de riesgos actualizadas y responder a las nuevas amenazas y vulnerabilidades.

La adopción de la norma ISO 27001 en un SOC no solo fortalece la seguridad de la información, sino que también establece un marco robusto para la gestión continua de los riesgos y la mejora de los controles de seguridad. El compromiso de la alta dirección y la asignación de recursos adecuados son vitales para el éxito de la implementación. Definir el alcance, realizar evaluaciones de riesgos, desarrollar políticas y procedimientos, e implementar controles de seguridad garantizan una protección integral de los activos de la organización. Las auditorías internas, la certificación externa y un enfoque de mejora continua aseguran que el SGSI del SOC permanezca eficaz y adaptable frente a nuevas amenazas y vulnerabilidades.

Propuesta Solución SIEM

La seguridad de la información es un pilar clave para cualquier organización en la era digital. Con el creciente número de amenazas cibernéticas, las soluciones SIEM se han convertido en un componente esencial para la detección y prevención de incidentes de seguridad. El benchmarking, o la comparación de prácticas y rendimientos con SIEM y IDS/IPS de referencia, es una estrategia útil para identificar mejoras y adoptar mejores prácticas, lo que resulta ideal para las PYMES que buscan robustez y eficiencia sin incurrir en grandes costos. A través del análisis de plataformas como Rapid7 Insight Platform, LogRhythm CDR Stack, Exabeam y Wazuh, se destaca como cada una de estas herramientas puede mejorar la seguridad, la gestión de incidentes y la protección de datos dentro de una organización. Wazuh, en particular ofrece una solución versátil, adaptable y de código abierto, posicionándose como una opción poderosa para las PYMES que desean fortalecer sus defensas cibernéticas de manera efectiva y económica.

Las soluciones SIEM seleccionadas por ser de licenciamiento GPL (General License Public) la cual es utilizada originalmente por la Free software Foundation (FSF) y es la licencia más utilizada en la actualidad para el software libre, se escogen este tipo de licenciamiento debido que es gratuita su instalación y utilización para las empresas Pymes, las soluciones de ciberseguridad que fueron seleccionados son los siguientes:

Rapid7 Insight Platform: Cuenta con controles continuos y orientación estratégica que permite adelantarse a los ataques, permite orientar al equipo de ciberseguridad para conectarse en las amenazas que importan, cuenta con panel de vulnerabilidades, seguridad de aplicaciones, detección, inteligencia de amenazas y respuestas, así como la posibilidad de automatizar procesos (Rapid7, n.d.).

LogRhythm CDR Stack: Permite realizar análisis intuitivos y de alto rendimiento, así como la recopilación y mejora de flujo de trabajo de respuesta a incidentes, con su sitema de de detección de amenazas LogRhythm SIem ayuda a su organización a descubrir amenazas, mitigar ataques y cumplir con los mandatos de la organización (Secreto, 2024).

Exabeam: Ofrece un paquete de software SIEM que se basa en un Siem-Cloud, incluye procesamiento fuera de sitio con recopilación de datos, Según Exabeam (n.d.) cuenta con administrador de registros que permite asegurar el cumplimento de estándar de privacidad de datos mediante el establecimiento de un registro de auditoría.

Wazuh: SIEM con robustos módulos en la mitigación y reconocimiento de incidencias en la red de la organización, cuenta con los módulos de protección en tiempo real que permite la respuesta rápida a incidencias o alertas, Según Wazuh (n.d.) con su robusto SIEM permite monitorear, detectar y alertar eventos de seguridad e incidentes, cuenta con la posibilidad de administrar todo el SIEM desde la nube.

En la siguiente tabla se analizan las principales funciones ventajas y desventajas de los principales SIEM de software libre del mercado actualmente, la cual permite ver los puntos fuertes de cada software para realizar una elección más fácil y adecuada.

Tabla 1

Comparativa de las Principales Ventajas y Desventajas de los SIEM más Populares de Software Libre

Siem	Funciones	Ventajas	Desventajas
Rapid7	**Monitoreo Continuo:** Ofrece monitoreo continuo de seguridad mediante su plataforma InsightIDR. **Detección de Amenazas:** Utiliza	Agente local que recopila datos y los comparte en la nube, el UEBA establece una línea base de actividad normal por busca	Implementa defensas a través de herramientas de terceros.

Siem	Funciones	Ventajas	Desventajas
	análisis de comportamiento de usuarios y entidades (UEBA) para identificar actividades anómalas. **Respuesta a Incidentes:** Incluye capacidades de respuesta a incidentes con playbooks automatizados. **Gestión de Vulnerabilidades:** Integración con Nexpose para la gestión de vulnerabilidades. **Automatización:** Soporta automatización de tareas de seguridad con InsightConnect (Rapid7, s. f.).	de tráfico, Detección de anomalías por análisis de comportamiento de ataques. **Integración Completa:** Facilita la integración con múltiples herramientas y plataformas. **Automatización Avanzada:** Reducción de tareas repetitivas y mejora en la respuesta a incidentes. **Interfaz Intuitiva:** Interface amigable y fácil de usar para la administración de seguridad (Rapid7, s. f.).	**Coste Elevado:** Puede ser costoso para organizaciones más pequeñas. **Curva de Aprendizaje:** La configuración y uso de todas las funcionalidades puede requerir tiempo y capacitación.
LogRhythm	**Monitoreo de Red:** Ofrece visibilidad completa de la red y los puntos finales. **Detección de Amenazas:** Utiliza machine learning para detectar amenazas en tiempo real. **Respuesta a Incidentes:** Incorpora un sistema de respuesta a incidentes con capacidades de automatización.	**Detección Precisa:** Capacidades avanzadas de machine learning para detección precisa de amenazas. **Automatización Integrada:** Fuerte enfoque en la automatización de la respuesta a incidentes. **Flexibilidad:** Amplias opciones de personalización y flexibilidad en la configuración.	**Complejidad:** Puede ser complejo de implementar y mantener. **Requisitos de Recursos:** Requiere recursos significativos de hardware y personal capacitado. Alto nivel para integrar sus otras herramientas

Siem	Funciones	Ventajas	Desventajas
	Gestión de Logs: Gestión centralizada y análisis de logs para mejorar la detección de amenazas. **Inteligencia de Amenazas:** Integración con múltiples fuentes de inteligencia de amenazas (Logrhythm, s.f).	Log en vivo que recopila y consolidad archivos de registro en búsqueda de amenazas, cuenta con ejecución de paquetes de red SaaS (Logrhythm, s.f).	de seguridad (Logsign, s. f.).
Exabeam	**Análisis de Comportamiento:** Focalizado en el análisis de comportamiento de usuarios y entidades (UEBA). **Detección y Respuesta:** Capacidades de detección y respuesta a incidentes con análisis automatizado. **Gestión de Incidentes:** Incluye herramientas para la gestión de incidentes y la automatización de respuestas. **Integración de SIEM:** Se integra con múltiples sistemas de información y gestión de eventos de seguridad (SIEM) (Exabeam, s. f.).	**Especialización en UEBA:** Fuerte en el análisis de comportamiento, útil para detectar amenazas internas. **Integración Fácil:** Fácil integración con sistemas SIEM existentes. **Escalabilidad:** Escalable para diferentes tamaños de organizaciones. UEBA para línea de base de actividad basada en IA, recopila datos desde la instancia local y permite respuestas automatizadas (Exabeam, s. f.).	**Costo:** Puede ser costoso, especialmente para pequeñas y medianas empresas. **Dependencia de Datos:** La efectividad depende de la calidad y cantidad de datos disponibles para análisis. Incluye de manera excesiva opciones de casos de uso que dificulta su implementación.
Wazuh	**Monitoreo de Seguridad:** Ofrece monitoreo de seguridad en tiempo real y detección de intrusos.	**Costo:** Gratuito y de código abierto, ideal para	**Curva de Aprendizaje:** Requiere conocimiento técnico para

Siem	Funciones	Ventajas	Desventajas
	Gestión de Vulnerabilidades: Escaneo y gestión de vulnerabilidades con informes detallados. **Cumplimiento Normativo:** Herramientas para el cumplimiento de normativas como GDPR y PCI DSS. **Open Source:** Plataforma de código abierto que permite personalización y extensibilidad. **Análisis de Logs:** Recolección y análisis de logs para identificar amenazas (Wazuh, s. f.).	organizaciones con presupuestos limitados. **Flexibilidad:** Altamente configurable y personalizable. **Comunidad Activa:** Gran soporte de la comunidad y actualizaciones frecuentes. (Wazuh, s. f.).	configuración y mantenimiento. **Menor Soporte Comercial:** Menos soporte comercial comparado con soluciones propietarias. Agentes multiexplorador se deben instalar desde línea de comandos de comandos (Peerspot, s. f.).

Nota. Elaboración propia

El benchmarking en los SIEM permite a las organizaciones comparar su desempeño y prácticas con otros softwares de referencia para identificar oportunidades de mejora y adoptar buenas prácticas. Al seleccionar SIEM con licenciamiento GPL, las empresas PYMES pueden beneficiarse de soluciones de software libre sin incurrir en costos de instalación y uso. Las plataformas seleccionadas, como Rapid7 Insight Platform, LogRhythm CDR Stack, Exabeam y Wazuh, ofrecen capacidades avanzadas de detección y respuesta a amenazas, gestión de incidentes, y cumplimiento de normativas. Estas herramientas proporcionan una combinación de monitoreo en tiempo real, análisis de datos, automatización de procesos y soporte en la nube, lo

que fortalece la seguridad de la información y la resiliencia ante ciberataques en las organizaciones.

La elección de un SIEM adecuado depende de las necesidades específicas de la organización. Rapid7 y LogRhythm CDR Stack son ideales para empresas que buscan soluciones robustas con capacidades avanzadas de automatización y análisis de amenazas, aunque a un costo más elevado. Exabeam destaca por su especialización en análisis de comportamiento y facilidad de integración con sistemas SIEM, pero también tiene un costo significativo. Wazuh, por otro lado, es una excelente opción para organizaciones con presupuestos limitados que buscan flexibilidad y una solución personalizable de código abierto.

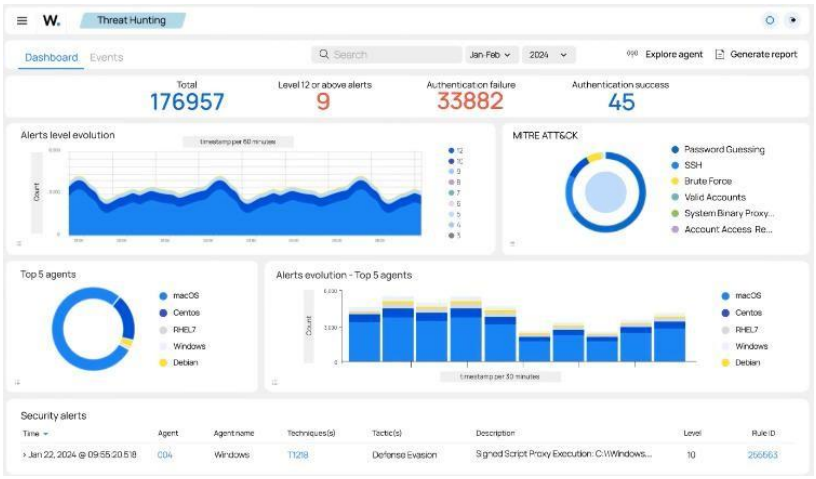
Wazuh es una plataforma de seguridad de código abierto que incluye capacidades de monitorización, detección y respuesta a incidentes, su instalación sencilla ya que la propia plataforma otorga la imagen del sistema operativo del servidor para ser instalada asi como los agentes para ejecutar en los equipos a analizar además de otras características:

Monitoreo y detección de amenazas: Wazuh permite la recolección y análisis de registros de eventos de seguridad en tiempo real, de acuerdo a la figura 3 se observa la interfaz muy intuitiva y grafica que permite monitorear los registros de sistemas, aplicaciones y dispositivos de red, y aplicar reglas predefinidas o personalizadas para detectar patrones y comportamientos sospechosos.

En la figura se observa el Dashboard de Wazuh con su interfaz grafica en donde se observa las alertas.

Figura 3

Dashboard Wazuh



Nota. Recuperado de: https://wazuh.com/

Gestión de incidentes: Wazuh facilita la gestión de incidentes al enviar alertas y notificaciones en tiempo real cuando se detectan eventos de seguridad relevantes. Estas alertas pueden ser integradas con sistemas de gestión de tickets o plataformas de colaboración para una respuesta efectiva como se aprecia en el grafico 4 como clasifica los incidentes para su gestión.

En la Figura se encuentra el panel de detección de vulnerabilidades de Wazuh.

Figura 4

Panel de Actividad

Nota. Recuperado de: https://wazuh.com/

Análisis forense: La plataforma Wazuh proporciona capacidades de análisis forense al recopilar y almacenar de forma segura los registros y datos relevantes de eventos de seguridad. Esto permite realizar investigaciones posteriores a un incidente y extraer información valiosa para el análisis y la mejora continua de la seguridad.

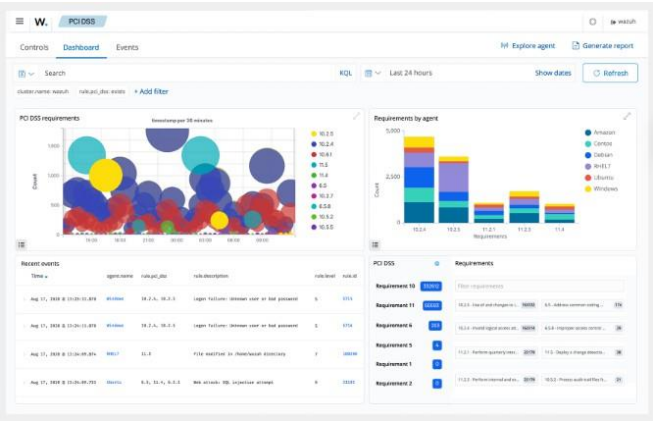
Integración con otras herramientas: Wazuh se puede integrar con otras soluciones y herramientas de seguridad, como sistemas de detección de intrusiones (IDS/IPS), sistemas de prevención de pérdida de datos (DLP) y sistemas de gestión de vulnerabilidades. Esto permite una visión más amplia de la seguridad de la organización y una respuesta más efectiva, en el grafico 5 se observa la vista grafica de los agentes instalados en los End-points y su compatibilidad con distintos sistemas operativos.

Reglas y políticas personalizables: Wazuh ofrece una amplia variedad de reglas predefinidas para la detección de amenazas comunes. Además, permite personalizar y crear reglas específicas para adaptarse a las necesidades y características únicas de la organización.

En la figura a continuación se observa la información que arroja desde el módulo de los agentes como el sistema operativo y distintos logs.

Figura 5

Vista agentes Instalados



Nota. Recuperado de: https://wazuh.com/platform/siem/

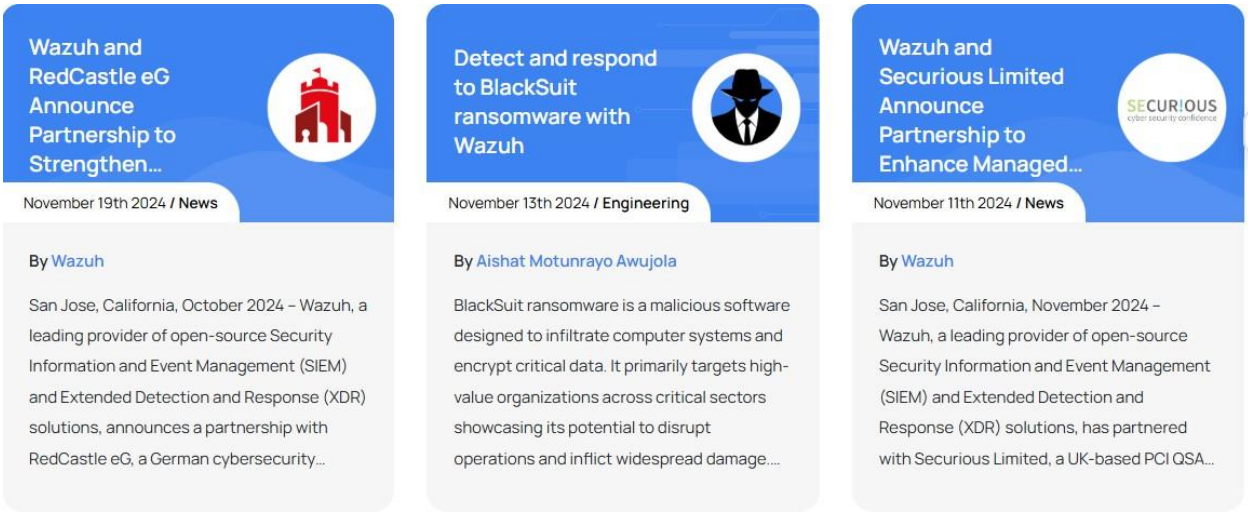
Paneles de control y visualización de datos: Wazuh proporciona paneles de control y visualización de datos que permiten supervisar y analizar de manera eficiente la información de seguridad. Estos paneles brindan una vista panorámica de los eventos de seguridad, alertas, tendencias y métricas clave para una toma de decisiones informada.

Comunidad activa y soporte: en el Grafico 6 se observa la web de la comunidad activa de usuarios y desarrolladores, lo que brinda acceso a recursos, documentación, foros y actualizaciones frecuentes. Además, existen opciones de soporte comercial disponibles para aquellos que requieran asistencia adicional.

En la figura se evidencia la comunidad de Wazuh para soporte y novedades así como sus partners.

Figura 6

Comunidad Wazuh



Nota. Recuperado de: https://wazuh.com/blog/

Instalación e Implementación

Su arquitectura modular incluye componentes como Wazuh Manager, Elasticsearch y Kibana, que trabajan en conjunto para analizar datos provenientes de agentes instalados en diferentes sistemas operativos.

Esta monografía detalla el proceso de instalación y configuración de un servidor Wazuh en una máquina virtual basada en Linux, así como la integración de un agente en un sistema operativo Windows. Asimismo, se explora la interacción entre los distintos componentes del SIEM de Wazuh, desde la recopilación de eventos por los agentes, su procesamiento y almacenamiento en Elasticsearch, hasta la visualización en tiempo real mediante la interfaz gráfica de Kibana.

El objetivo principal es proporcionar una guía práctica que no solo facilite la implementación de Wazuh, sino que también demuestre su capacidad para gestionar y responder a incidentes de seguridad en entornos heterogéneos, promoviendo así una cultura de ciberseguridad proactiva. La instalación puede ser realizada en diversos entornos, incluyendo on-premises, en la nube o en una configuración híbrida, en el grafico 7 se observan sus requerimientos de Hardware son relativamente poco exigentes.

Figura 7

Requerimientos Wazuh

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

Nota. Recuperado de: https://documentation.wazuh.com/current/quickstart.html

En este trabajo se realizará la instalación en una distribución Ubuntu Desktop 24.04 con 8 Gigas de memoria Ram, 100 Gigas de disco duro y conexión a internet.

Para la instalación es necesario ejecutar con permisos los siguientes comandos:

Descarga e instale la clave GPG del repositorio:

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/share/keyrings/wazuh-keyring.gpg

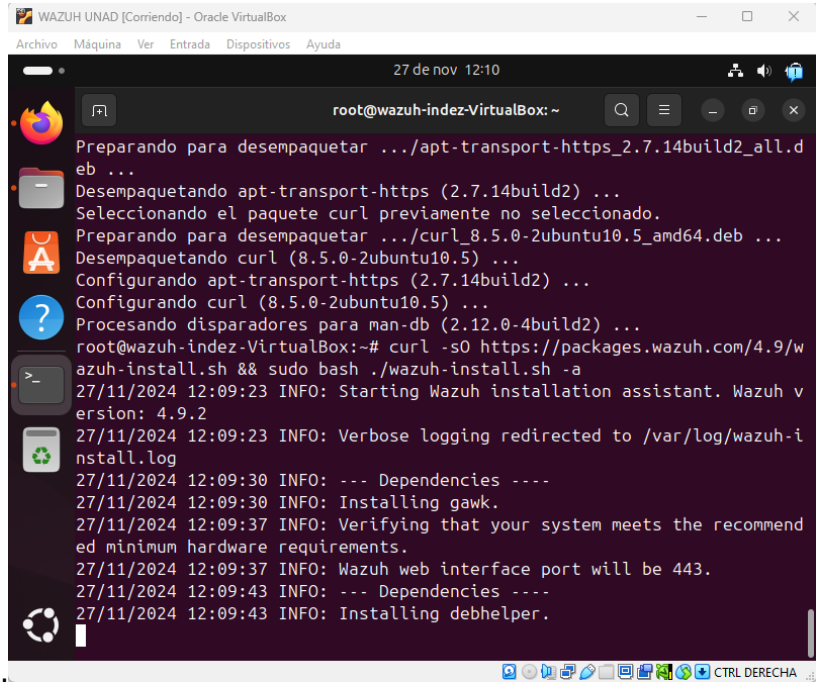
Inicio del repositorio:

echo "deb [signed-by=/usr/share/keyrings/wazuh-keyring.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list

En la figura a continuación se visualiza la ejecución de los comandos para instalar los repositorios de Wazuh.

Figura 8

Instalación Repositorios



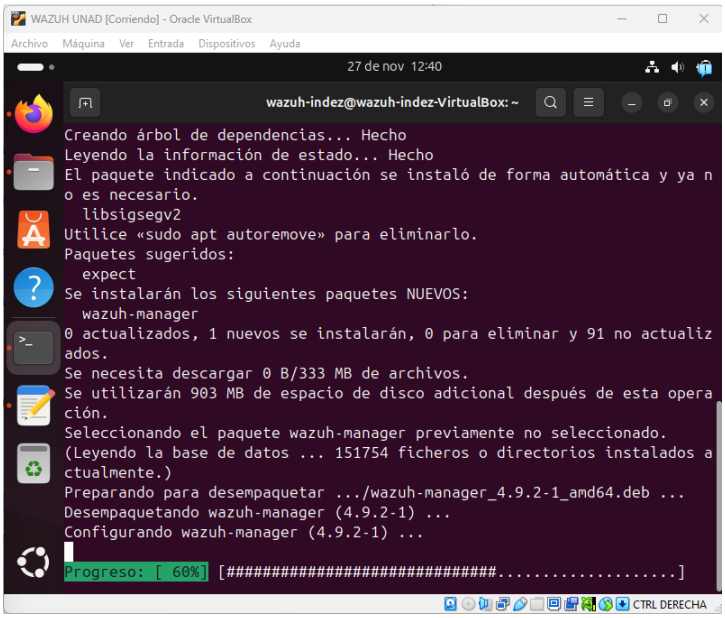
Nota. Elaboración propia

Instalar el servicio. sudo apt install wazuh-manager -y

Se observa en la figura como avanza la descarga y posterior instalación de los paquetes de Wazuh, de manera opcional se puede eliminar el paquete descargado para no consumir espacio en el disco el tiempo de descarga depende de la conexión a internet.

Figura 9

Instalación Wazuh Manager



Nota. Elaboración propia

Instalar Elasticsearch el cual se utiliza para almacenar y buscar los datos procesados por Wazuh, para agregar el repositorio hay que agregar el siguiente comando y su posterior ejecución.

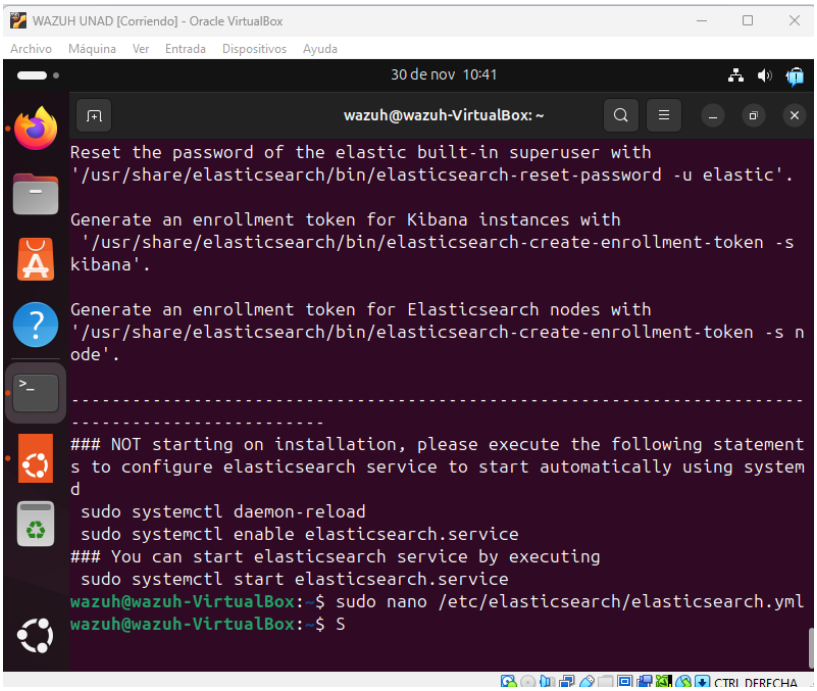
curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic-keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/elastic-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

Con los commandos sudo apt update y sudo apt install elasticsearch -y se visualiza la correcta instalación y ejecución de Elasticsearch cabe aclarar que hay que ejecutar el servicio ya que este por defecto esta detenido como lo muestra la figura 10.

Figura10

Instalación Elasticsearch

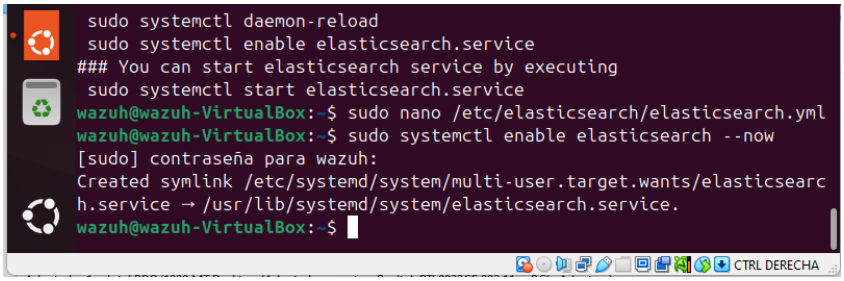


Nota. Elaboración propia

Ejecutar el siguiente comando como se observa en la figura 11.

Figura11

Ejecución Servicio Elasticsearch



Nota. Elaboración propia

Instalar Filebeat que se utiliza para enviar los logs de Wazuh Manager a Elasticsearch con el siguiente comando instalar y proceder habilitar dicho modulo.

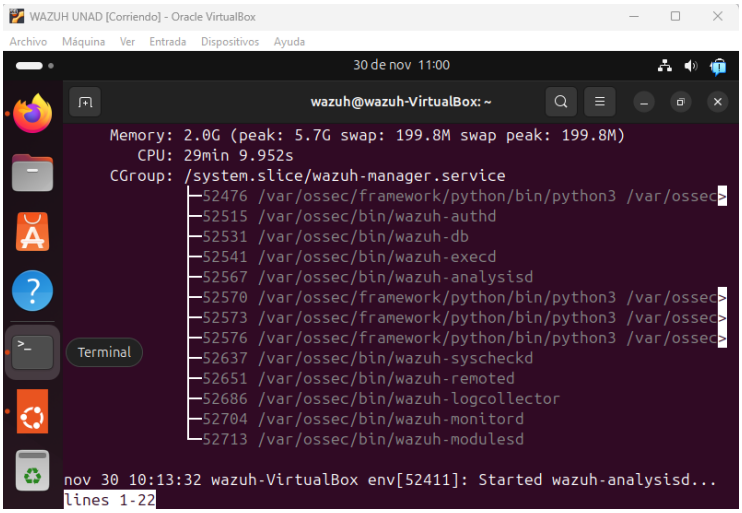
sudo apt install filebeat -y

sudo filebeat modules enable wazuh

En la figura 12 se observa la instalación de los paquetes de Filebeat

Figura12

Instalación Filebeat



Nota. Elaboración propia

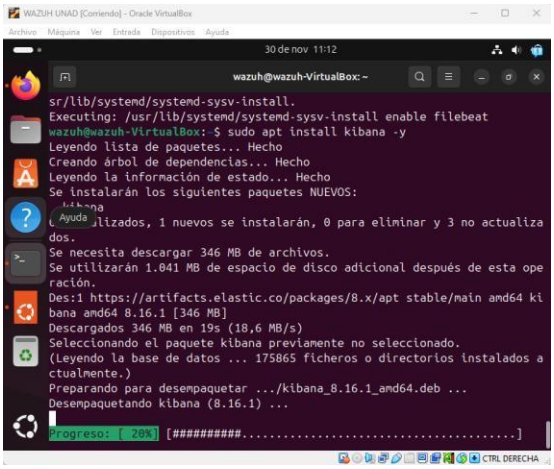
Instalar Kibana que proporciona la interfaz gráfica para monitorear y analizar los datos de Wazuh para lo cual ejecutar el siguiente comando:

Sudo apt install kibana -y

Si todo esta correcto como se visualiza en la imagen iniciara la descarga e instalación de Kibana, siempre ejecutar los comandos de instalación o ejecución de daemons debe ser con el usuario administrador que en este caso está el por defecto sudo.

Figura 13

Instalación Kibana 1



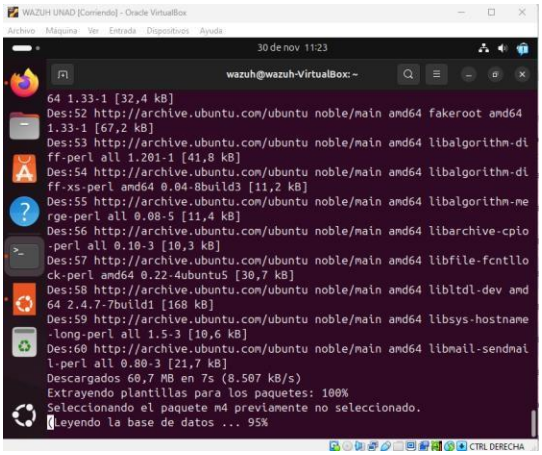
Nota. Elaboración propia

Instalar el plugin de Wazuh en Kibana para la comunicación y administración de los módulos desde el entorno gráfico con los siguientes comandos:

Sudo apt install wazuh-kibana -app -y Sudo systemctl status kibana, continua la descarga e instalación de sus componentes así como la comprobación del servicio de Kibana como se observa en la figura 14.

Figura 14

Instalación Kibana 2

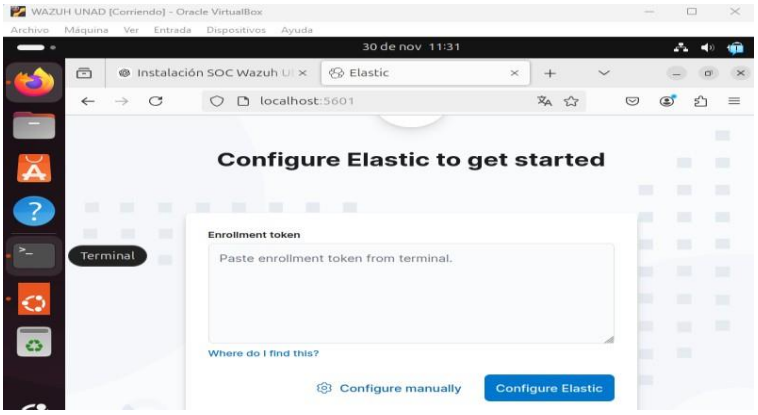


Nota. Elaboración propia

Como se observa en la figura 15 abrir Ventana del navegador y en el localhost configurado previamente con el puerto 5601 y debe cargar la siguiente ventana.

Figura 15

Instalación Kibana 3

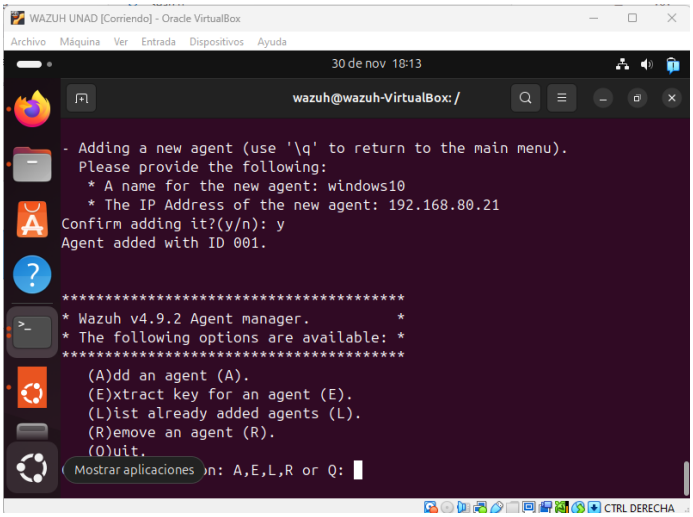


Nota. Elaboración propia

En el servidor de Linux ingresar a la administración de agentes para añadir el equipo, Sudo /var/ossec/bin/mange_agents, En la imagen a continuación se observa en el servidor de Wazuh el anclaje de un agente.

Figura 16

Validación Agente

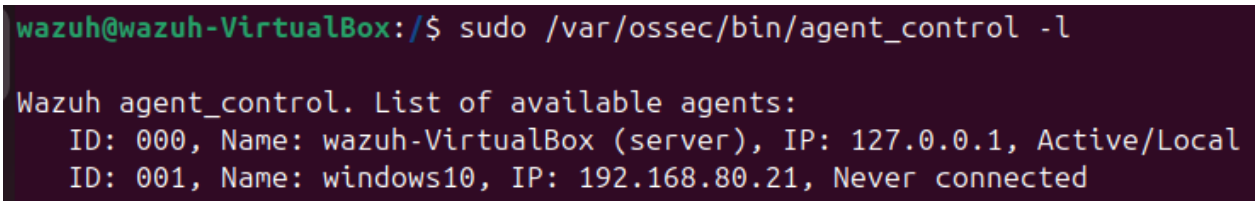


Nota. Elaboración propia

Ahora Se puede visualizar el Endpoint desde el servidor como se observa en la imagen a continuación.

Figura 17

Instalación Kibana 4



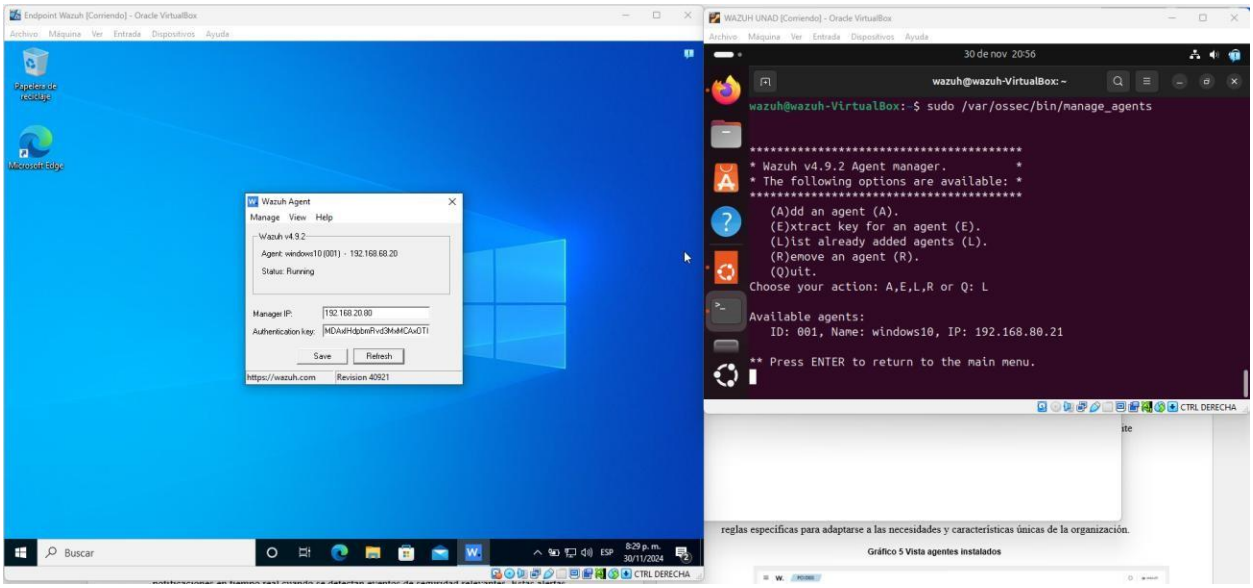
Nora. Elaboración propia

En los equipos a monitorear instalar el agente y anclar con la dirección IP del servidor Ahora es posible observar la interacción entre el servidor y el agente una vez cargado el agente

esto se puede comprobar en la máquina de Endpoint el agente Wazuh se encuentra ejecutado y con la Key cargada correctamente como se puede apreciar en la figura 18.

Figura 18

Validación Operación SIEM



Nota. Elaboración propia

Los Componentes Principales de Wazuh Incluyen

- Manager: El corazón del sistema, responsable de la recopilación y análisis de datos de seguridad.
- Agents: Desplegados en los dispositivos finales para monitorear la actividad y enviar datos al manager.
- Elastic Stack: Utilizado para el almacenamiento, búsqueda y visualización de datos.
- Dashboard: Interfaz gráfica basada en Kibana para visualizar y gestionar alertas y eventos de seguridad.

La instalación puede realizarse mediante scripts automatizados proporcionados por Wazuh o manualmente para configuraciones más específicas.

Configuración y Personalización

Una vez instalado, es necesario configurar Wazuh para adaptarse a las necesidades específicas de la organización. Esto incluye:

Políticas de Monitoreo: Definir qué actividades deben ser monitoreadas y cómo deben ser reportadas.

Integración con Otros Sistemas: Configurar integraciones con otros sistemas de TI y seguridad, como SIEM, firewalls y soluciones de gestión de identidades.

Alertas y Notificaciones: Configurar las reglas de alerta para detectar actividades sospechosas y notificar a los equipos correspondientes.

Mantenimiento y Actualización

El mantenimiento de Wazuh implica la actualización regular del software para aprovechar las nuevas funcionalidades y correcciones de seguridad. También incluye la revisión y ajuste continuo de las políticas de seguridad y la respuesta a incidentes basados en las alertas generadas.

Mecanismo de Acción de los Componentes de Wazuh

El manager es el componente central de Wazuh, encargado de recibir y analizar los datos de los agentes desplegados en los endpoints. Utiliza reglas predefinidas y personalizables para correlacionar eventos y generar alertas sobre actividades sospechosas.

Análisis de Logs: El manager puede analizar logs de diversos tipos, incluyendo logs de sistemas operativos, aplicaciones y dispositivos de red.

Correlación de Eventos: Utiliza reglas para correlacionar eventos y detectar patrones que indiquen posibles amenazas.

Generación de Alertas: Basado en las reglas configuradas, el manager genera alertas que pueden ser visualizadas en el dashboard o enviadas a otros sistemas de respuesta a incidentes.

Agents

Los agentes son software ligero que se instala en los endpoints para monitorear actividades específicas y enviar datos al manager.

Monitoreo de Integridad de Archivos: Detecta cambios no autorizados en archivos y carpetas críticos.

Detección de Malware: Monitorea la presencia de malware utilizando firmas y heurísticas.

Análisis de Logs Locales: Recopila y envía logs locales al manager para su análisis centralizado.

Elastic Stack, compuesto por Elasticsearch, Logstash y Kibana, es utilizado para el almacenamiento, búsqueda y visualización de los datos de seguridad.

Elasticsearch: Almacena y permite la búsqueda rápida de grandes volúmenes de datos.

Logstash: Procesa y transforma los datos antes de enviarlos a Elasticsearch.

Kibana: Proporciona una interfaz gráfica para visualizar y analizar los datos almacenados en Elasticsearch.

Dashboard

El dashboard de Wazuh, basado en Kibana, permite a los usuarios visualizar y gestionar las alertas y eventos de seguridad.

Tomado de: https://documentation.wazuh.com/current/installation-guide/wazuh-server/index.html

Visualización de Alertas: Muestra alertas en tiempo real con detalles sobre las actividades sospechosas.

Análisis de Datos: Herramientas de análisis que permiten profundizar en los datos para identificar la causa raíz de los incidentes.

Reportes de Conformidad: Genera reportes para demostrar el cumplimiento con diversas normativas y estándares de seguridad.

La selección de un SIEM adecuado es fundamental para garantizar una defensa efectiva contra las crecientes amenazas de ciberseguridad, al optar por soluciones de código abierto con licencia GPL, como Wazuh, las organizaciones PYMES pueden beneficiarse de una plataforma robusta y flexible sin costos prohibitivos. En conjunto con otras plataformas como Rapid7, LogRhythm y Exabeam, el benchmarking de las principales SIEM gratuitas del mercado permite adoptar soluciones que se ajusten a las necesidades y desafíos específicos de cada empresa. De esta manera, las organizaciones pueden fortalecer su postura de seguridad, mejorar la resiliencia ante ataques cibernéticos y garantizar la protección integral de sus sistemas de información.

La plataforma de seguridad de código abierto Wazuh ofrece una solución integral para la monitorización, detección y respuesta a incidentes de seguridad. Su facilidad de instalación, gracias a la provisión de imágenes del sistema operativo y agentes para los equipos a analizar, simplifica su despliegue en las organizaciones.

Una de las principales ventajas de Wazuh es su capacidad para monitorear y analizar eventos en tiempo real, lo que permite detectar comportamientos sospechosos antes de que representen un riesgo crítico para la organización (OSINT-PH, 2024). Además, su sistema

avanzado de detección de intrusiones y correlación de eventos le permite identificar ataques de manera temprana, brindando a las empresas la posibilidad de actuar con rapidez ante cualquier incidente (OSINT-PH, 2024). Esto es posible gracias a que en una sola plataforma de código abierto se tiene el monitoreo y análisis de eventos (SIEM) y las funciones de IDS/IPS gracias a sus Endpoint permite contener la posible amenaza para que no escale por la infraestructura esto es posible gracias a sus respuestas automáticas lo que genera un valor agregado a la herramienta y permite a los encargados de la ciberseguridad centrarse en demás tareas de análisis.

Finalmente, al ser una solución gratuita y de código abierto, Wazuh se convierte en una opción accesible para cualquier organización que desee fortalecer su seguridad informática sin comprometer su presupuesto (OSINT-PH, 2024). Su flexibilidad y capacidad de integración con otras tecnologías lo hacen una herramienta imprescindible para el resguardo de la información en las Pymes de Bogotá y en cualquier otra parte del mundo.

Según Wazuh (n.d.), la integración con el marco MITRE ATT&CK permite mapear las alertas generadas a tácticas y técnicas específicas, proporcionando una mejor comprensión de las amenazas y facilitando el desarrollo de estrategias de mitigación efectivas y para su soporte cuenta con una comunidad, foro y ayudas en línea muy útil en caso de requerir soporte.

Propuesta de Metodología para el Fortalecimiento de la Ciberseguridad

El diseño de una estrategia efectiva para la detección y prevención de intrusos en redes organizacionales es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información. Este capítulo desarrolla una propuesta metodológica alineada con el cuarto objetivo de este trabajo: fortalecer la ciberseguridad en las PyMES mediante la implementación de un SIEM basado en Wazuh y alineado con la norma ISO/IEC 27001. La metodología propuesta se compone de seis fases, cada una estructurada con objetivos, actividades específicas

y herramientas tecnológicas que permiten a las PyMES mejorar su postura de seguridad de forma gradual, ordenada y adaptable a sus recursos limitados.

Evaluación Inicial y Planificación

Objetivo: Diagnosticar el estado actual de la ciberseguridad y establecer los lineamientos iniciales del proyecto.

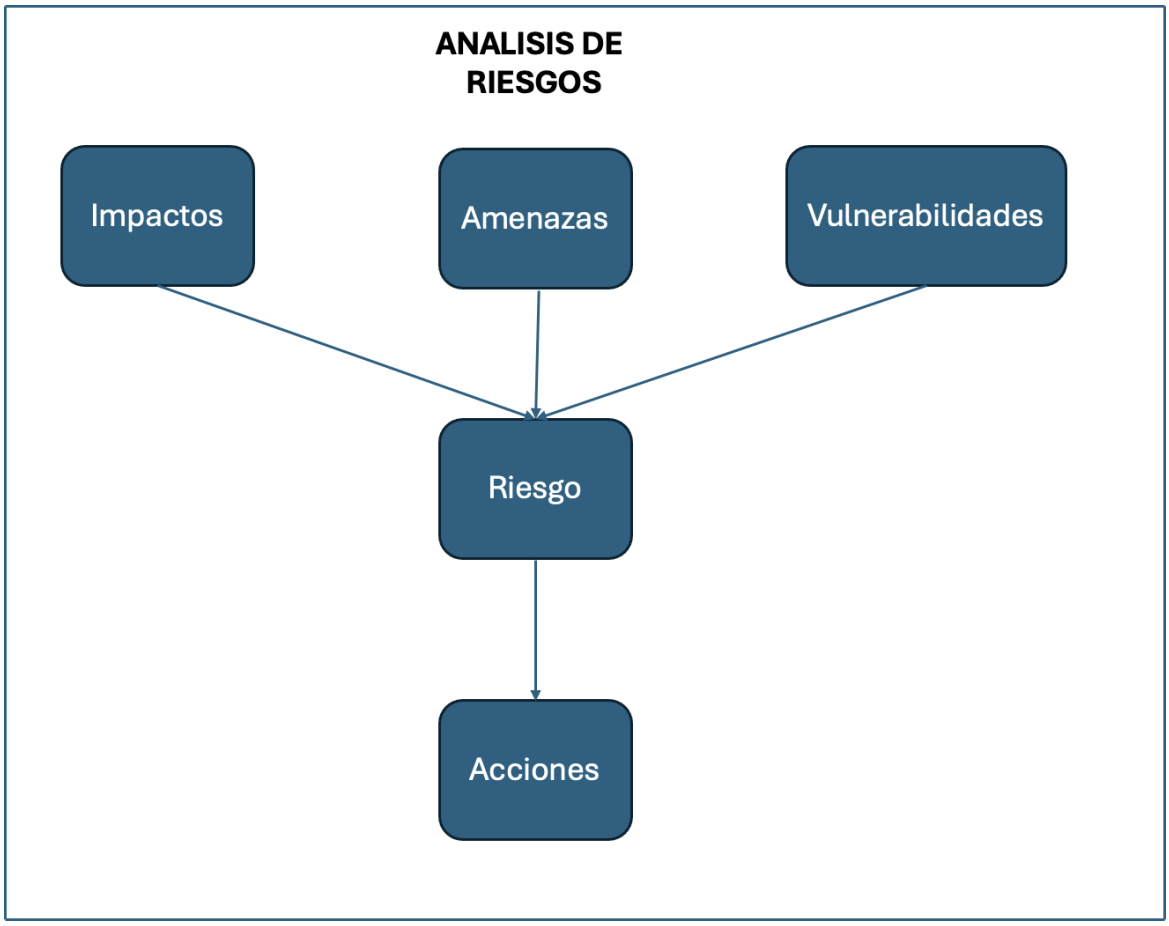
Actividades:

- Evaluación de riesgos: Identificación de activos, amenazas, vulnerabilidades, impactos y probabilidad, siguiendo la ISO 27001.
- Definición del alcance: Determinar los sistemas y activos que serán monitoreados por el SIEM.
- Planificación del proyecto: Establecer cronograma, recursos, presupuesto y responsables.

En la Figura se observa el análisis de riesgos y según su naturaliza su acción a tomar.

Figura 19

Análisis de Riesgo



Nota. Elaboración propia

la norma ISO/IEC 27001 establece que es fundamental definir el contexto de la organización, identificar las partes interesadas y determinar el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) ya que al tener el inventario de los activos digitales y así como definir su importancia y criticidad para la continuidad del negocio.

La identificación de activos constituye el primer paso fundamental en cualquier estrategia de gestión de riesgos de seguridad de la información. En esta etapa, se busca reconocer y

clasificar todos los elementos que poseen valor para la organización y que, por lo tanto, deben ser protegidos frente a posibles amenazas. En el contexto de las pequeñas y medianas empresas (PyMEs), este proceso adquiere una relevancia estratégica, ya que los recursos suelen ser limitados y es necesario priorizar de manera efectiva la protección de los activos más críticos.

Para llevar a cabo esta actividad de forma estructurada, se propone la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) la cual permite identificar los activos en diferentes niveles desde la información y los servicios clave, hasta la infraestructura tecnológica y los recursos humanos, evaluando su importancia en función de los criterios de confidencialidad, integridad y disponibilidad (CIA). A través de este enfoque se facilita la priorización de los activos permitiendo enfocar los esfuerzos de seguridad en aquellas áreas que representan un mayor impacto para la continuidad del negocio.

Según Pirani Risk (s. f.), la metodología MAGERIT permite identificar, analizar y tratar riesgos en los sistemas de información a través de un enfoque estructurado y adaptable por lo cual es esencial no solo para establecer controles adecuados, sino también para definir el alcance del sistema de gestión de seguridad y alimentar eficazmente herramientas como los sistemas de información y eventos de seguridad (SIEM), como Wazuh, que serán implementados en fases posteriores de esta propuesta metodológica.

Identificación y Priorización de Activos

Según MAGERIT, los activos se pueden clasificar en diferentes niveles jerárquicos. En el entorno de una PyME, como se observa en la tabla 2 esta clasificación puede adaptarse de la siguiente forma:

Tabla 2

Comparativa Clasificación de Activos Según MAGERIT

Categoría	Subcategorías	Ejemplos
Información	Datos críticos, confidenciales, operativos	Base de datos de clientes, contratos
Servicios	Servicios TIC, aplicaciones empresariales	Sistema contable, sitio web de ventas
Aplicaciones	Software de gestión, ERP, CRM	Software de facturación, Software de nomina
Infraestructura	Servidores, redes, estaciones de trabajo	Servidor de archivos, Switch, routers
Personas	Usuarios clave o VIP, administradores de sistemas	Gerente de TI, operador de sistemas, Gerente de ventas.
Instalaciones	Oficinas, datacenter	Cuarto de servidores, redes eléctricas

Nota. Elaboración propia

Criterios de Valoración de Activos

Para establecer una prioridad, cada activo se evalúa según tres dimensiones clave del modelo CIA: Confidencial (C) ¿Qué tan crítico es mantener la información del activo inaccesible a personas no autorizadas? Integridad (I) ¿Qué nivel de impacto tendría una alteración no autorizada de su contenido? Disponibilidad (D) ¿Qué consecuencias tendría la falta de acceso al activo en el momento requerido?

Se puede usar una escala de valoración de 1 (bajo) a 5 (crítico) como se aprecia en la siguiente tabla.

Tabla 3

Ejemplo de Matriz de Valoración de Activos

Activo	Confidencialidad	Integridad	Disponibilidad	Valor total (c+i+d)	Prioridad
Base de datos de clientes	5	5	4	14	Alta
Servidor de archivos	4	4	5	13	Alta
Sistema contable	5	4	3	12	Alta
Página web institucional	3	3	4	10	Mediana
PC del área comercial	2	3	3	8	Media
Impresora compartida	1	1	2	4	Baja

Nota. Elaboración propia

Documentación del Proceso

Según Baloo Security (s. f.), el inventario de activos es un paso fundamental en la metodología MAGERIT, ya que permite identificar los elementos clave para la operación y evaluar sus riesgos, incluyendo:

- Identificador único del activo.
- Nombre y descripción.
- Responsable.
- Clasificación según categoría.
- Valoración CIA.

- Justificación del valor asignado.
- Nivel de prioridad.
- Relación con otros activos (dependencias).

Esta documentación servirá de base para el análisis de riesgos posterior y facilitará la definición de controles específicos durante la implementación del SIEM.

Análisis de Riesgos y Amenazas

Una vez priorizados los activos de información, es necesario identificar y analizar los riesgos que podrían afectarlos, considerando las amenazas y vulnerabilidades existentes. Este análisis busca establecer el nivel de riesgo para cada activo, lo que servirá de insumo para definir controles adecuados en las siguientes fases del proyecto.

Identificación de Amenazas y Vulnerabilidades

En el contexto de las PyMEs, las amenazas más comunes pueden incluir según la naturaleza de la amenaza como lo muestra la tabla 4:

Tabla 4

Tabla de Amenazas

Categoría de amenaza	Ejemplos específicos
Errores Humanos	Configuración incorrecta, pérdida de contraseñas
Malware y ransomware	Infecciones por phishing o navegación insegura
Acceso no autorizado	Intrusiones externas, privilegios mal gestionados
Fallos técnicos	Corte eléctrico, caída del servidor, corrupción de datos
Desastres naturales	Incendios, inundaciones, sismos
Problemas físicos	Robo de equipos, acceso físico no controlado

Nota. Elaboración propia

Las vulnerabilidades típicas pueden ser:

- Software desactualizado.
- Falta de antivirus o sistemas de detección.
- Ausencia de políticas de contraseñas seguras.
- Infraestructura sin respaldo ni redundancia.
- Usuarios sin capacitación en seguridad.

Evaluación del Riesgo

Para evaluar el nivel de riesgo, se aplica la siguiente fórmula: Riesgo = Impacto × Probabilidad, usar una escala de 1 (bajo) a 5 (alto) para ambos factores, en la siguiente figura se observa un ejemplo práctico con amenazas muy comunes en el entorno de las Pymes.

Tabla 5

Tabla de Evaluación de Riesgos

Archivo	Amenaza	Vulnerabilidad asociada	Impacto	Probabilidad	Nivel de riesgo	Clasifica
Base de datos de clientes	Acceso no autorizado	Contraseñas débiles	5	4	20	Critico
Servidor de archivos	Ransomware	Falta de copias de seguridad	5	4	20	Critico
Sistema contable	Fallo técnico	Sin UPS, hardware obsoleto	4	3	12	Alto
Página web	Ataque DDoS	Sin protección perimetral	3	4	12	Alto
PC comercial	Malware por USB	Antivirus desactualizado	3	3	9	Medio

Impresora compartida	Acceso físico no controlado	Sin monitoreo de red	1	2	2	Bajo

Nota. Elaboración propia

Mapa de Calor de Riesgos

Al representar los niveles de riesgo en una matriz para facilitar la visualización y priorización se obtiene una mejor comprensión de la amenaza como se observa en la siguiente tabla:

Tabla 6

Tabla Calor de Riesgos

Probabilidad	1 (bajo)	2 (medio-bajo)	3 (medio)	4 (alto)	5 (critico)
5 (Muy alto)	5	10	15	20	25
4 (Alto)	4	8	12	16	20
3 (Medio)	3	6	9	12	15
2 (Bajo)	2	4	6	8	10
1 (Muy bajo)	1	2	3	4	5

Nota. Elaboración propia

Riesgos clasificados:

Crítico (≥ 16): Acción inmediata.

Alto (12–15): Acción en el corto plazo.

Medio (6–11): Evaluar y monitorear.

Bajo (≤ 5): Aceptable, monitoreo periódico.

Tratamiento de Riesgos y Definición de Controles

Una vez realizado el análisis de riesgos, es esencial establecer una estrategia de tratamiento que permita reducirlos a niveles aceptables. Esta etapa consiste en decidir qué hacer con cada riesgo identificado y qué controles implementar para mitigarlos, transferirlos, aceptarlos o evitarlos.

Actividades principales:

Clasificación de Riesgos por Prioridad. Con base en los niveles de riesgo obtenidos (por ejemplo, usando la matriz de impacto/probabilidad), se establecen los riesgos más críticos que requieren acción inmediata. Se consideran criterios como:

- Impacto en la continuidad operativa
- Cumplimiento normativo (e.g., Ley 1266 de 2008, Ley 1581 de 2012)
- Afectación a datos personales o confidenciales

Estrategias de Tratamiento de Riesgos. Las decisiones sobre los riesgos se agrupan en las siguientes opciones, según ISO 27005.

Mitigación: Aplicar controles para reducir la probabilidad o el impacto (por ejemplo, segmentación de red, respaldo automático, monitoreo con SIEM como Wazuh).

Transferencia: Contratar seguros o tercerizar ciertos servicios con cláusulas de seguridad (por ejemplo, servicios en la nube con garantías contractuales).

Aceptación: Para riesgos residuales cuyo impacto sea bajo o el costo del control sea superior al beneficio.

Eliminación o evitación: Cambiar procesos o tecnologías para eliminar completamente el riesgo.

Definición de Controles

Se seleccionan los controles aplicables del Anexo A de la ISO/IEC 27001:2022, agrupados por dominios como:

- Controles organizacionales (ej. políticas de seguridad)
- Controles técnicos (ej. cifrado, IDS/IPS, antivirus, control de acceso)
- Controles físicos (ej. CCTV, control de ingreso)
- Controles legales (ej. acuerdos de confidencialidad)

Se puede apoyar en el catálogo MAGERIT de medidas de seguridad y en herramientas como el Wazuh SIEM para automatizar parte del monitoreo y la respuesta a incidentes.

En la tabla 7 se observa el tratamiento de riesgos las cuales se seleccionaron siendo comunes en las organizaciones de menor tamaño.

Tabla 7

Tabla de Tratamiento de Riesgos

Riesgo identificado	Nivel de riesgo	Estrategia de tratamiento	Control propuesto	Responsable	Fecha límite
Acceso no autorizado a servidor	Alto	Mitigación	Implementar autenticación multifactor (MFA)	Área de TI	30/06/2025
Fuga de información por USB	Medio	Mitigación	Política de restricción de puertos y DLP	Seguridad Informática	15/07/2025
Fallo eléctrico en el CPD	Alto	Mitigación / Transferencia	UPS + contrato de mantenimiento externo	Infraestructura	01/07/2025

Malware por phishing	Alto	Mitigación	Capacitación + firewall + antimalware	Talento Humano + TI	15/08/2025

Nota. Elaboración propia

Diseño de la Arquitectura de Seguridad

Objetivo: Definir la infraestructura de red, roles, controles y mecanismos de protección.

Actividades:

Diseño del SIEM: Arquitectura basada en Wazuh, con integración de Elastic Stack para la gestión de logs y visualización.

Segmentación y monitoreo: Definición de zonas de red y controles de acceso.

Configuración de monitoreo centralizado desde Wazuh.

Defensa en profundidad: Asignación de roles mínimos, control de autenticación, detección de cambios no autorizados (FIM).

El diseño de la arquitectura de seguridad es una fase crítica dentro de cualquier estrategia de protección de la información, ya que establece la base sobre la cual se implementan los controles técnicos, administrativos y físicos.

Esta etapa busca definir no solo la topología de red y los roles dentro del sistema, sino también los mecanismos de vigilancia y protección activa de los activos tecnológicos. La implementación de un sistema SIEM como Wazuh, combinado con la plataforma Elastic Stack, permite diseñar una arquitectura capaz de recopilar, analizar y correlacionar eventos de seguridad en tiempo real, adaptándose a distintos tipos de activos como servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios en la nube.

Mediante un enfoque de defensa en profundidad, segmentación de red y control de accesos, esta etapa asegura que cada componente de la red esté protegido de acuerdo con su

criticidad, estableciendo las bases para una gestión de seguridad alineada con estándares internacionales como la ISO/IEC 27001.

Según Ključnikov, Mura y Sklenár (2019), existen 4 factores clave que influyen en el éxito de la gestión de la seguridad de la información en las PYMES, controles de seguridad, cumplimiento de la gestión de la seguridad de la información con las actividades de la empresa, conciencia organizacional y el apoyo de la gerencia. Por lo cual es fundamental que toda la organización se comprometa a cumplir con los objetivos propuestos, así como contar con la política de mínimo privilegios en las aplicaciones y accesos de la red para garantizar la aplicación de controles.

Diseño del SIEM con Wazuh y Elastic Stack

La arquitectura se construye sobre una base de Wazuh, integrando el stack de Elastic (Elasticsearch, Logstash y Kibana) para la gestión avanzada de registros y visualización de alertas. Esta estructura permite una consola centralizada desde donde se reciben, correlacionan y analizan eventos provenientes de múltiples tipos de activos, en la siguiente tabla se observa la clasificación de activos que se desea monitorear por el SIEM Wazuh, se seleccionaron tipos de activos comunes en las organizaciones Pymes.

Tabla 8

Clasificación de Activos A Monitorear y su Integración con Wazuh

Tipo de activo	Ejemplos	Monitoreo con Wazuh
Servidores	Windows Server, Linux, bases de datos	Instalación de agentes para análisis de logs, integridad de archivos, auditoria de accesos
Equipos de usuario	PC Windows, Mac, Linux	Agente local que recopila eventos de seguridad, actividad del usuario,

Tipo de activo	Ejemplos	Monitoreo con Wazuh
		software instalado y vulnerabilidades
Dispositivos de red	Routers, switches, firewalls	Integración vía syslog o SNMP para registros de eventos de red, tráfico inusual
Aplicaciones empresariales	ERP, CRM, mail, sitios web	Recolección de logs de apache, MySQL, Exchange, detección de anomalías.
Servicios en la nube	Google, Workspace, Microsoft 365, AWS, Azure	Monitoreo mediante APIs, syslog remoto para accesos externo, cambios de configuración
Bases de datos	PostgreSQL, MySQL, Oracle	Auditoria de queries, monitoreo de conexiones
Documentación sensible	Repositorios compartidos, carpetas de red	FMI, alertas por modificación o eliminación no autorizada

Nota. Elaboración propia

Segmentación de Red y Controles de Acceso

Se define la red en zonas segmentadas (por ejemplo: zona de usuarios, zona de servidores, DMZ), implementando controles como:

- Políticas de firewall y VLAN
- Monitorización de tráfico lateral entre segmentos
- Alertas ante conexiones no autorizadas entre zonas

Defensa en Profundidad y Roles Mínimos

Se aplican principios de mínimo privilegio, con control de roles y autenticación robusta (2FA).

Wazuh detecta accesos privilegiados inusuales, uso de cuentas por defecto o intentos de escalamiento de privilegios.

Control de integridad de archivos (FIM) permite detectar alteraciones en configuraciones clave del sistema.

Gracias a esta arquitectura, Wazuh permite monitorear en tiempo real todos los activos clave de la organización, correlacionando datos desde múltiples fuentes y proporcionando alertas tempranas sobre posibles incidentes, todo desde una única interfaz de gestión y visualización.

Implementación Técnica del SIEM

Objetivo: Instalar, configurar y poner en funcionamiento la solución de monitoreo.

Actividades:

- Despliegue de Wazuh: Instalación de manager, agentes en servidores y endpoints, integración con Elastic Stack.
- Pruebas funcionales: Validar alertas, correlación de eventos, trazabilidad y visibilidad en tiempo real.
- Detección de amenazas: Wazuh permite identificar movimientos laterales, comportamientos anómalos, uso indebido de privilegios y vulnerabilidades conocidas (mediante integración con NVD).

Mejores Prácticas en la Implementación

La implementación de herramientas de monitoreo y detección de amenazas como Wazuh debe ir más allá de una simple instalación técnica. Requiere planificación estratégica, gestión de

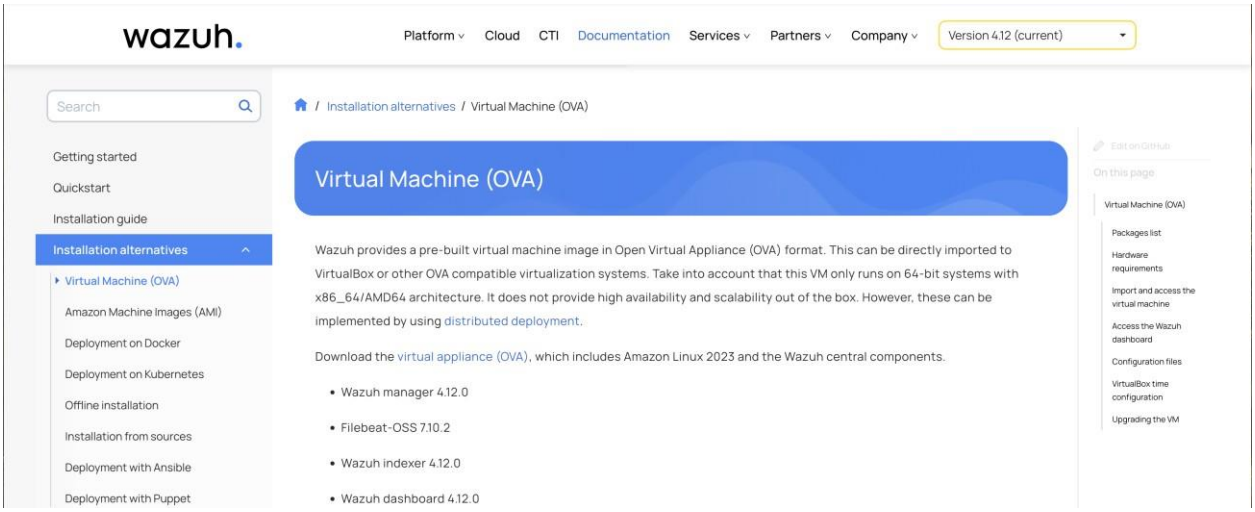
configuraciones, y un enfoque continuo de mejora que garantice su eficacia frente a los riesgos reales de seguridad. En el contexto de las pequeñas y medianas empresas (PyMEs), donde los recursos técnicos y financieros suelen ser limitados, seguir buenas prácticas permite optimizar el desempeño del sistema, reducir falsos positivos, mejorar la respuesta ante incidentes y fortalecer la postura de ciberseguridad de forma sostenible.

Diversas fuentes especializadas, como Tetrain (s. f.), destacan que aspectos clave como la definición de una arquitectura adecuada, la configuración personalizada de agentes, la gestión eficiente de reglas y la activación de módulos críticos de Wazuh son elementos determinantes para garantizar un entorno de seguridad proactivo y alineado con estándares internacionales como la norma ISO/IEC 27001.

Para su instalación Wazuh nos ofrece varias alternativas según las necesidades y nivel de experticia que se cuente, poder realizar el proceso de forma manual comando por comando y despliegue de todos sus componentes como se realizó en este trabajo, una opción más sencilla que agiliza la instalación y reduce posibles errores es utilizar las máquinas virtuales que ya tienen los módulos instalados con toda la configuración estándar listo para su uso, en la siguiente figura se observa las distintas opciones de instalación de Wazuh por medio de una máquina virtual preconfigurada para minimizar posibles errores en su ejecución.

Figura 20

Máquina Virtual Wazuh



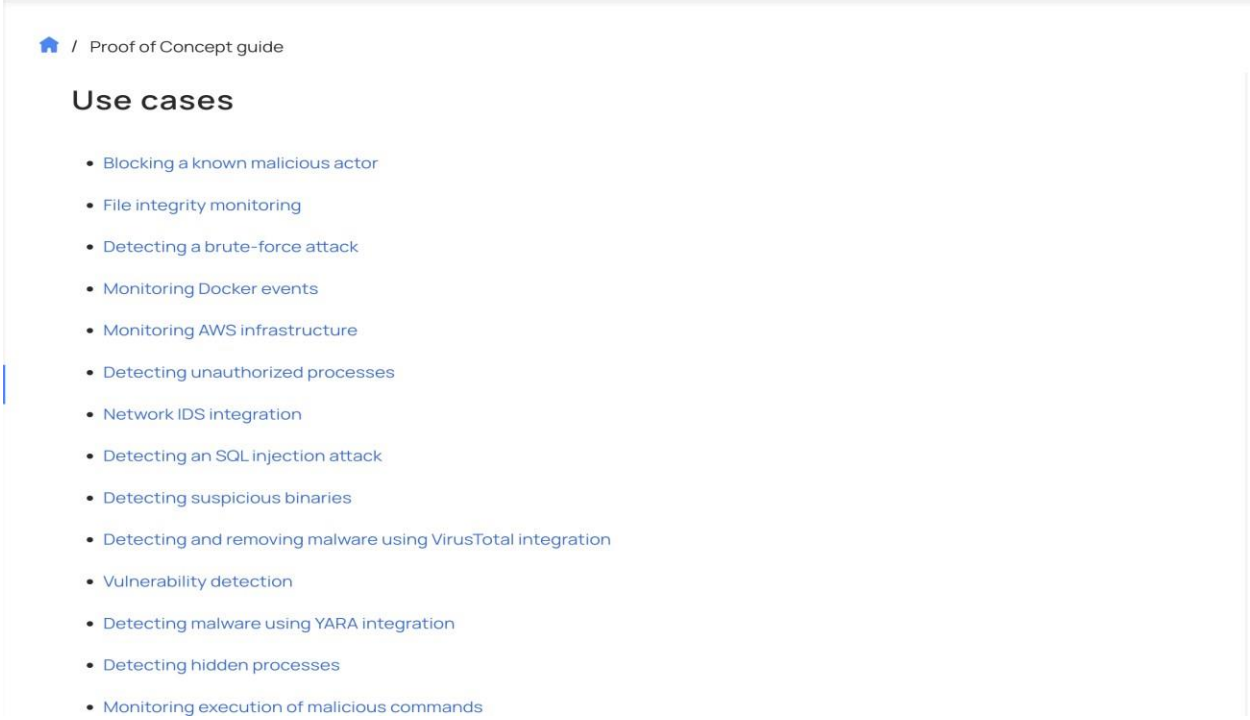
Nota. Recuperado de: https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

Wazuh incluye muchas alertas por defecto. Estas se pueden ver en /var/ossec/ruleset/rules/ en el administrador o en el repositorio de GitHub, para recibir alertas, los eventos deben ocurrir y analizarse. Para configurar qué eventos nos interesan, se tiene que modificar el archivo ossec.conf del administrador o del agente, en ossec.conf también hay una configuración predeterminada que nos permitirá recibir alertas, por ejemplo, de syscheck o localfile.

Para probar estas capacidades y respuesta de una manera segura antes de realizar la puesta en marcha en las pruebas de concepto que ofrece en la página web de como configurar el entorno, en la figura se visualiza los escenarios que Wazuh puede analizar o detectar amenazas y con un paso a paso orientado se puede implementar la prueba de concepto.

Figura 21

Casos de Uso



Nota. Recuperado de: https://documentation.wazuh.com/current/proof-of-concept-guide/index.html

Para el caso de monitorio de integración de archivos como se observó en la instalación de los end-points de Windows se tiene que ejecutar el siguiente comando en el Wazuh server para habilitar el reporte de cambios en tiempo real del directorio especifico:

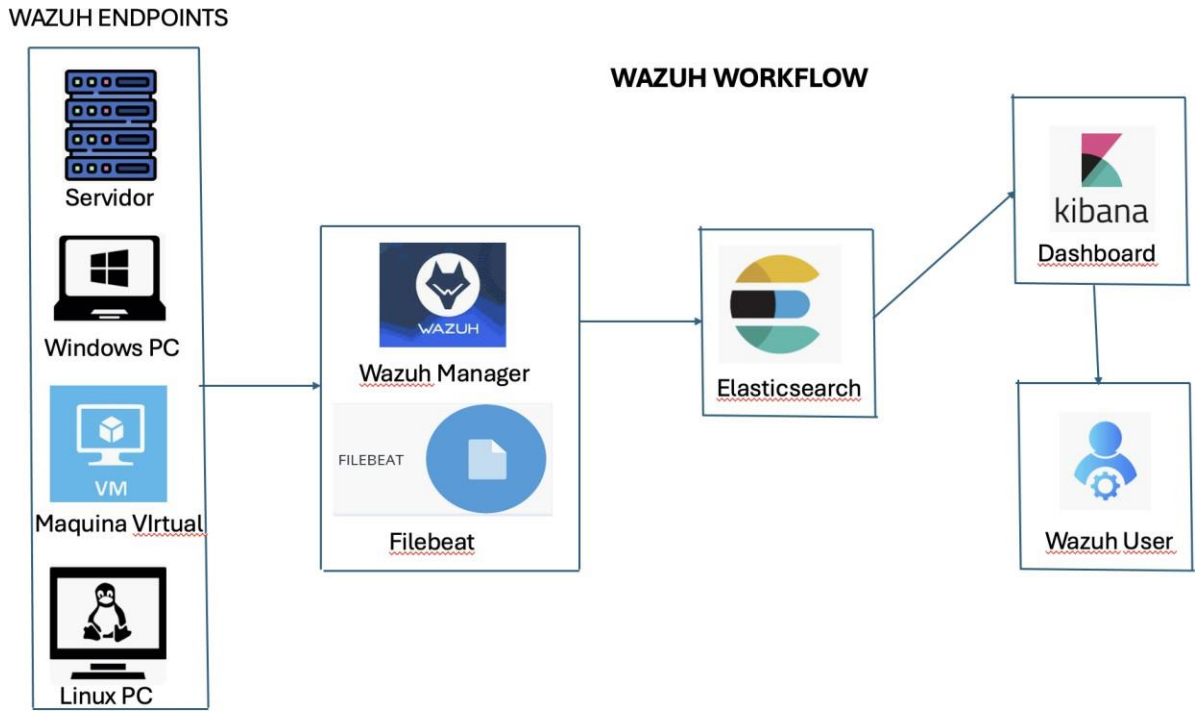
<directories check_all=”yes” report_changes=”yes” realtime=”yes”>C:\users\<USER_NAME>\Desktop</directories>

Probar que está funcionando si se modifica el directorio anterior y este debe ser visible desde la dashboard de File Integrity Monitoring.

En la figura 20 se observa el diagrama de cómo se integran los distintos módulos de Wazuh junto con sus componentes para proteger la red y la interacción de los mismos.

Figura 20

Wazuh Workflow



Nota. Elaboración propia.

Gracias a su arquitectura adaptable es posible implementar el SIEM de varias formas que se adapte a la infraestructura de la organización.

En un solo servidor (implementación todo-en-uno) Todos los componentes (Wazuh Manager, Elasticsearch, Logstash y Kibana) se instalan en un único servidor físico o virtual.

Ventajas:

- Fácil de desplegar y mantener.
- Ideal para entornos pequeños o de prueba.
- Bajo consumo de recursos iniciales.

Limitaciones:

- Escalabilidad reducida.
- Si el servidor falla, toda la solución se ve afectada.
- Distribuido en varios servidores (alta disponibilidad o balanceo de carga) Se separan los componentes: por ejemplo, un nodo para Wazuh Manager, uno para Elasticsearch, y uno para Kibana.

Ventajas:

- Mayor rendimiento y escalabilidad.
- Posibilidad de implementar alta disponibilidad.
- Aislamiento de servicios críticos.

Limitaciones:

- Mayor complejidad en la instalación y gestión.
- Requiere más infraestructura y experiencia técnica.
- En la nube (IaaS o preconfigurado) Se implementa en servicios cloud como AWS, Azure o GCP, ya sea manualmente o usando plantillas de despliegue automatizado (Terraform, scripts de Wazuh).

Ventajas:

- Accesibilidad remota y disponibilidad garantizada.
- Facilidad de escalado según demanda.
- Integración con otros servicios cloud (logs de Office 365, AWS GuardDuty, etc.).

Limitaciones:

- Dependencia de conectividad a Internet.
- Costos variables según uso.
- Requiere consideraciones especiales de seguridad (control de acceso, cifrado en tránsito y reposo).

Validación

Una vez instalado y configurado Wazuh, es fundamental realizar un proceso estructurado de validación para asegurar que todos los componentes del sistema funcionan correctamente, que los activos están siendo monitoreados de forma adecuada y que las alertas se generan según lo esperado. Esta etapa no solo verifica la instalación técnica, sino también su eficacia frente a posibles escenarios reales de amenaza, en la tabla 9 se pretende ilustrar las distintas pruebas que se pueden realizar para comprobar la validación de las distintas funciones del SIEM.

Tabla 9

Validación Funcional

Prueba	Propósito	Resuelto esperado
Intento de acceso con contraseña errada	Verificar si Wazuh genera una alerta por intento fallido de login	Alerta generada con usuario, IP, y timestamp
Modificación de un archivo crítico	Validar el control de integridad de archivos (FIM)	Detección del cambio y alerta correspondiente en el panel de Wazuh
Instalación de software no autorizado	Evaluar si se detectan nuevas aplicaciones instaladas	Alerta de software sospechoso o fuera de política
Ejecución de comandos como root/sudo	Evaluar si se monitorea el uso de privilegios	Registro en logs + alerta si se excede el uso

Nota. Elaboración propia

Es importante validar que todos los end-points cuentan con el agente instalado y funcionando, en la Dashboard es posible validar si hay agentes desconectados o sin actividad reciente. Los distintos Dashboards que ofrece Wazuh también deben contar con registro en tiempo real al igual que Kibana, poder validar que los filtros funcionan correctamente asi como la generación de reportes. Las alertas y correlación de eventos validar que no se presenten en exceso los falsos positivos.

Una validación rigurosa de Wazuh no solo permite confirmar la efectividad técnica del despliegue, sino que garantiza que la organización cuenta con una herramienta operativa que genera valor real en la prevención, detección y respuesta a incidentes. Estas validaciones deben repetirse de forma periódica y tras cada cambio significativo en la infraestructura.

La arquitectura propuesta se basa en instalar en todos los servidores y equipos de usuario el agente Wazuh los cuales enviaran los datos al servidor de Wazuh y el agente Filebeat el cual decodifica y analiza la información entrante y envía los resultados al indexador de Wazuh para su indexación y almacenamiento de esta manera será visible en la dashboard lo cual permite al equipo SOC ver en tiempo real el comportamiento de la red y tomar acciones pertinentes.

Desarrollo de Políticas y Procedimientos

Objetivo: Formalizar las prácticas operativas para garantizar el cumplimiento de la ISO 27001.

Actividades:

- Políticas de seguridad: Redacción de políticas sobre uso aceptable, gestión de incidentes, control de accesos, entre otras.
- Procedimientos operativos estándar (SOP): Instrucciones detalladas para monitoreo, análisis y respuesta ante incidentes.

- Capacitación: Formación del personal en normativas, herramientas y mejores prácticas de seguridad.

Contar con una documentación detallada de toda la gestión por parte del equipo Soc sobre incidentes y manejo de falso positivos según Detection at Scale (n.d.), uno de los principales retos en el uso de soluciones SIEM es reducir los falsos positivos sin comprometer la capacidad de detección, ya que en algunas organizaciones puede llegar hacer más del 75% de las alertas pueden ser falsos positivos lo que conlleva a una gran cantidad de tiempo y recursos humanos perdidos por lo cual, Wazuh contribuye a mitigar este problema mediante su motor de correlación de eventos, reglas ajustables y análisis contextual basado en logs, lo que permite reducir alertas irrelevantes y enfocar la atención en amenazas reales.

Monitoreo Continuo y Mejora

Objetivo: Establecer un sistema de vigilancia permanente y ajuste dinámico de la seguridad.

Actividades:

- Alertas y dashboards: Configuración de paneles de control en Kibana, alertas personalizadas y auditorías continuas.
- Control de endpoints: Wazuh permite aislar sistemas comprometidos, monitorear en tiempo real mediante SSH, y ejecutar comandos automatizados.
- Análisis forense: Registro histórico de eventos para trazabilidad y evaluaciones periódicas.

La implementación de un SIEM es un trabajo continuo ya que las amenazas evolucionan constantemente y como lo establece la ISO 27001 la importancia de mantener un proceso cíclico de revisión y mejora del SGSI por lo cual Wazuh con sus agentes y logs facilita aplicar las

políticas sobre los activos de información, al ser un software libre y contar con una comunidad activa se puede acceder a soporte y actualizaciones críticas.

Auditoría Interna y Certificación

Objetivo: Asegurar la mejora continua y preparación para auditorías externas.

Actividades:

- Auditorías internas: Evaluar la conformidad con la ISO 27001 y el funcionamiento del SGSI.
- Acciones correctivas: Aplicar medidas para corregir desviaciones detectadas.
- Preparación documental: Compilar y mantener actualizada la documentación necesaria para la certificación.

Como se mencionó anteriormente es proceso es continuo y debe participar toda la organización para minimizar riesgos por lo cual las auditorías internas y realizadas por agentes externos y acciones de mejora debe ser manejadas con alta importancia para garantizar un sistema eficiente.

La metodología propuesta para el fortalecimiento de la ciberseguridad en las PyMES de Bogotá ofrece un enfoque integral y adaptable a las condiciones técnicas y económicas de este tipo de organizaciones. Mediante la adopción de la norma ISO/IEC 27001 como marco de referencia y la implementación de la plataforma Wazuh como solución SIEM de código abierto, es posible establecer un sistema estructurado de gestión de la seguridad de la información. Esta propuesta no solo permite identificar y mitigar riesgos, sino también asegurar una mejora continua a través del monitoreo constante, la respuesta oportuna a incidentes y la alineación con estándares internacionales. En un entorno donde las amenazas cibernéticas evolucionan

rápidamente, contar con una metodología sólida y herramientas eficaces representa una ventaja competitiva y una necesidad estratégica para garantizar la resiliencia digital de las PyMES.

Conclusiones

De acuerdo a la revisión se pueden identificar que la adopción de una solución SIEM acompañados con IDS/IPS son hoy en día una de las mejores soluciones en la lucha con las ciber amenazas, así como el correcto despliegue de sus componentes pueden proteger la información de las organizaciones Pymes en Bogotá.

Al realizar la instalación de los agentes Wazuh y validar su interacción con los end-points se comprobó que su puesta en marcha no es un proceso de todo sencillo por lo cual se requiere un personal capacitado con experiencia y conocimiento técnico en terminal Linux, redes protocolo SSH por lo cual puede dificultarse para las PYMES disponer de los recursos para tener este tipo de personal especializado.

El benchmarking permite identificar buenas prácticas y oportunidades de mejora al comparar el desempeño con otros SIEM de referencia, en la comparativa se compararon los 5 principales herramientas de software referentes del mercado siendo Wazuh la única que ofrece la solución integral de SIEM al contar con el XDR y SIEM en una misma plataforma por lo cual es vital que las organizaciones realicen la selección de su sistema de detección de intrusos partiendo como punto la comparativa de las alternativas disponibles en el mercado la cual puede adaptarse fácilmente a las necesidades de la organización Pymes así como con el estándar o normativa con la que se trabajara en conjunto de esta manera Wazuh permite cubrir el 80-90% de las funcionalidades esenciales de un SIEM comercial, con una fracción del costo, y con suficiente robustez técnica como para adaptarse a entornos empresariales medianos, especialmente en sectores donde el presupuesto es limitado pero la seguridad es crítica, al no contar con IA en ninguno de sus agentes se recomienda contar con un herramienta como Microsoft Sentinel para fortalecer la respuesta a incidentes y reducir tiempos, Wazuh es una excelente base para un

SIEM modular, especialmente en entornos con recursos limitados. Sin embargo, para obtener un ecosistema SIEM completo, conviene integrarlo con herramientas complementarias que fortalezcan el análisis, la respuesta automatizada y el contexto de amenazas.

Adoptar la norma ISO 27001 en una organización apoyado por una herramienta SIEM como Wazuh posibilita el monitoreo continuo de toda la red de la organización al contar con una Dashboard en tiempo real, como lo establece la norma debe contar una política de detección de incidentes con este SIEM es posible programar la generar alertas automáticas, con el monitoreo de integridad de archivos FIM de Wazuh que detecta modificaciones no controladas en archivos críticos del sistema, como la norma lo indica es de vital importancia auditar y controlar los accesos a sistemas de información con Wazuh con el análisis de Logs de los End-Points se puede realizar la auditoria y controlar los privilegios que pueden tener los usuarios de acuerdo al perfil, la ISO 27001 exige cumplir con requisitos legales y contractuales de seguridad de la información por lo cual Wazuh genera reportes y registros que ayudan a demostrar el cumplimiento y permiten realizar auditorías internas o externas al igual que desde la dashboards y análisis históricos, Wazuh facilita la evaluación del estado de seguridad y la toma de decisiones informadas para reducir riesgos y como lo indica en su página web Wazuh permite detectar amenazas, controlar accesos, auditar eventos y generar reportes que apoyan directamente el cumplimiento de controles exigidos por normas como la ISO/IEC 27001 (Wazuh, n.d.).

La implementación de marcos de trabajo y normativas como MITRE ATT&CK, ISO 27001, y NIST SP 800-61 es fundamental para el desarrollo de contramedidas efectivas y garantizar la seguridad de la información, Wazuh integra MITRE ATT&CK en su motor de correlación de reglas, lo que le permite identificar eventos que coincidan con técnicas específicas documentadas en ATT&CK igualmente debe estar involucrado metodología SIEM que permita

la recolección, análisis y correlación de datos de seguridad en tiempo real, facilitando una respuesta rápida a incidentes.

Recomendaciones

La Adopción y manteniendo de una solución SIEM y IDS/IPS permite a las organizaciones estar protegidos a la mayoría de los riesgos modernos por lo cual es muy importante que los empresarios en Bogotá reconozcan e invistan en la implementación de estas herramientas para disminuir el aumento de los ciberataques.

Seleccionar herramientas de seguridad adecuadas que se adapten a las necesidades específicas de la organización, considerando tanto capacidades técnicas como el costo de implementación.

Para las PYMES, considerar herramientas de software libre como Wazuh, que ofrece una solución completa y económica para la seguridad de la información.

Implementar programas de capacitación y concientización en seguridad de la información para todo el personal, asegurando que todos comprendan y sigan las mejores prácticas de seguridad.

Fomentar una cultura de seguridad en la organización, donde la seguridad de la información sea una responsabilidad compartida.

Establecer un proceso de monitoreo y evaluación continua de la estrategia de detección y prevención de intrusos, asegurando que las políticas y controles de seguridad se ajusten a las nuevas amenazas.

Realizar auditorías internas y externas periódicas para evaluar la conformidad y eficacia del sistema de gestión de seguridad de la información (SGSI)

Estar en continua investigación de las nuevas tendencias de protección, así como las nuevas modalidades que presentan los ciber atacantes ya que están en constante cambio y es muy fácil quedar obsoletos en materia de protección.

Referencias Bibliográficos

Alcaldía de Bogotá. (2013). *Decreto 1377 de 2013 [Nivel Nacional]*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

Baloo Security. (s. f.). *MAGERIT: análisis de riesgos paso a paso*. https://baloo-security.com/magerit-analisis-de-riesgos-paso-a-paso/

Congreso de la República de Colombia. (2008). *Ley 1266 de 2008.* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Detection at Scale. (n.d.). *Zero false positives from your SIEM*. https://www.detectionatscale.com/p/zero-false-positives-from-your-siem

Exabeam. (s. f.). *LogRhythm SIEM overview*. https://www.exabeam.com/platform/logrhythm-siem/

Exabeam. (n.d.). *What is SIEM?* https://www.exabeam.com/explainers/siem/what-is-siem/

Gartner. (n.d.). *Security Information and Event Management (SIEM) reviews. Gartner*. https://www.gartner.com/reviews/market/security-information-event-managementGonzalez, D. (2023, marzo 14). Ciberataques en Colombia en el 2023 siguen en aumento. Intexus.com.co. https://intexus.com.co/CIBERATAQUES-EN-COLOMBIA-EN-EL-2023/

Ingens Networks. (n.d.). *¿Qué es SIEM y SOC? ¿Es segura tu empresa frente a ciberataques y malware?* https://info.ingens-networks.com/blog/siem-y-soc

Karagiannis, S., Magkos, E., & Karavaras, E. et al. (2024). *Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams. Journal of Network and Systems Management*, 32(42). https://doi-org.bibliotecavirtual.unad.edu.co/10.1007/s10922-024-09816-w

Ključnikov, A., Mura, L., & Sklenár, D. (2019). *Information security management in SMEs: Factors of success. Entrepreneurship and Sustainability Issues, 6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Kosutic, D. (2023). *Una introducción simple a los aspectos básicos*. Advisera. https://advisera.com/27001academy/es/que-es-iso-27001/

LogRhythm. (s. f.). *Features*. https://logrhythm.com/products/features/

Logsign. (s. f.). *Top challenges in implementing SIEM solutions*. https://www.logsign.com/blog/top-challenges-in-implementing-siem-solutions/

NewControl. (n.d.). *Ciberseguridad*. https://www.newcontrol.com.pe/ciberseguridad/ ISO 27000. (n.d.). SGSI. https://www.iso27000.es/sgsi.html

OSINT-PH. (2024). *Understanding Wazuh: The free, open-source security platform for XDR & SIEM*. Medium. https://osintph.medium.com/understanding-wazuh-the-free-open-source-security-platform-for-xdr-siem-48b3c3dfba9d

Pachon, C. (2023, febrero 25). *Qué es un SOC: funciones y objetivos principales*. NSIT.com.co. https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

PeerSpot. (s. f.). Wazuh: Pros and cons. https://www.peerspot.com/products/wazuh-pros-and-cons

Pirani Risk. (s. f.). *Metodología MAGERIT: Gestión de riesgos en sistemas de información*. https://www.piranirisk.com/es/blog/metodologia-magerit-gestion-riesgos-sistemas-de-informacion

Rapid7. (s. f.). Benefits of Insight Agent. https://docs.rapid7.com/insight-agent/benefits/

Rapid7. (s. f.). *Data collected by the Insight Agent*. https://docs.rapid7.com/insight-agent/data-collected/

Red Seguridad. (2021, diciembre 16). *¿Sabes cómo funciona un SOC? Definición, cometidos y tipos*. https://www.redseguridad.com/actualidad/ciberseguridad/sabes-para-que-funciona-un-soc-definicion-cometidos-y-tipos-de-centros-de-operaciones-de-seguridad_20211216.html

Reinares, D. (2020, octubre 15). *Qué es el análisis de riesgos*. OpenWebinars.net. https://openwebinars.net/blog/que-es-el-analisis-de-riesgos/

Secreto. (2024). *The benefits of integrated architecture with LogRhythm NextGen SIEM*. https://secreto.com.tr/en/the-benefits-of-integrated-architecture-with-logrhythm-nextgen-siem/

Teamwin. (2024, julio 1). *Best Intrusion Detection & Prevention Systems* (IDS/IPS). https://teamwin.in/index.php/2024/07/01/best-intrusion-detection-prevention-systems-ids-ips/

TechTarget. (n.d.). *Security operations center (SOC).* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOCOracle. (2023). *¿Qué es un SOC?* Oracle.com. https://www.oracle.com/es/database/security/que-es-un-soc.html

Tetrain. (s. f.). *Best practices for deploying Wazuh: Tips for optimized security*. Tetrain Blogs. https://www.tetrain.com/blogs/post/104/best-practices-for-deploying-wazuh-tips-for-optimized-security.html

SonicWall. (2023). Seguimiento de las actividades de los cibercriminales en la sombra. https://www.sonicwall.com/es-mx/

TICTAC. (2022, abril). Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno. Cámara Colombiana de Informática y Telecomunicaciones (CCIT).

https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Toledo, R. (2023). *Pasos esenciales para realizar un análisis de riesgo de ciberseguridad. Grupo Cibernos.* https://www.grupocibernos.com/blog/pasos-esenciales-para-realizar-un-analisis-de-riesgo-de-ciberseguridad

Urbina, G. B. (2016). *Introducción a la seguridad informática. Google Books.* https://books.google.es/books?id=IhUhDgAAQBAJ&lpg=PP1&ots=0XSA1ysbLo&dq=que%20es%20la%20seguridad%20inform%C3%A1tica%20&lr&hl=es&pg=PR3#v=onepage&q=que%20es%20la%20seguridad%20inform%C3%A1tica&f=false

Villnius. (2023). *Sistemas de gestión de la seguridad de la información*. ISOTools.us. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Wazuh. (2023). Blog. Wazuh.com. https://wazuh.com/blog/

Apéndices

Apéndice A

Formato RAE

Fecha de Realización: 8/05/2025
Título: DISEÑO DE ESTRATEGIA PARA LA DETECCIÓN DE AMENAZAS CON SOFTWARE WAZUH EN LAS EMPRESAS PYMES EN BOGOTÁ
Autor: ALMANZA, Hernando
Palabras Claves: Ciberseguridad, Iso 27001, Malware, Pymes, SIEM
Descripción: Monografía sobre la propuesta de ciberseguridad con SIEM Wazuh para empresas PYMES en Bogotá
Alcaldía de Bogotá. (2013). *Decreto 1377 de 2013 [Nivel Nacional]*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646 Baloo Security. (s. f.). *MAGERIT: análisis de riesgos paso a paso*. https://baloo-security.com/magerit-analisis-de-riesgos-paso-a-paso/ Congreso de la República de Colombia. (2008). *Ley 1266 de 2008.* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488 Detection at Scale. (n.d.). *Zero false positives from your SIEM*. https://www.detectionatscale.com/p/zero-false-positives-from-your-siem Exabeam. (s. f.). *LogRhythm SIEM overview*. https://www.exabeam.com/platform/logrhythm-siem/ Exabeam. (n.d.). *What is SIEM?* https://www.exabeam.com/explainers/siem/what-is-siem/ Gartner. (n.d.). *Security Information and Event Management (SIEM) reviews. Gartner*. https://www.gartner.com/reviews/market/security-information-event-managementGonzalez, D. (2023, marzo 14). Ciberataques en Colombia en el 2023 siguen en aumento. Intexus.com.co. https://intexus.com.co/CIBERATAQUES-EN-COLOMBIA-EN-EL-2023/ Ingens Networks. (n.d.). *¿Qué es SIEM y SOC? ¿Es segura tu empresa frente a ciberataques y malware?* https://info.ingens-networks.com/blog/siem-y-soc Karagiannis, S., Magkos, E., & Karavaras, E. et al. (2024). *Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams. Journal of Network and Systems Management*, 32(42). https://doi-org.bibliotecavirtual.unad.edu.co/10.1007/s10922-024-09816-w

Ključnikov, A., Mura, L., & Sklenár, D. (2019). *Information security management in SMEs: Factors of success. Entrepreneurship and Sustainability Issues, 6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Kosutic, D. (2023). *Una introducción simple a los aspectos básicos*. Advisera. https://advisera.com/27001academy/es/que-es-iso-27001/

LogRhythm. (s. f.). *Features*. https://logrhythm.com/products/features/

Logsign. (s. f.). *Top challenges in implementing SIEM solutions*. https://www.logsign.com/blog/top-challenges-in-implementing-siem-solutions/

NewControl. (n.d.). *Ciberseguridad*. https://www.newcontrol.com.pe/ciberseguridad/ ISO 27000. (n.d.). SGSI. https://www.iso27000.es/sgsi.html

OSINT-PH. (2024). *Understanding Wazuh: The free, open-source security platform for XDR & SIEM*. Medium. https://osintph.medium.com/understanding-wazuh-the-free-open-source-security-platform-for-xdr-siem-48b3c3dfba9d

Pachon, C. (2023, febrero 25). *Qué es un SOC: funciones y objetivos principales*. NSIT.com.co. https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

PeerSpot. (s. f.). Wazuh: Pros and cons. https://www.peerspot.com/products/wazuh-pros-and-cons

Pirani Risk. (s. f.). *Metodología MAGERIT: Gestión de riesgos en sistemas de información*. https://www.piranirisk.com/es/blog/metodologia-magerit-gestion-riesgos-sistemas-de-informacion

Rapid7. (s. f.). Benefits of Insight Agent. https://docs.rapid7.com/insight-agent/benefits/

Rapid7. (s. f.). *Data collected by the Insight Agent*. https://docs.rapid7.com/insight-agent/data-collected/

Red Seguridad. (2021, diciembre 16). *¿Sabes cómo funciona un SOC? Definición, cometidos y tipos*. https://www.redseguridad.com/actualidad/ciberseguridad/sabes-para-que-funciona-un-soc-definicion-cometidos-y-tipos-de-centros-de-operaciones-de-seguridad_20211216.html

Reinares, D. (2020, octubre 15). *Qué es el análisis de riesgos*. OpenWebinars.net. https://openwebinars.net/blog/que-es-el-analisis-de-riesgos/

Secreto. (2024). *The benefits of integrated architecture with LogRhythm NextGen SIEM*. https://secreto.com.tr/en/the-benefits-of-integrated-architecture-with-logrhythm-nextgen-siem/

Teamwin. (2024, julio 1). *Best Intrusion Detection & Prevention Systems* (IDS/IPS). https://teamwin.in/index.php/2024/07/01/best-intrusion-detection-prevention-systems-ids-ips/

TechTarget. (n.d.). *Security operations center (SOC).* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOCOracle. (2023). *¿Qué es un SOC?* Oracle.com. https://www.oracle.com/es/database/security/que-es-un-soc.html

Tetrain. (s. f.). *Best practices for deploying Wazuh: Tips for optimized security*. Tetrain Blogs. https://www.tetrain.com/blogs/post/104/best-practices-for-deploying-wazuh-tips-for-optimized-security.html

SonicWall. (2023). Seguimiento de las actividades de los cibercriminales en la sombra. https://www.sonicwall.com/es-mx/

TICTAC. (2022, abril). Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno. Cámara Colombiana de Informática y Telecomunicaciones (CCIT). https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Toledo, R. (2023). *Pasos esenciales para realizar un análisis de riesgo de ciberseguridad. Grupo Cibernos.* https://www.grupocibernos.com/blog/pasos-esenciales-para-realizar-un-analisis-de-riesgo-de-ciberseguridad

Urbina, G. B. (2016). *Introducción a la seguridad informática. Google Books.* https://books.google.es/books?id=IhUhDgAAQBAJ&lpg=PP1&ots=0XSA1ysbLo&dq=que%20es%20la%20seguridad%20inform%C3%A1tica%20&lr&hl=es&pg=PR3#v=onepage&q=que%20es%20la%20seguridad%20inform%C3%A1tica&f=false

Villnius. (2023). *Sistemas de gestión de la seguridad de la información*. ISOTools.us. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Wazuh. (2023). Blog. Wazuh.com. https://wazuh.com/blog/

Contenido del documento:

Metodología:
Trabajo sobre el análisis y estudio de los distintos SIEM de software libre y propuesta de ciberseguridad enfocado a las Pymes en Bogotá

Conceptos nuevos: Docker event, FIM (File Integrity Monitoring), Prueba de concepto,

Conclusiones: De acuerdo a la revisión se pueden identificar que la adopción de una solución SIEM acompañados con IDS/IPS son hoy en día una de las mejores soluciones en la lucha con las ciber amenazas, así como el correcto despliegue de sus componentes pueden proteger la información de las organizaciones Pymes en Bogotá.

Al realizar la instalación de los agentes Wazuh y validar su interracion con los end-points se comprobó que su puesta en marcha no es un proceso de todo sencillo por lo cual se requiere un personal capacitado con experiencia y conocimiento técnico en terminal Linux, redes protocolo SSH por lo cual puede dificultarse para las PYMES disponer de los recursos para tener este tipo de personal especializado.

El benchmarking permite identificar buenas prácticas y oportunidades de mejora al comparar el desempeño con otros SIEM de referencia, en la comparativa se compararon los 5 principales herramientas de software referentes del mercado siendo Wazuh la única que ofrece la solución integral de SIEM al contar con el XDR y SIEM en una misma plataforma por lo cual es vital que las organizaciones realicen la selección de su sistema de detección de intrusos partiendo como punto la comparativa de las alternativas disponibles en el mercado la cual puede adaptarse fácilmente a las necesidades de la organización Pymes así como con el estándar o normativa con la que se trabajara en conjunto de esta manera Wazuh permite cubrir el 80-90% de las funcionalidades esenciales de un SIEM comercial, con una fracción del costo, y con suficiente robustez técnica como para adaptarse a entornos empresariales medianos, especialmente en sectores donde el presupuesto es limitado pero la seguridad es crítica, al no contar con IA en ninguno de sus agentes se recomienda contar con un herramienta como Microsoft Sentinel para fortalecer la respuesta a incidentes y reducir tiempos, Wazuh es una excelente base para un SIEM modular, especialmente en entornos con recursos limitados. Sin embargo, para obtener un ecosistema SIEM completo, conviene integrarlo con herramientas complementarias que fortalezcan el análisis, la respuesta automatizada y el contexto de amenazas.

Adoptar la norma ISO 27001 en una organización apoyado por una herramienta SIEM como Wazuh posibilida el monitoreo continuo de toda la red de la organización al contar con una Dashboard en tiempo real, como lo establece la norma debe contar una política de detección de incidentes con este SIEM es posible programar la generar alertas automáticas, con el monitoreo de integridad de archivos FIM de Wazuh que detecta modificaciones no controladas en archivos críticos del sistema, como la norma lo indica es de vital importancia auditar y controlar los accesos a sistemas de información con Wazuh con el análisis de Logs de los End-Points se puede realizar la auditoria y controlar los privilegios que pueden tener los usuarios de acuerdo al perfil, la ISO 27001 exige cumplir con requisitos legales y contractuales de seguridad de la información por lo cual Wazuh genera reportes y registros que ayudan a demostrar el cumplimiento y permiten realizar auditorías internas o externas al igual que desde la dashboards y análisis históricos, Wazuh facilita la evaluación del estado de

seguridad y la toma de decisiones informadas para reducir riesgos y como lo indica en su página web Wazuh permite detectar amenazas, controlar accesos, auditar eventos y generar reportes que apoyan directamente el cumplimiento de controles exigidos por normas como la ISO/IEC 27001 (Wazuh, n.d.). La implementación de marcos de trabajo y normativas como MITRE ATT&CK, ISO 27001, y NIST SP 800-61 es fundamental para el desarrollo de contramedidas efectivas y garantizar la seguridad de la información, Wazuh integra MITRE ATT&CK en su motor de correlación de reglas, lo que le permite identificar eventos que coincidan con técnicas específicas documentadas en ATT&CK igualmente debe estar involucrado metodología SIEM que permita la recolección, análisis y correlación de datos de seguridad en tiempo real, facilitando una respuesta rápida a incidentes.
AUTOR: HERNANDO ALMANZA