# UNIVERSIDAD TECNOLÓGICA ISRAEL

## ESCUELA DE POSGRADOS "ESPOG"

## MAESTRÍA EN SEGURIDAD INFORMÁTICA

*Resolución:* **RPC-SO-02-No.053-2021**

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER**

| **Título del proyecto:** |
|---|
| PROPUESTA DE MONITORIZACIÓN DE EVENTOS DE SEGURIDAD CON WAZUH PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR. |
| **Línea de Investigación:** |
| Sistemas de Información e Informática |
| **Campo amplio de conocimiento:** |
| Tecnologías de la Información y la Comunicación (TIC) |
| **Autor:** |
| Danny Marcelo Fernández Gallardo |
| **Tutor:** |
| MSC. Pablo M Recalde V |

**Quito – Ecuador**

**2023**

**APROBACIÓN DEL TUTOR**

Yo, MSc. Pablo Recalde con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de monitorización de seguridad con Wazuh para Instituciones de educación superior.

Elaborado por: Danny Fernández, de C.I: 1717715237, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre del 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

**Firma**

## DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Danny Marcelo Fernández Gallardo con C.I: 1717715237, autor del proyecto de titulación denominado: **Propuesta de monitorización de seguridad con Wazuh para Instituciones de educación superior.** Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre del 2023

Firmado electrónicamente por:
DANNY MARCELO FERNANDEZ GALLARDO

**Firma**

**Orcid:** 0000-0001-9614-3863

**Tabla de contenidos**

## Índice de tablas

## Índice de figuras

## INFORMACIÓN GENERAL

El monitoreo de seguridad se refiere al monitoreo y revisión de la seguridad cibernética de un ecosistema informático. De esta forma es posible conocer su nivel o estado, permitiendo así asegurar que el sistema es fiable, estable y capaz de detectar incidencias. (Lavín, 2022).

### Contextualización del tema

Para garantizar la seguridad se deben hacer pruebas constantes para verificar que no hay brechas de seguridad, amenazas en el sistema o programas potencialmente peligrosos instalados que pongan en riesgo las políticas de seguridad informática del sistema.

Acorde el portal Wazuh (2023), Wazuh al inicio fue creado como sistema de detección de intrusos y monitoreo de seguridad de código abierto que proporciona la localización de amenazas en tiempo real, capacidades de respuesta a incidentes y análisis de registros.

El proceso de implementación implica varios pasos claves, incluido el despliegue de agentes de Wazuh en todos los sistemas y servidores críticos dentro de la red de la institución. Estos agentes recopilan datos relevantes para la seguridad, incluidos registros, eventos e información del sistema, y los envían a un administrador para su análisis.

El administrador de Wazuh correlaciona y analiza los datos recibidos, aprovechando un conjunto de reglas predefinidas y algoritmos de aprendizaje automático para identificar posibles incidentes de seguridad o infracciones de políticas. Una vez que se detecta un incidente de seguridad, Wazuh genera alertas y notificaciones, lo que permite que el equipo de seguridad de la institución responda con prontitud. y mitigar la amenaza. Las alertas se pueden personalizar según la gravedad y el tipo de incidente, lo que garantiza que el equipo pueda priorizar sus esfuerzos de manera efectiva.

Además, Wazuh proporciona un entorno gráfico centralizado que ofrece una vista integral de la postura de seguridad de la institución, lo que permite a los administradores de seguridad monitorear y administrar la infraestructura de seguridad de manera eficiente.

Por último, las capacidades centralizadas de administración y generación de informes de Wazuh permiten a los administradores de seguridad obtener información valiosa sobre el panorama de seguridad de la institución y tomar decisiones informadas sobre mejoras de seguridad y ajustes de políticas.

En conclusión, la implementación de Wazuh en una institución de educación superior fortalece la infraestructura de seguridad cibernética al detectar de manera proactiva amenazas, facilitando la respuesta a incidentes y mejorando el cumplimiento de los

estándares de seguridad. Al aprovechar las potentes funciones de Wazuh, las instituciones de educación superior garantizan un entorno de seguridad a la comunidad universitaria.

**Problema de investigación**

En los últimos años, el uso de ordenadores ha crecido espectacularmente. Cientos de tareas de las que antes se encargaba un ser humano ahora las gestiona un programa informático. Incluso puede darse el caso de que toda la información vital de las instituciones de educación superior esté almacenada en un pequeño disco duro. Esto ha generado que, en el día a día, exista aglomeración de información sensible y esto ha hecho que muchas personas vean oportunidades para aprovecharse o enriquecerse ilícitamente.

Por tanto, se puede concluir que cualquier entidad, ya sea pequeña o grande, necesita urgentemente medidas para garantizar la seguridad de sus datos. Se han producido varias formas de seguridad de los sistemas de información. Básicamente existen dos acciones: acciones activas y pasivas. El primero intenta evitar que los equipos informáticos sean infectados por malos actores, como el uso de contraseñas seguras, antivirus, cortafuegos, cifrado de datos o auditorías de seguridad. Por otro lado, están las medidas pasivas, que toman parte una vez se abre una brecha a causa de un ataque (Edix, 2023).

La implementación de medidas de seguridad pasiva puede resolver parte del problema, ya que brindan soluciones para mitigar el impacto de los ataques. Por ejemplo, copias de seguridad, uso de la nube, configuración del sistema operativo, propiedades del hardware. Normalmente, las empresas cubren con éxito medidas pasivas, pero esto no es suficiente. Según los informes de CyberEdge sobre las amenazas cibernéticas, el 85% de las organizaciones sufrieron ataques exitosos el año pasado (Cyber Edge Group, 2022).

Es por eso que, las instituciones de educación superior necesitan mejorar su despliegue y reforzar sus medidas activas. En cambio, la visión empresarial nunca elude el aspecto que más suele preocupar en una decisión. El costo de las mejoras es un gran obstáculo para desarrollar cualquier ampliación o proyecto. Por eso, los programas de código abierto “Open Source”, son la clara solución para este problema de presupuestos al que tantas pequeñas y medianas empresas se enfrentan diariamente.

La fusión de estos dos motivos en este proyecto es proporcionar una medida de seguridad activa que vigila, previene y en caso excepcional, mitiga intrusiones. Todo esto de manera eficiente y gratuita. Este sistema de defensa activa se denomina Información de seguridad y gestión de eventos (SIEM), y es el responsable de incorporar a cualquier sistema la posibilidad de monitorear fácilmente los equipos finales de una organización en busca de una actividad anómala y en caso necesario, efectuar un análisis o investigación.

¿Con el uso de un Información de seguridad y gestión de eventos (SIEM) se podrá prevenir de mejor manera los posibles ataques a la infraestructura informática de la Universidad de la Israel?

**Objetivo general**

Mostrar una solución de análisis de vulnerabilidades viable y gratuita con la que cualquier organización mejore su despliegue en infraestructura de seguridad informática.

**Objetivos específicos**

Analizar las medidas de seguridad informática actuales en la Universidad Tecnológica Israel en la infraestructura de seguridad cibernética existente.

Evidenciar vulnerabilidades y brechas de impacto en la infraestructura de seguridad de la institución, como software desactualizado.

Implementar la herramienta Wazuh y su compatibilidad con los sistemas existentes de la institución.

**Vinculación con la sociedad y beneficiarios directos**

En el presente trabajo de investigación provee a la comunidad y a la Universidad Tecnológica Israel un análisis de herramientas Open Source que son de fácil acceso y no es necesario una gran inversión económica para proteger sus sistemas de comunicación y redes.

Al desarrollar este proyecto se pretende anticipar un posible ataque a la infraestructura digital institucional; de igual manera mejorar la administración con herramientas que se pueden implementar Security Information and Event Management y también contar con un mecanismo de defensa ante un sin número de ataques que ocurren diariamente en el mundo.

Se pretende mejorar el esquema para agilizar las respuestas de los sistemas de seguridad de procesamientos de datos o de Información, a fin de garantizar una adecuada gestión de la seguridad; para mantener procedimientos de seguridad de datos de la infraestructura de la información de la Universidad Tecnológica Israel. Los sistemas de información y comunicaciones ahora más que nunca son determinantes para la toma de decisiones y, por tanto; también son más vulnerables a ataques internos y externos.

«El objetivo de desarrollo sostenible (ODS) nueve tiene como objetivo contar con una infraestructura sostenible, robusta y de calidad para todos en 2030, promover una industria sostenible que utilice tecnologías y procesos industriales limpios y eco amigables con el medio ambiente, promover la tecnología, la innovación y la investigación, para lograr el

acceso al conocimiento y la información, a través de Internet» (Naciones Unidas Ecuador, 2023).

«Las infraestructuras de comunicaciones han aumentado en los últimos años, hoy en día la mitad de población a nivel mundial se encuentra conectada y casi toda la población global se encuentra asentada en áreas que cuentan con cobertura móvil» (ODS, 2017)

Según Pathak (2022) el uso de soluciones SIEM permite automatizar las tareas de seguridad. Ya no se necesita monitorear y configurar todo de forma manual; los sistemas SIEM permiten automatizar estas tareas para liberar el tiempo en el crecimiento de los negocios. Con esto no solo reduce el esfuerzo, sino que también ahorra costos.

En resumen, Wazuh se vincula con la sociedad al ayudar a proteger los sistemas y datos de las organizaciones, y los beneficiarios directos son las propias organizaciones que utilizan esta plataforma para fortalecer su seguridad cibernética.

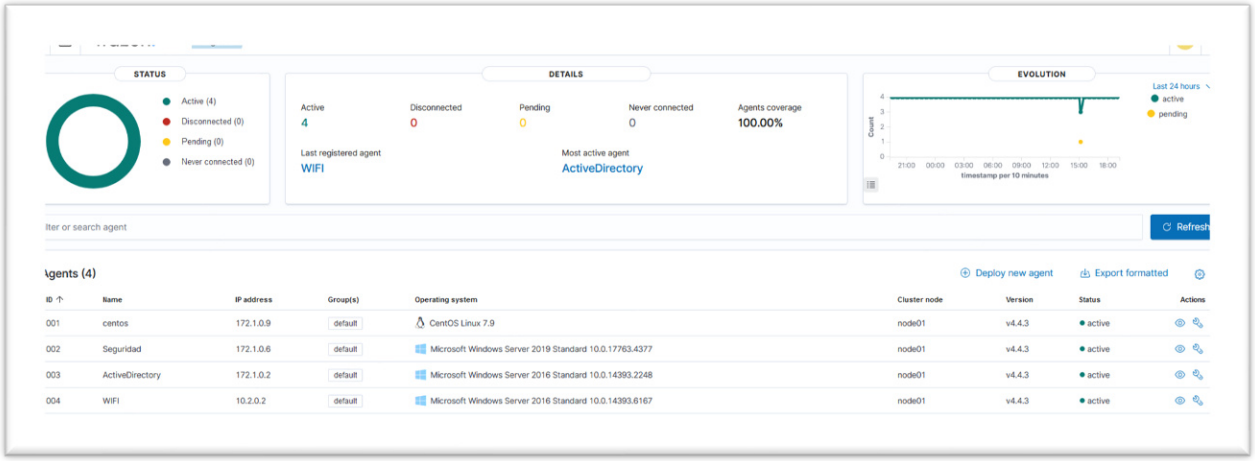
# CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La herramienta de seguridad llamada Security Information and Event Management, ayuda a las empresas a identificar, evaluar y responder a las amenazas antes de que tengan un impacto en las operaciones o transacciones que se realizan diariamente en instituciones de educación superior.

## 1.1. Contextualización general del estado del arte

Wazuh es una plataforma gratuita de código abierto para detección de amenazas, monitoreo de seguridad, respuesta a incidentes y cumplimiento. Esto permite monitorear puntos finales, servicios en la nube y contenedores y recopilar y analizar datos de fuentes externas. Wazuh tiene las siguientes características. (Morales, 2022)

**Figura 1.**
*Interfaz gráfica de wazuh*




Nota: Captura del sistema

Algunas características clave de Wazuh incluyen:

Detección de amenazas: Wazuh utiliza reglas predefinidas y personalizables para detectar patrones de comportamiento malicioso en registros y tráfico de red. Estas reglas se basan en eventos y patrones conocidos de ataques y actividades sospechosas.

Integración con Elasticsearch y Kibana: Wazuh almacena los datos de registro en Elasticsearch y proporciona una interfaz de usuario a través de Kibana para visualizar y analizar los datos de seguridad. Esto permite la búsqueda y análisis avanzado de eventos para identificar amenazas y tendencias.

Monitorización en tiempo real: Wazuh es capaz de monitorizar eventos y registros en tiempo real, lo que permite al administrador de seguridad detectar y responder rápidamente a incidentes de seguridad.

Integración con otros sistemas: Wazuh se puede integrar con otros sistemas y herramientas de seguridad, como SIEM, firewalls, y sistemas de gestión de vulnerabilidades, para una visión más completa de la postura de seguridad de una organización.

Automatización de respuestas: Wazuh permite la automatización de respuestas a eventos de seguridad mediante acciones predefinidas, como bloquear direcciones IP sospechosas o tomar medidas específicas en función del tipo de amenaza detectada.

Arquitectura flexible: Wazuh se puede implementar en diferentes tipos de entornos, incluyendo servidores, estaciones de trabajo y dispositivos de red, lo que permite una adaptación a las necesidades específicas de cada organización.

Código abierto y comunidad activa: Wazuh es un proyecto de código abierto, lo que significa que su código fuente está disponible públicamente. Esto permite a la comunidad de seguridad contribuir al desarrollo y mejorar continuamente la plataforma.

## 1.2. Proceso investigativo metodológico

El marco metodológico describe la forma en que se ha llevado la investigación; bajo una metodología científica. Esto permite explicar la propiedad y características de la metodología de investigación que usa la aprobación de resultados, con el tipo de información adecuada para comprender, aceptar y demostrar la capacidad de replicar el análisis de los resultados de la investigación, o es una estructura que permite estudiar los medios y formas de investigar y demostrar una verdad.

### La investigación experimental

El nombre se refiere a una investigación que deriva información de las acciones conscientes del investigador con el objetivo de cambiar la realidad para crear el fenómeno en estudio de modo que pueda ser observado. (Universidad de Veracruz, 2022)

El uso de la investigación experimental sirve para el estudio, análisis y resultados de la recolección de los datos más relevantes por Wazuh que ayuden al desarrollo del presente trabajo, mismo que está enmarcado en el análisis frecuente de los datos que se han recolectado por medio de la aplicación de varios instrumentos investigativos, al igual que la aplicación de herramientas completamente necesarias para el análisis de información.

### Investigación inductiva

La inducción es un proceso de razonamiento que extrae conclusiones generales a partir de ejemplos específicos basados en observaciones y experimentos. A partir de estos patrones o tendencias, se pueden extraer conclusiones o teorías generales que son válidas

en todas las situaciones similares. Es importante señalar que las conclusiones generales extraídas por inducción son provisionales y están sujetas a revisión a la luz de nuevas observaciones y experimentos. (Narvaez, 2023).

Se aplicó el proceso de investigación inductivo para realizar el estudio sobre la factibilidad al usar herramientas de software libre o código abierto; de igual manera con este proceso se va a determinar un reporte con el detalle de los eventos de seguridad registrados en base a los registros de la herramienta Wazuh.

# CAPÍTULO II: PROPUESTA

En este capítulo se desarrollará la propuesta del tema de investigación planteado como monitorización de seguridad con Wazuh para instituciones de educación superior.

## 2.1 Fundamentos teóricos aplicados

Wazuh es una plataforma de seguridad de código abierto diseñada para la detección de amenazas, monitorización de seguridad y respuesta a incidentes. Combina la detección de intrusos basada en reglas Sistema de Detección de Intrusos (IDS), la monitorización de registros SIEM y la gestión de la seguridad en una solución integral. Los fundamentos teóricos aplicados en Wazuh se basan en varios conceptos clave:

Detección de Intrusos (IDS): Wazuh utiliza un motor de detección de intrusos basado en reglas para analizar eventos y tráfico de red en busca de patrones asociados a ataques o comportamientos maliciosos. Las reglas describen condiciones específicas que, cuando se cumplen, indican una posible actividad maliciosa. Estas reglas pueden ser creadas por la comunidad o personalizadas según las necesidades del entorno.

Monitorización de Registros (SIEM): Wazuh recopila y normaliza registros de diferentes fuentes, como sistemas operativos, aplicaciones y dispositivos de red. Luego, correlaciona y analiza estos registros para identificar patrones y actividades anómalas que podrían indicar una amenaza. El análisis de registros es crucial para detectar actividades sospechosas o incidentes de seguridad.

Inteligencia de Amenazas: Wazuh utiliza listas de inteligencia de amenazas conocidas, como direcciones IP maliciosas y dominios de malware, para mejorar la detección. Estas listas se actualizan regularmente para mantenerse al día con las últimas amenazas conocidas.

Escalación y Respuesta a Incidentes: Cuando Wazuh identifica una actividad maliciosa o sospechosa, puede tomar medidas automáticas o enviar alertas al equipo de seguridad. Las alertas pueden ser personalizadas y priorizadas según la gravedad del incidente, lo que permite al equipo responder de manera eficiente.

Análisis de Comportamiento: Además de las reglas específicas, Wazuh puede utilizar análisis de comportamiento para detectar actividades inusuales o anómalas en función de los patrones de actividad normal en el entorno. Esto permite detectar amenazas que podrían no estar cubiertas por reglas específicas.

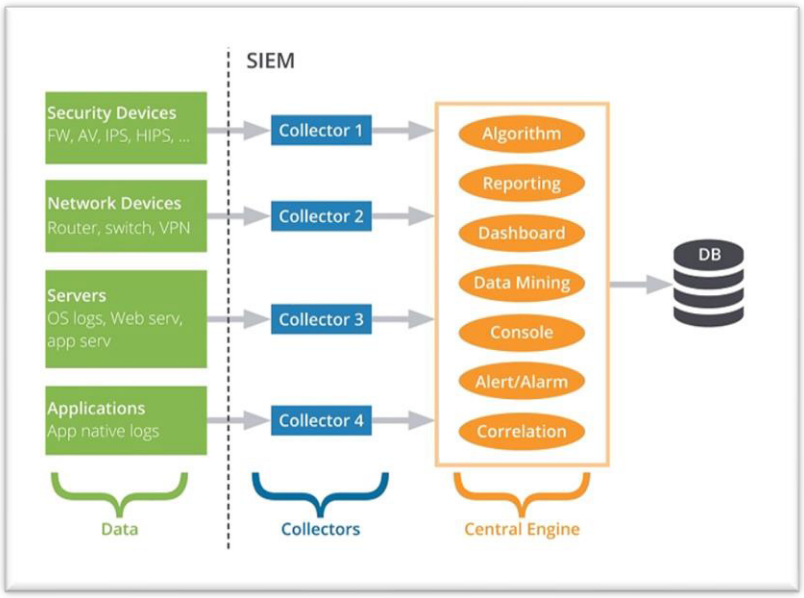
Visualización y Paneles de Control: Wazuh ofrece paneles de control y visualizaciones que permiten a los equipos de seguridad tener una visión general de la salud de la seguridad

y la actividad del sistema. Estas visualizaciones pueden ayudar a identificar tendencias y patrones de ataque.

Automatización e Integración: Wazuh se puede integrar con otras herramientas y sistemas de seguridad, lo que permite una respuesta automatizada y una mayor eficiencia en la gestión de incidentes. También puede interactuar con sistemas de orquestación y automatización para realizar acciones correctivas automáticamente.

En resumen, Wazuh se basa en la detección de intrusos, la monitorización de registros, la inteligencia de amenazas y la respuesta a incidentes para ofrecer una solución integral de seguridad. Combina principios teóricos con implementación práctica para ayudar a las organizaciones a proteger sus sistemas y datos de amenazas cibernéticas. (Mundhada, 2019).

**Figura 2.**
*Arquitectura referencia de SIEM*




Nota: Oracle (2022)

## 2.2 Descripción de la propuesta

Este documento presentará las principales características de la herramienta Wazuh instalada en el Departamento de Recursos Tecnológicos (DRT) de la Universidad Tecnológica Israel y una vez realizado el Check list de verificación de seguridad informática Universidad Tecnológica Israel (Anexo 1).

El presente trabajo describe cómo se puede utilizar la herramienta Wazuh que recopila datos exclusivamente de servidores web y aplicaciones. Los resultados obtenidos a través de

este documento brindar a los administradores una idea de lo que debe cambiarse dentro de sus configuraciones para llevar sus servidores y toda la infraestructura a mejorar la seguridad.

**Componentes Wazuh**

La solución de Wazuh se basa en los siguientes componentes:

Agente de Wazuh: ofrece funciones de prevención, detección y respuesta cuando se despliega en terminales como laptops, computadores, servidores o máquinas virtuales. Funciona desde windows XP hasta un Windows 2019 corren todas las versiones de Linux incluso en versiones de unix .

Servidor Wazuh: analiza la información recibida de los servidores, los procesa a través de reglas y utiliza inteligencia sobre amenazas, analiza los datos recibidos de los agentes, los procesa a través de decodificadores y reglas, y usa inteligencia de amenazas para buscar indicadores conocidos de compromiso.

Elastic Stack: es una colección unificada de proyectos de código abierto, incluidos Elasticsearch, Kibana, Filebeat y otros.

Elastic Search: es un motor de análisis y búsqueda de texto completo altamente escalable. Una interfaz web flexible e intuitiva para extraer, analizar y visualizar datos. Se ejecuta sobre el contenido indexado en un clúster de Elasticsearch.

La interfaz de usuario web de Wazuh se ha integrado completamente en Kibana, en forma de complemento. Arquitectura Wazuh.

**Arquitectura Wazuh**

La arquitectura de Wazuh se basa en agentes que se ejecutan en puntos finales monitoreados y envían información de seguridad al administrador del sistema. Además, admiten dispositivos sin agentes (como firewalls, conmutadores, enrutadores, puntos de acceso, etc.) y pueden enviar activamente información de registro a través de syslog. El administrador extrae y analiza los datos entrantes y envía los resultados a Elasticsearch para su indexación y almacenamiento.

**Configuración de Wazuh**

Los resultados descritos en este artículo se recopilaron de varios servidores web y de aplicaciones sistema operativo CentOS con la versión 7.9, dos servidores Microsoft Windows Server 2016 Standard y un servidor Microsoft Windows Server 2019 Standard ubicados en el Departamento de Recursos Tecnológicos (DRT) de la Universidad Tecnológica Israel.

El agente proporcionado por Wazuh están instalados en ellos para enviar datos del administrador de Wazuh. Se ha instalado en 3 máquina virtual y en un servidor. Como alternativa a la implementación en máquina virtual, se pueden utilizar dockers.

**Tabla 1.**
*Infraestructura Tecnológica a Implementar*

| Host | Servidor | Sistema Operativo | Descripción |
|---|---|---|---|
| Servidor Wazuh | Servidor SIGE | Windows Server 2019 | Servidor Web, servidor DB, servidor FTP, |
| | Servidor Repositorio DSPACE | Centos 7.9 | Servidor Web, servidor DB, servidor FTP, |
| | Servidor Radius Wifi Active Directory y Certificados de Autenticación | Windows Server 2016 | Servidor NTP. |
| | Servidor Active Directory | Windows Server 2016 | Servidor de autenticación (ADDS), servidor DB, servidor LDAP. |

Nota: Infraestructura Universidad Tecnológica Israel.

**Resultados del estudio de Wazuh**

Los resultados dentro de cada elemento de Wazuh Managers se presentan en esquemas y se hace especial énfasis en el análisis de ataques conocidos. Dentro de la pantalla principal, hay 4 secciones básicas con opciones en las que puede monitorear datos en tiempo real.

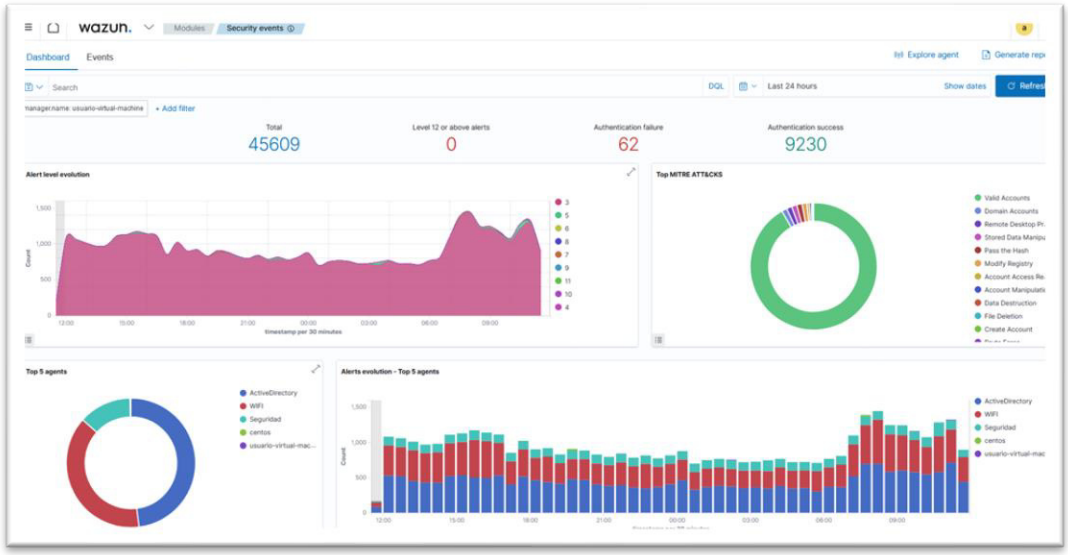
**Gestión de la información de seguridad**

**Eventos de seguridad**

En esta sección, es posible buscar todos los eventos de seguridad registrados dentro del sistema Wazuh. El funcionamiento del sistema se basa en agentes que envían datos (logs) al servidor donde son procesados.

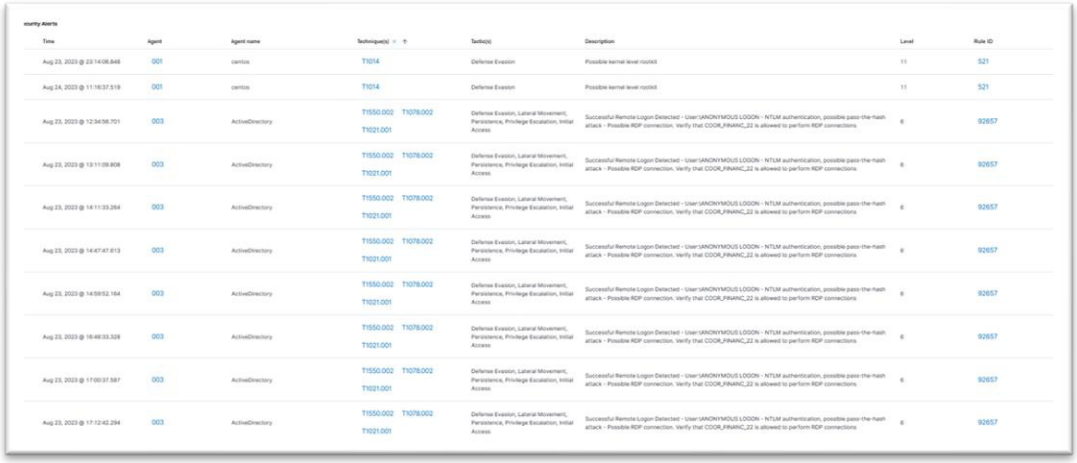
Hay todo un conjunto de reglas definidas para identificar las amenazas. Los resultados se procesan y cuando se cumple una regla, se registra en la pantalla principal.

**Figura 3.**
*Pantalla principal Wazuh Uisrael*




Nota: Wazuh instalado en servidor institucional de la Uisrael.

**Figura 4.**
*Alertas de Seguridad Wazuh Uisrael*



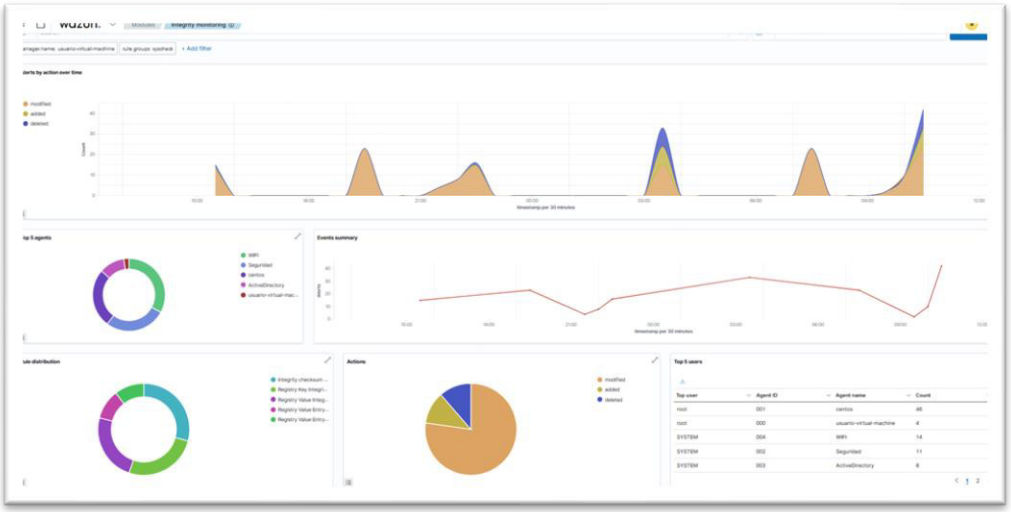
Nota: Reporte de alertas de seguridad producidos por los servidores de la Uisrael.

Wazuh ofrece la opción de escribir reglas personalizadas según las necesidades del usuario. La figura 4 muestra la lista ordenada de alertas de seguridad. Vemos que el 'Código de error T1550' es el error más frecuente. En cada unidad dentro del administrador de Wazuh, es posible mostrar los resultados en un rango de tiempo determinado. Dentro de cada

sección, hay una opción para generar informes y, para una mejor visibilidad, se mostrarán las 10 alertas principales de cada informe.

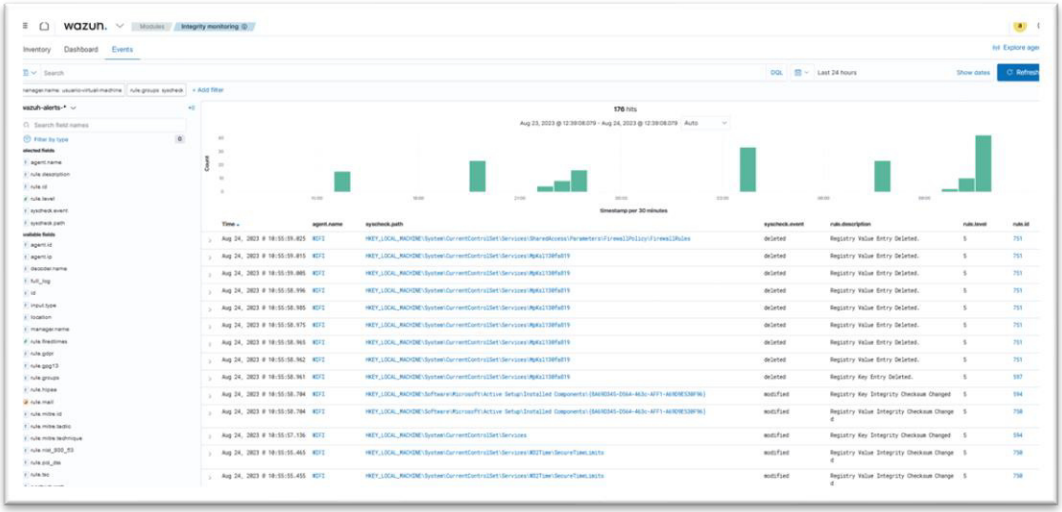
## Monitoreo de integridad

**Figura 5.**
*Monitoreo de integridad de la información*



Nota: Gráfica integridad de los archivos en los servidores de la Uisrael.

**Figura 6.**
*Eventos suscitados en archivos de los servidores de la Uisrael*



Nota: Eventos integridad de los archivos en los servidores de la Uisrael.

En este módulo, es posible monitorear las estadísticas de cambios en los archivos del sistema en el host con el agente instalado.

Estos cambios incluyen la modificación, eliminación y el incremento de nuevos archivos. Los cambios se detectan en función del cambio en la suma de comprobación de cada archivo.

Dentro de la pestaña Eventos, es posible seguir cada cambio en detalle, donde puede conocer los detalles de cuándo se modificó un archivo, qué usuario realizó la acción y cuáles son los permisos del archivo. Este tipo de monitoreo puede ser muy útil, especialmente para sistemas sensibles. Las acciones realizadas y la lista de archivos que se modifican con mayor frecuencia se muestran en la Figura 6.

## 2.3 Validación de la propuesta

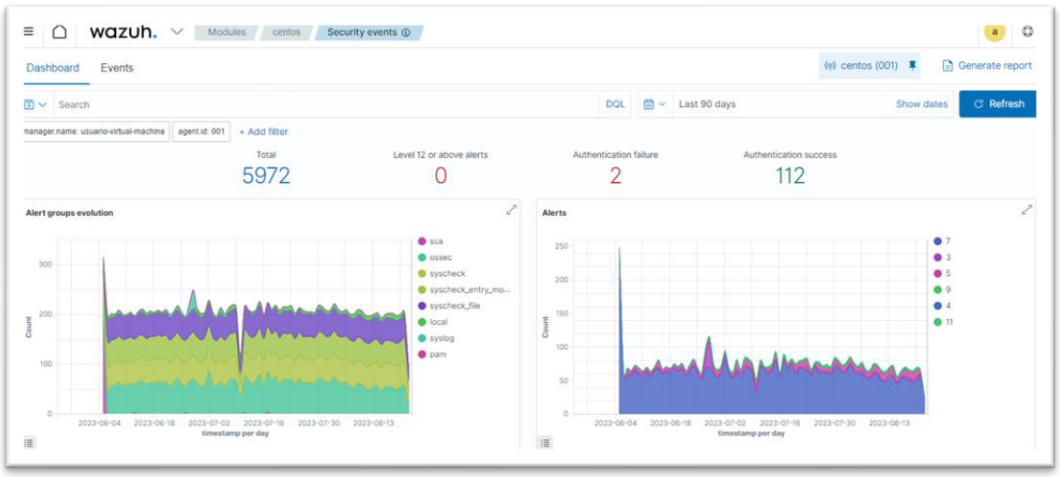
### Vulnerabilidades repositorio digital

Una vez recibidos los resultados hay que revisar el módulo de vulnerabilidades de Wazuh.

El administrador Wazuh crea una base de datos a partir de repositorios, en ese momento se van generando alertas en vulnerabilidades y exposiciones comunes (CVE) cuando se afecta a un paquete.

Tras 90 días de análisis se han obtenido 5972 eventos, 0 alertas críticas, 2 errores de autenticación, 112 autenticación correctas. Todas ellas son del servidor repositorio digital UIsrael, ya que no ha detectado alertas críticas en la máquina de Centos 7.9.

**Figura 7.**
*Visualización de las alertas repositorio digital Uisrael*



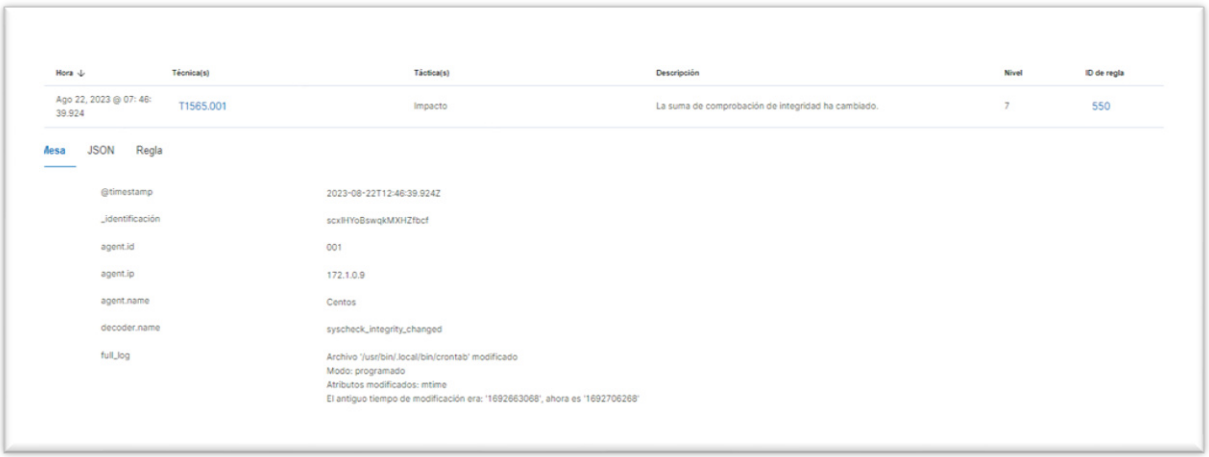

Nota: Imagen wazuh servidor institucional

Cada notificación brinda mucha información relevante. Además de proporcionar el vulnerabilidades y exposiciones comunes (CVE), la fecha y hora de la alerta, la gravedad y el paquete afectado por la vulnerabilidad, podremos ver información adicional al ampliar la alerta. Hay una breve descripción con los efectos que provoca y algunos consejos sobre cómo solucionarlo. Además, aunque Wazuh nos dice la gravedad de la vulnerabilidad (Crítica, Alta, Media y Baja).

**Figura 8.**
*Descripción, impacto y referencias repositorio digital*


Nota: Imagen alertas de eventos

**Figura 9.**
*Descripción de las alertas repositorio digital Uisrael*




Nota: Imagen alertas de eventos

Se ha realizado una selección de las vulnerabilidades y exposiciones más comunes (CVEs) que han aparecido en el análisis y de los paquetes más afectados.

## Vulnerabilidad (T1078)

**Tabla 2.**
*Descripción y solución Vulnerabilidad T1078*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden obtener y abusar de las credenciales de las cuentas existentes para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensa. Las credenciales comprometidas se pueden usar para eludir los controles de acceso colocados en varios recursos en sistemas dentro de la red e incluso se pueden usar para el acceso persistente a sistemas remotos y servicios disponibles externamente, como VPN, Outlook Web Access y escritorio remoto. Las credenciales comprometidas también pueden otorgar a un atacante un mayor privilegio para sistemas específicos o acceso a áreas restringidas de la red. Los atacantes pueden optar por no usar malware o herramientas junto con el acceso legítimo que proporcionan esas credenciales para dificultar la detección de su presencia. |
| **Posibles soluciones:**<br>Audite el dominio y las cuentas locales y sus niveles de permiso, de forma rutinaria para buscar situaciones que permitan a un atacante obtener un amplio acceso obteniendo credenciales de una cuenta privilegiada. |

Nota: Análisis y posibles soluciones vulnerabilidad S.O. Centos 7.9

## Vulnerabilidad (T1014)

**Tabla 3.**
*Descripción y solución Vulnerabilidad T1014*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden usar rootkits para ocultar la presencia de programas, archivos, conexiones de red, servicios, controladores y otros componentes del sistema. Los rootkits son programas que ocultan la existencia de malware interceptando/enganchando y modificando las llamadas API del sistema operativo que proporcionan información del sistema. |
| **Posibles soluciones:**<br>Identifique el software potencialmente malintencionado que pueda contener la funcionalidad del rootkit y audite y/o bloquee mediante el uso de herramientas de listas. |

Nota: Análisis y posibles soluciones vulnerabilidad S.O. Centos 7.9

## Vulnerabilidad (T1565.001)

**Tabla 4.**
*Descripción y solución Vulnerabilidad T1565*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden insertar, eliminar o manipular datos en reposo para influir en los resultados externos u ocultar la actividad, amenazando así la integridad de los datos. Al manipular los datos almacenados, los atacantes pueden intentar afectar un proceso de negocio, la comprensión organizacional y la toma de decisiones. |
| **Posibles soluciones:**<br>Restrinja el acceso estableciendo permisos de directorio y archivo que no sean específicos de usuarios o cuentas con privilegios. |

Nota: Análisis y posibles soluciones vulnerabilidad S.O. Centos 7.9

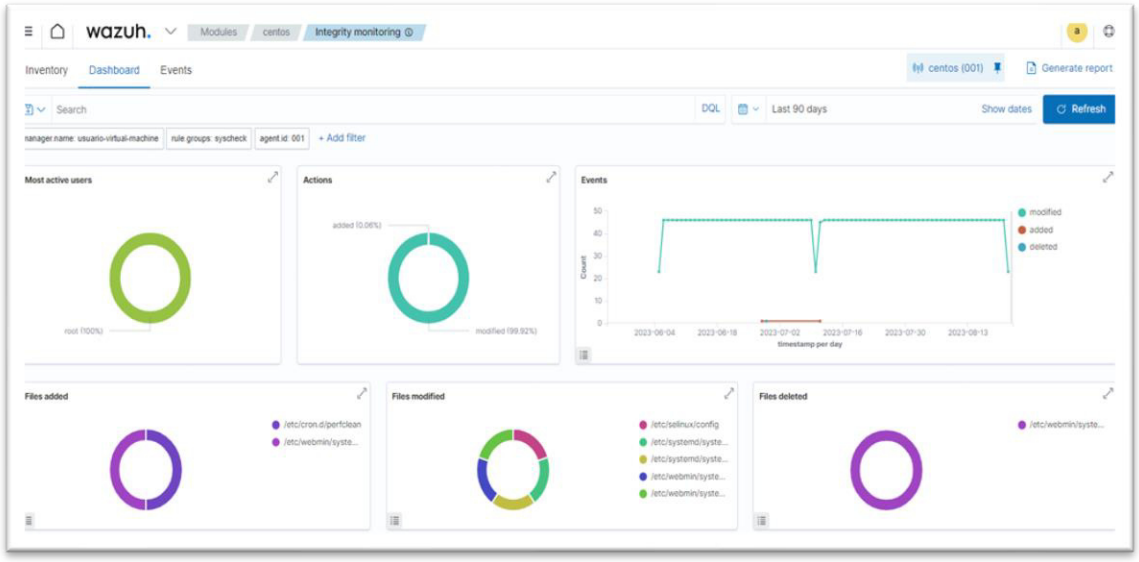
Principalmente hay 2 paquetes que se ven afectados:

**crontab:** es un ejecutable que permite a los usuarios realizar tareas y ejecutarlas automáticamente a una hora determinada.

**sislog:** es un protocolo de registros que lo posee dispositivos como routers, switches, firewalls, puntos de acceso Wi-Fi y servidores Linux generan sus propios registros.

Monitoreo de integridad de archivos es un módulo proporcionado por Wazuh para detectar cambios en los permisos y contenido de los archivos.

**Figura 10.**
*Alertas del módulo Integrity Monitoring*




Nota: Imagen wazuh servidor institucional.

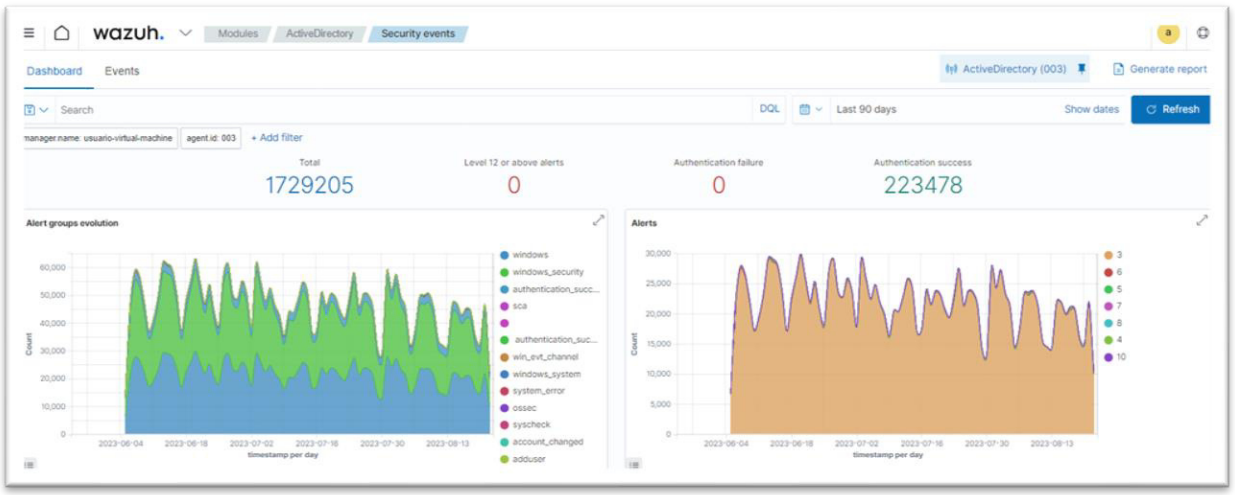
El resultado de alertas en las que se puede observar cuando se ha añadido y cuando se ha borrado el archivo. Para ello tendremos que expandir las alertas y ver con más detalle los datos que nos dan.

## Resultados del estudio de Wazuh directorio activo Ulsrael

### Vulnerabilidades

Tras 90 días de análisis se han obtenido 1’729.205 eventos, 0 alertas críticas, 0 errores de autenticación, 223.478 autenticación correctas. Todas ellas son del servidor active directory, ya que no ha detectado ninguna alerta en la máquina de Windows server 2016.

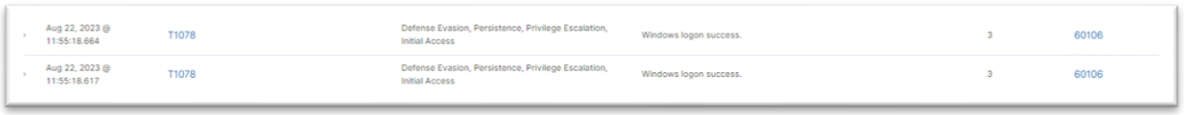
**Figura 11.**
*Visualización de las alertas active directory*




Nota: Imagen wazuh servidor institucional

De igual manera las alerta que nos va a proporcionar nos proporciona por medio de mucha información relevante por medio de vulnerabilidades y exposiciones comunes (CVE),

**Figura 12.**
*Descripción, impacto y referencias active directory*




Nota: Imagen alertas de eventos

**Figura 13.**
*Descripción de alerta active directory Uisrael*


Nota: Imagen alertas de eventos

Se ha realizado una selección de las vulnerabilidades más comunes (CVEs) que han aparecido en el análisis y de los paquetes más afectados.

### Vulnerabilidad (T1078)

**Tabla 5.**
*Descripción y solución Vulnerabilidad T1018 Windows 2016*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden obtener y abusar de las credenciales de las cuentas existentes como un medio para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensa. Las credenciales comprometidas se pueden usar para eludir los controles de acceso colocados en varios recursos en sistemas dentro de la red e incluso se pueden usar para el acceso persistente a sistemas remotos y servicios disponibles externamente, como VPN, Outlook Web Access y escritorio remoto. Las credenciales comprometidas también pueden otorgar a un atacante un mayor privilegio para sistemas específicos o acceso a áreas restringidas de la red. |
| **Posibles soluciones:**<br>Audite el dominio y las cuentas locales y sus niveles de permiso, de forma rutinaria para buscar situaciones que permitan a un atacante obtener un amplio acceso obteniendo credenciales de una cuenta privilegiada. |

Nota: Análisis y posibles soluciones vulnerabilidad S.O. Windows Server 2016

### Vulnerabilidad (T16001)

**Tabla 6.**
*Descripción y solución Vulnerabilidad T16001 windows server 2016*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Cuanto más tiempo exista una contraseña, mayor será la probabilidad de que se vea comprometida por un ataque de fuerza bruta, por un atacante que obtenga conocimiento general sobre el usuario o por el usuario que comparte la contraseña. Configurar la configuración de Antigüedad máxima de la contraseña en 0 para que los usuarios nunca tengan que cambiar sus contraseñas es un riesgo de seguridad importante porque permite que el usuario malintencionado use una contraseña comprometida mientras el usuario válido tenga acceso autorizado. |
| **Posibles soluciones:**<br>Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de acceso de la interfaz de usuario en 60 días o menos, pero no 0: Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas de cuenta\Directiva de contraseña\Antigüedad máxima de la contraseña. |

Nota: Análisis y posibles soluciones vulnerabilidad S.O. Windows Server 2016

### Vulnerabilidad (T16004)

**Tabla 7.**
*Descripción y solución Vulnerabilidad T16004 windows server 2016*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>El tráfico de red sin firmar es susceptible a ataques man-in-the-middle. En tales ataques, un intruso captura paquetes entre el servidor y el cliente, los modifica y luego los reenvía al cliente. En lo que respecta a los servidores protocolo ligero de acceso a directorios LDAP, un atacante podría hacer que un cliente tome decisiones basadas en registros falsos del directorio LDAP. Para reducir el riesgo de una intrusión de este tipo en la red de una organización, puede implementar medidas de seguridad física sólidas para proteger la infraestructura de red. Además, puede implementar el modo de encabezado de autenticación (AH) de seguridad de protocolo de Internet (IPsec), que realiza la autenticación mutua y la integridad de paquetes para el tráfico IP para dificultar todo tipo de ataques man-in-the-middle. Además, permitir el uso de LDAP regular y sin firmar permite que las |

| |
|---|
| credenciales se reciban a través de la red en texto no cifrado, lo que podría resultar fácilmente en la interceptación de contraseñas de cuentas por parte de otros sistemas de la red. |
| **Posibles soluciones:**<br>Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de acceso de la interfaz de usuario en Requerir firma: Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad\Controlador de dominio: requisitos de firma del servidor LDAP. |

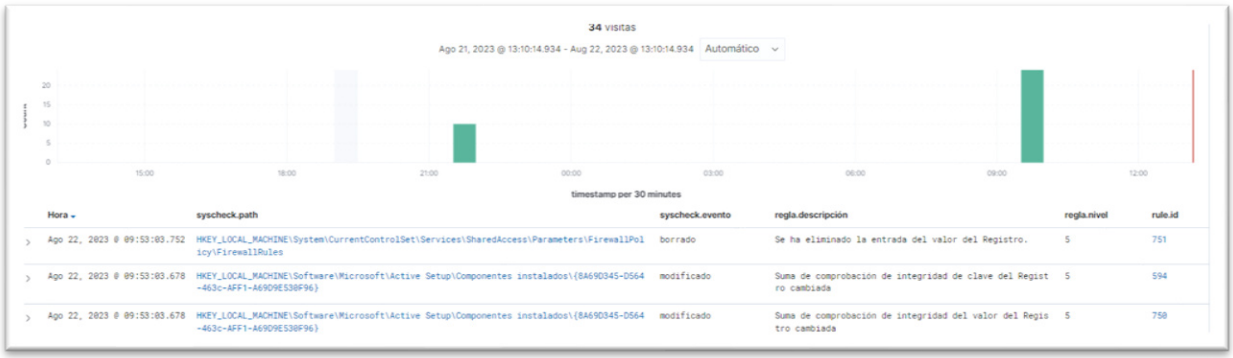
Nota: Análisis y posibles soluciones vulnerabilidad S.O. Windows Server 2016

Principalmente hay 2 registros que se ven afectados:

\CurrentVersion\Winlogon: es un proceso que implemente la función del gestor de conexión de Windows.

\CurrentControlSet\Services\NTDS\Parameters: es el componente de back-end de Active Directory y almacena todos los datos del dominio.

**Figura 14.**
*Alertas del módulo Integrity Monitoring*




Nota: Imagen wazuh servidor institucional

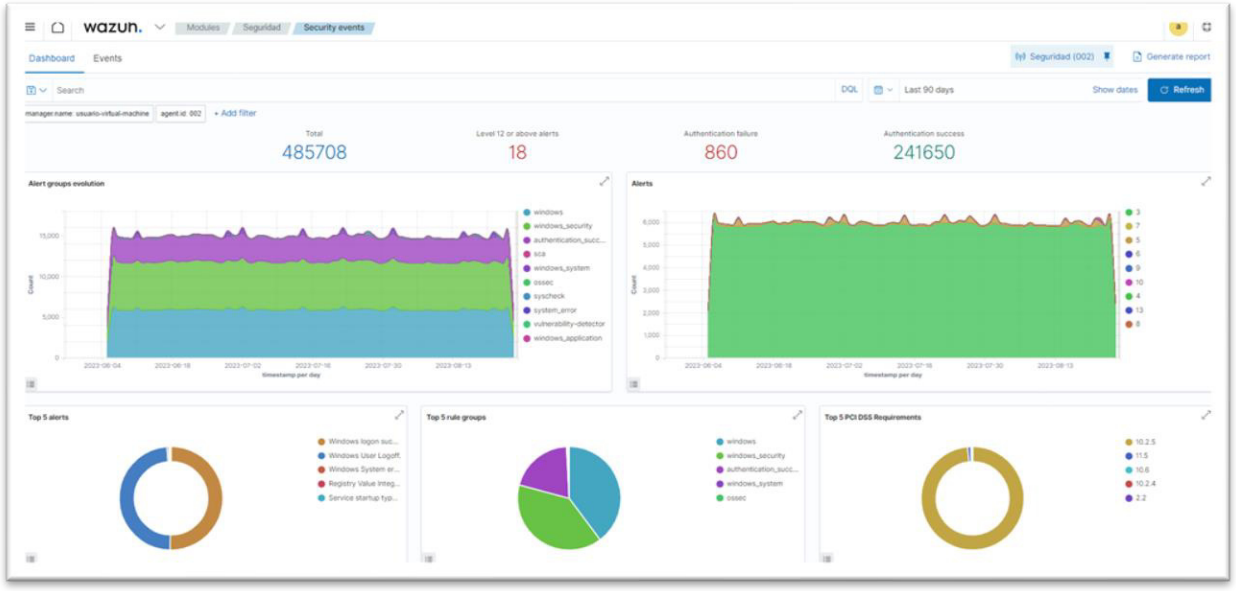
El resultado de las alertas se puede observar que hay modificaciones en la edición en archivos del sistema.

**Resultados del estudio de Wazuh servidor Sistema de Gestión Estratégica (SIGE)**

**Vulnerabilidades**

Tras 90 días de análisis se han obtenido 485.708 eventos, 18 bajas, 860 errores de autenticación, 241.650 autenticación correctas. Todas ellas son del servidor active directory, ya que no ha detectado ninguna alerta en la máquina de Windows server 2016.

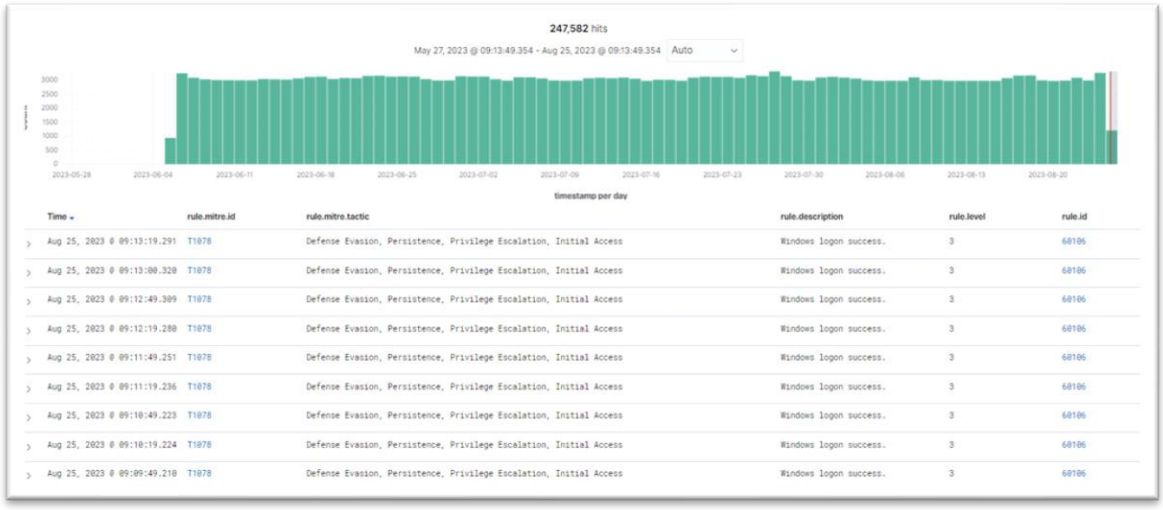
**Figura 15.**
*Visualización de las alertas servidor sistema de gestión estratégica (SIGE)*




Nota: Imagen wazuh servidor institucional Windows server 2016

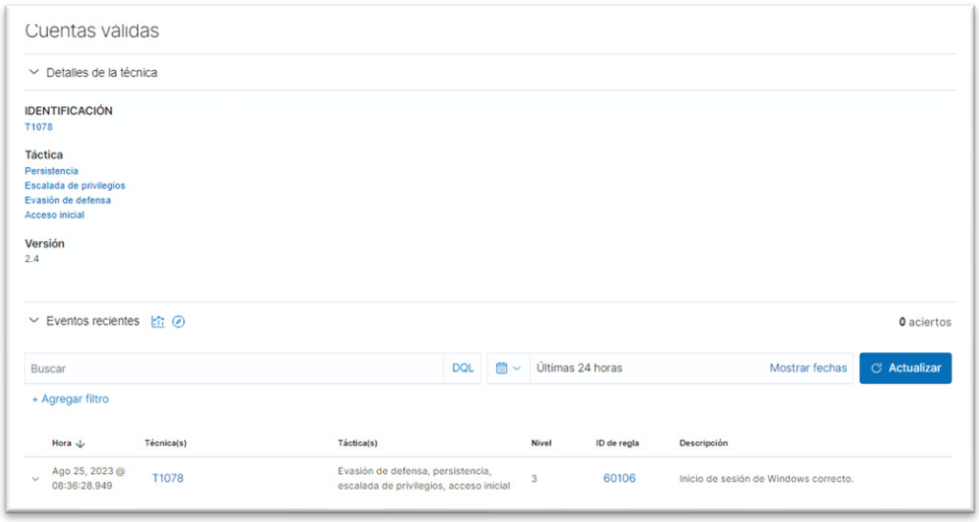
De igual manera las alerta que nos va a proporcionar nos proporciona por medio de mucha información relevante por medio de vulnerabilidades y exposiciones comunes (CVE),

**Figura 16.**
*Descripción referencias servidor sistema de gestión estratégica (SIGE)*




Nota: Imagen wazuh servidor institucional Windows server 2019

**Figura 17.**
*Descripción de alerta active servidor radius Windows server 2019*




Nota: Imagen alertas de eventos servidor radius Windows server 2016

Se ha realizado una selección de las vulnerabilidades más comunes (CVEs) que han aparecido en el análisis y de los paquetes más afectados.

## Vulnerabilidad (T1078)

**Tabla 8.**
*Descripción y solución Vulnerabilidad T1018 Windows 2019*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden obtener y abusar de las credenciales de las cuentas existentes como un medio para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensa. Las credenciales comprometidas se pueden usar para eludir los controles de acceso colocados en varios recursos en sistemas dentro de la red e incluso se pueden usar para el acceso persistente a sistemas remotos y servicios disponibles externamente, como VPN, Outlook Web Access y escritorio remoto. Las credenciales comprometidas también pueden otorgar a un atacante un mayor privilegio para sistemas específicos o acceso a áreas restringidas de la red. |
| **Posibles soluciones:**<br>Audite el dominio y las cuentas locales y sus niveles de permiso, de forma rutinaria para buscar situaciones que permitan a un atacante obtener un amplio acceso obteniendo credenciales de una cuenta privilegiada. |

Nota: Análisis y posibles soluciones vulnerabilidad S.O. Windows Server 2016

## Vulnerabilidad (T1098)

***Tabla 9.***
*Descripción y solución Vulnerabilidad T1098 windows server 2019*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden manipular las cuentas para mantener el acceso a los sistemas de las víctimas. La manipulación de la cuenta puede consistir en cualquier acción que preserve el acceso del adversario a una cuenta comprometida, como modificar credenciales o grupos de permisos. |
| **Posibles soluciones:**<br>Administre la creación, modificación, uso y permisos asociados a cuentas privilegiadas, incluidos SYSTEM y root. |

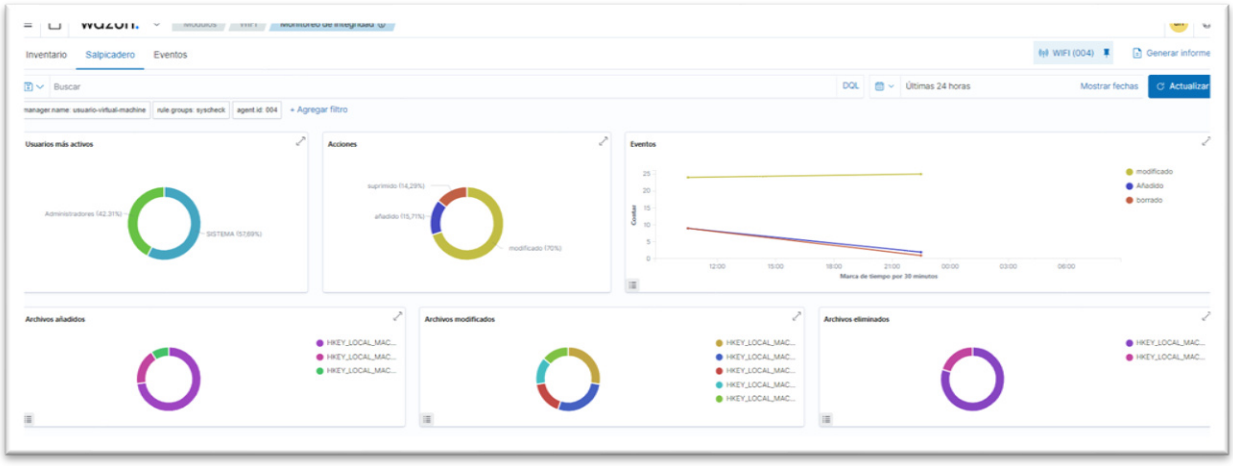
Nota: Análisis y posibles soluciones vulnerabilidad servidor WIFI S.O. Windows Server 2016

Principalmente hay 2 registros que se ven afectados:

\CurrentVersion\Winlogon: es un proceso que implemente la función del gestor de conexión de Windows.

\CurrentControlSet\Services\NTDS\Parameters: es el componente de back-end de Active Directory y almacena todos los datos del dominio.

**Figura 18.**
*Alertas del módulo Integrity Monitoring servidor radius*




Nota: Imagen wazuh servidor institucional eventos servidor radius Windows server 2016

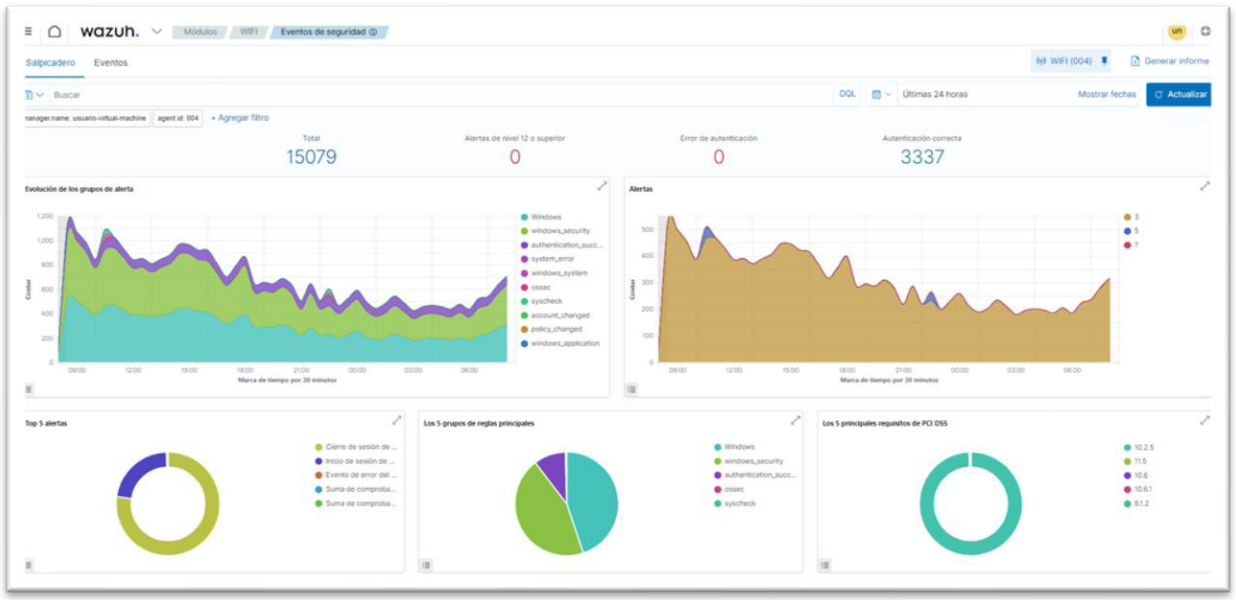
Ha dado como resultado de alertas en las que se puede observar cuando se ha añadido y cuando se ha borrado el archivo. Para ello tendremos que expandir las alertas y ver con más detalle los datos que nos dan

## Resultados del estudio de Wazuh servidor radius con certificados

### Vulnerabilidades

Tras 90 días de análisis se han obtenido 1’729.205 eventos, 0 alertas críticas, 0 errores de autenticación, 223.478 autenticación correctas. Todas ellas son del servidor active directory, ya que no ha detectado ninguna alerta en la máquina de Windows server 2016.

**Figura 19.**
*Visualización de las alertas servidor radius*



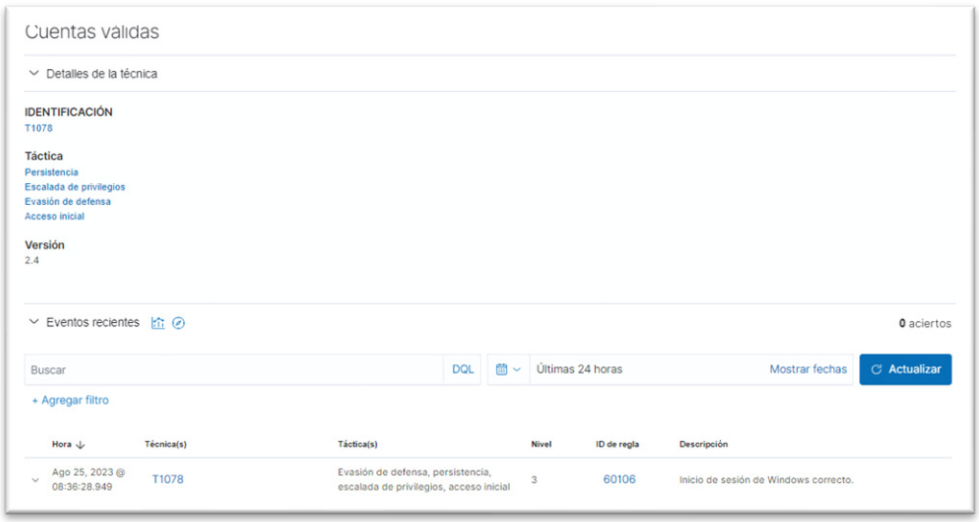

Nota: Imagen wazuh servidor institucional Windows server 2016

De igual manera las alerta que nos va a proporcionar nos proporciona por medio de mucha información relevante por medio de vulnerabilidades y exposiciones comunes (CVE),

**Figura 20.**
*Descripción, impacto y referencias servidor radius*


Nota: Imagen wazuh servidor institucional Windows server 2016

**Figura 21.**
*Descripción de alerta active servidor radius Windows server 2016*




Nota: Imagen alertas de eventos servidor radius Windows server 2016

Se ha realizado una selección de las vulnerabilidades más comunes (CVEs) que han aparecido en el análisis y de los paquetes más afectados.

## Vulnerabilidad (T1078)

**Tabla 10.**
*Descripción y solución Vulnerabilidad T1018 Windows 2016*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden obtener y abusar de las credenciales de las cuentas existentes como un medio para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensa. Las credenciales comprometidas se pueden usar para eludir los controles de acceso colocados en varios recursos en sistemas dentro de la red e incluso se pueden usar para el acceso persistente a sistemas remotos y servicios disponibles externamente, como VPN, Outlook Web Access y escritorio remoto. Las credenciales comprometidas también pueden otorgar a un atacante un mayor privilegio para sistemas específicos o acceso a áreas restringidas de la red. |
| **Posibles soluciones:**<br>Audite el dominio y las cuentas locales y sus niveles de permiso, de forma rutinaria para buscar situaciones que permitan a un atacante obtener un amplio acceso obteniendo credenciales de una cuenta privilegiada. |

Nota: Análisis y posibles soluciones vulnerabilidad S.O. Windows Server 2016

## Vulnerabilidad (T1098)

**Tabla 11.**
*Descripción y solución Vulnerabilidad T1098 windows server 2016*

| |
|---|
| **Información sobre la vulnerabilidad:**<br>Los atacantes pueden manipular las cuentas para mantener el acceso a los sistemas de las víctimas. La manipulación de la cuenta puede consistir en cualquier acción que preserve el acceso del adversario a una cuenta comprometida, como modificar credenciales o grupos de permisos. |
| **Posibles soluciones:**<br>Administre la creación, modificación, uso y permisos asociados a cuentas privilegiadas, incluidos SYSTEM y root. |

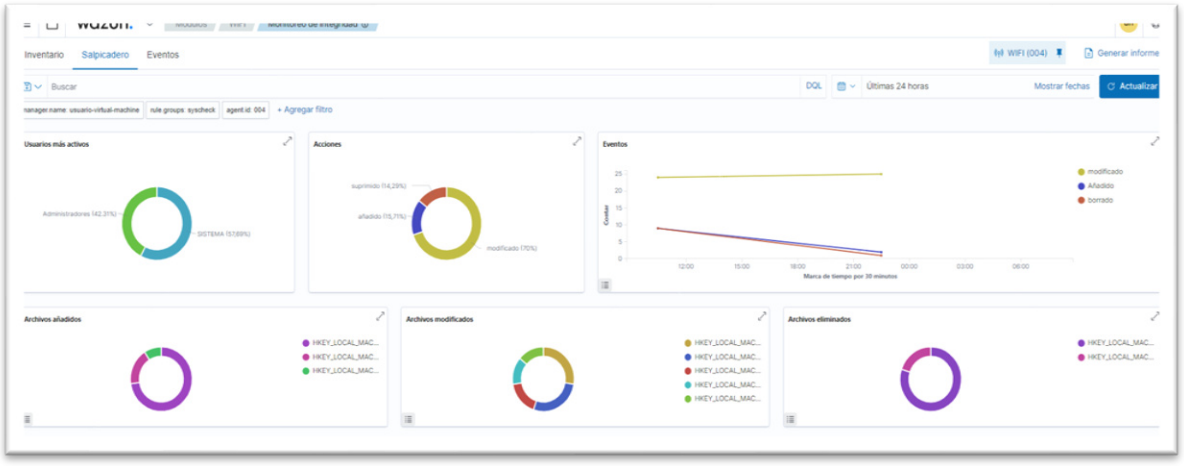
Nota: Análisis y posibles soluciones vulnerabilidad servidor WIFI S.O. Windows Server 2016

Principalmente hay 2 registros que se ven afectados:

\CurrentVersion\Winlogon: es un proceso que implemente la función del gestor de conexión de Windows.

\CurrentControlSet\Services\NTDS\Parameters: es el componente de back-end de Active Directory y almacena todos los datos del dominio.

**Figura 22.**
*Alertas del módulo Integrity Monitoring servidor radius*




Nota: Imagen wazuh servidor institucional eventos servidor radius Windows server 2016

Ha dado como resultado de alertas en las que se puede observar cuando se ha añadido y cuando se ha borrado el archivo. Para ello tendremos que expandir las alertas y ver con más detalle los datos que nos dan.

### 2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

**Tabla 12.**
*Matriz de articulación*

| EJES O PARTES PRINCIPALES | SUSTENTO TEÓRICO | SUSTENTO METODOLÓGICO | ESTRATEGIAS / TÉCNICAS | DESCRIPCIÓN DE RESULTADOS | INSTRUMENTOS APLICADOS |
|---|---|---|---|---|---|
| **SIEM** | Herramienta de gestión de análisis de eventos de correlación de eventos en tiempo real. | Metodología de investigación bibliográfica que permitió tener los conceptos del SIEM | Fuente bibliográfica | Permitió verificar la funcionalidad de la herramienta SIEM | |
| **WAZUH** | Es diseñado para recopilar, analizar y correlacionar eventos de seguridad de la información en tiempo real. Su arquitectura flexible y extensible. | La metodología de investigación fue bibliográfica que permitió tener los conceptos sobre un SIEM | Fuente bibliográfica | Permitió identificar las características generales y específicas de la plataforma de seguridad | |
| **SOFTWARE LIBRE** | Es software cuyo código fuente es libre de estudiar, modificar y utilizar para cualquier fin, y de redistribuir con cambios o mejoras. | La metodología de investigación fue bibliográfica que permitió obtener conceptos de software libre. | Fuente bibliográfica | Permitió conocer la ventaja y desventaja del uso de herramienta en software libre | |

**Nota:** Elaboración propia

## CONCLUSIONES

Las amenazas y vulnerabilidades en seguridad de la información están constantemente renovando y buscando brechas de seguridad es por eso que actualmente que las instituciones de educación superior sean públicas y privadas buscan la forma de mitigar los ataques.

Actualmente más instituciones de educación superior se ven en la imperiosa necesidad de implementar un SIEM, con diferentes tipos de herramientas o soluciones, ya sean en software libre o bajo licencias.

Al analizar las funcionalidades de cada herramienta a implementar en un SIEM, fue muy importante, ya que hay que validar la utilidad de cada herramienta para determinar el alcance de las necesidades.

La elección entre software libre o bajo licencia dependerá en su gran mayoría del tamaño de la organización y del presupuesto económico asignado.

Se elaboró un proceso para levantar un reporte de seguridad según la información recibida por las herramientas aplicadas en el SIEM y de cada servidor de la Universidad Tecnológica Israel.

## RECOMENDACIONES

Responder inmediatamente ante cualquier sospecha de amenaza o vulnerabilidad de los sistemas institucionales, una vez analizadas las brechas desarrollar políticas para mitigar las escaneadas al momento de realizar este trabajo

Realizar un afinamiento mucho más preciso de las herramientas que se implementaron en el SIEM

Mantener como un proceso inicial las herramientas de seguridad bajo software libre para adquirir conocimiento de los reportes y luego proponer a las instituciones herramientas más especializadas y con licencia para mitigar los ciberataques.

Mantener constantemente actualizados los sistemas operativos de los servidores que se desarrolló el presente trabajo y de las herramientas del SIEM que son bajo software libre para evitar vulnerabilidades en las mismas

Cumplir con el proceso de reportes de seguridad indicado y mantener dichos reportes cada día para poder evaluar, auditar o recomendar a los directivos sobre temas de seguridad

## BIBLIOGRAFÍA


Aldaz López, W. (2019). “Vulnerabilidades de Seguridad Informática en la Administración Zonal Norte “Eugenio Espejo” a través del Phishing”. Universidad Tecnológica Israel.

Alonso, C. (5 de Marzo de 2020). *globalsuitesolutions*. Obtenido de globalsuitesolutions: https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:~:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

Anscombe, T. (8 de 7 de 2021). *welivesecurity*. Obtenido de Ransomware: ¿Pagar o no pagar? ¿Es legal o ilegal?: https://www.welivesecurity.com/la-es/2021/07/08/ransomware-pagar-o-no-pagar-es-legal-o-ilegal/

ATICO34. (5 de Octubre de 2018). *Hosting pedia*. Obtenido de Hosting pedia: https://hostingpedia.net/copias-de-seguridad.html

BSIGROUP. (4 de Junio de 2022). *bsigroup*. Obtenido de bsigroup: https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

Bulletin, M. S. (14 de 10 de 2022). *microsoft*. Obtenido de microsoft: https://learn.https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-023?source=recommendations.com/en-us/security-updates/securitybulletins/2017/ms17-023?source=recommendations

Ceruzzi, P. E. (2015). *BBAOPENMIND*. Obtenido de BBAOPENMIND: https://www.bbvaopenmind.com/articulos/historia-de-la-informatica/

Cloudflare. (27 de Marzo de 2020). *cloudflare*. Obtenido de cloudflare: https://www.cloudflare.com/es-es/learning/cloud/what-is-a-cloud-firewall/

cloudflare. (2022). *cloudflare*. Obtenido de https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

Cyber Edge Group. (2022). *Cyber Edge* . Obtenido de https://cyber-edge.com/wp-content/uploads/2022/11/CyberEdge-2022-CDR-Report.pdf

Edix. (4 de 1 de 2023). *Edix*. Obtenido de Edix: https://www.edix.com/es/instituto/seguridad-activa-y-pasiva-informatica/

Fernandez, Y. (6 de Marzo de 2020). *Ayuda le proteccion datos*. Obtenido de Ayuda le proteccion datos: https://ayudaleyprotecciondatos.es/2022/02/11/encriptacion-datos/#:~:text=La%20encriptaci%C3%B3n%20de%20datos%20es%20un%20proceso%20de,la%20informaci%C3%B3n%20mientras%20viaja%20del%20emisor%20al%20receptor.

INTEDYA. (1 de Septiembre de 2019). *INTEDYA*. Obtenido de INTEDYA INTERNATIONAL DYNAMIC ADVISORS: https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

kaspersky. (2022). *kaspersky*. Obtenido de Qué es el ransomware WannaCry.

Klusaité, L. (7 de Abril de 2022). *NordVPN*. Obtenido de NordVPN: https://nordvpn.com/es/blog/seguridad-cloud-computing/

Lavín, N. (7 de 4 de 2022). *https://cloner.cl/*. Obtenido de ¿Por qué hacer monitoreo de seguridad informática en tu empresa?

Marc RiveroLopez. (30 de 4 de 2020). *trellix*. Obtenido de Tales From the Trenches; a Lockbit Ransomware Story: https://www.trellix.com/en-us/about/newsroom/stories/research/tales-from-the-trenches-a-lockbit-ransomware-story.html

Martínez, E. (21 de Abril de 2021). *Seguridad en América*. Obtenido de Seguridad en América: https://www.seguridadenamerica.com.mx/noticias/articulos/27438/soluciones-de-seguridad-en-data-centers

Méndez. (2008). *La investigación bibliográfica se puede comprender.*

Moes, T. (25 de Marzo de 2018). *SoftwareLab*. Obtenido de SoftwareLab ORG: https://softwarelab.org/es/que-es-un-firewall/

Morales, F. (16 de Febrero de 2022). *Sysadminis de Cuba*. Obtenido de https://www.sysadminsdecuba.com/2022/02/servidor-wazuh-siem/

Mundhada, C. (Enero de 2019). Obtenido de https://www.darkreading.com/vulnerabilities-threats/the-evolution-of-siem

Naciones Unidas Ecuador. (2023). *Naciones Unidas Ecuador*. Obtenido de https://ecuador.un.org/es/sdgs/9

Narvaez, M. (2023). *Questionpro*. Obtenido de https://www.questionpro.com/blog/es/metodo-inductivo/

NORMA ISO. (25 de Junio de 2019). *normaiso27001*. Obtenido de normaiso27001: https://advisera.com/27001academy/es/que-es-iso-27001/

O'Brien, D. (Julio de 2017). *Ransomware*. Obtenido de Informe sobre amenazas a la seguridad de Internet, Symantec: https://www.symantec.com/content/dam/symantec/docs/ securitycenter/white-papers/istr-ransomware-2017-en.pdf

Ramírez, A. (1 de Junio de 2022). *Community*. Obtenido de FS Community: https://community.fs.com/blog/what-is-a-data-center-firewall.html

Solís, L. D. (26 de noviembre de 2019). *Investigaliacr*. Obtenido de Investigaliacr.

theZoo. (19 de 08 de 2022). *Ytisf*. Obtenido de https://github.com/ytisf/theZoo/tree/master/malware/Binaries

Universidad de Veracruz. (2022). *Universidad de Veracruz*. Obtenido de https://www.uv.mx/apps/bdh/investigacion/unidad1/investigacion-tipos.html

Wazuh. (2023). *Wazuh*. Obtenido de Wazuh: https://documentation.wazuh.com/current/getting-started/components/wazuh-indexer.html

## ANEXOS

### Anexos 1

| Check list de verificación de seguridad informática Universidad Tecnológica Israel | | | | | | |
|---|---|---|---|---|---|---|
| **SEGURIDAD DE DATOS** | | | | | | |
| | | **CUMPLE** | | **RIESGO** | | |
| **INDICADOR** | **ASPECTO A EVALUAR** | **SI** | **NO** | **BAJO** | **MEDIO** | **ALTO** |
| 1 | La organización tiene definidas políticas de seguridad informática | X | | X | | |
| 2 | Las políticas de seguridad informática son revisadas periódicamente | | X | | | X |
| 3 | Se dispone de un inventario de activos tecnológicos | X | | X | | |
| 4 | Se monitoriza y registra la actualización, instalación de software en equipos de producción | X | | X | | |
| 5 | Se tiene definidos perfiles de usuario para evitar la instalación de software en pc de usuarios finales | X | | X | | |
| 6 | Dispone de implementación de listas de control de acceso (ACL) | X | | X | | |
| 7 | Se tiene software antivirus licenciado instalado en cada uno de los computadores que cuenta la organización | | X | | | X |
| 8 | Se tiene instalado antimalware en los equipos de la organización | X | | | X | |
| 9 | Se dispone de repositorios externos para salvaguarde backup y datos relevantes | X | | X | | |
| 10 | Se monitoriza y registra la actividad de las líneas telefónica | X | | X | | |
| **SEGURIDAD DE INFRAESTRUCTURA Y SERVICIO** | | | | | | |
| | | **CUMPLE** | | **RIESGO** | | |
| **INDICADOR** | **ASPECTO A EVALUAR** | **SI** | **NO** | **BAJO** | **MEDIO** | **ALTO** |
| 11 | Se dispone de firewall | X | | X | | |
| 12 | Se han definido y documentado parámetros de seguridad (DMZ en la intranet para equipos con información de alto riesgo) | | X | | X | |
| 13 | Se dispone, implementado un sistema de protección anti-DDOS | X | | X | | |
| 14 | Dispone de redundancia de hardware | X | | X | | |
| 15 | Dispone de redundancia de software | X | | X | | |
| 16 | La organización cuenta con procesos para brindar mantenimiento preventivo al software | X | | X | | |
| 17 | La organización cuenta con procesos para brindar mantenimiento preventivo al hardware | X | | X | | |
| 18 | Dispone con contratos externos de soporte | X | | X | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | Dispone de ups en cada estación de trabajo | | X | | X | |
| 20 | Las instalaciones eléctricas cuentan con bajada de tierra | X | | X | | |
| **CONTROLES DE ACCESO** | | | | | | |
| | | **CUMPLE** | | **RIESGO** | | |
| **INDICADOR** | **ASPECTO A EVALUAR** | **SI** | **NO** | **BAJO** | **MEDIO** | **ALTO** |
| 21 | Se ha definido e implementado un proceso para la creación de usuario su contraseña | X | | X | | |
| 22 | Se ha definido un proceso de altas y bajas de usuarios | | X | | X | |
| 23 | Se dispone de controles de acceso lógico a los servicios críticos de TI que dispone la organización | X | | X | | |
| 24 | Se monitoriza y registra la actividad de accesos lógicos en los equipos críticos que dispone | X | | X | | |
| 25 | En los equipos de los usuarios finales dispone de dos cuentas de inicio de sesión una como administrador y otra como usuario normal | X | | X | | |
| 26 | Se dispone de controles de accedo físico al data center de la organización | | X | | X | |
| 27 | Se monitoriza y registra la actividad de accesos físicos al data center de la organización | | X | | | X |
| 28 | Se monitoriza y autentica las conexiones a la red inalámbrica de la organización | X | | X | | |
| **PLANES DE RESPALDO** | | | | | | |
| | | **CUMPLE** | | **RIESGO** | | |
| **INDICADOR** | **ASPECTO A EVALUAR** | **SI** | **NO** | **BAJO** | **MEDIO** | **ALTO** |
| 29 | Se tiene establecido políticas de backup en caso de desastres | X | | X | | |
| 30 | Se ha documentado e implementado un proceso para la gestión de incidentes de seguridad informática | | X | X | | |
| 31 | Se ha definido planes de continuidad y respaldos de la información critica | X | | X | | |
| 32 | Se tiene definido planes de continuidad de negocio en la organización | X | | X | | |
| 33 | Dispones la organización de respaldos de energía eléctrica en caso de fallas | X | | X | | |
| 34 | Dispone de cuartos de acometidas para los servicios provistos por proveedores externos | | X | | X | |
| **HÁBITOS DE SEGURIDAD Y PREPARACIÓN** | | | | | | |
| | | **CUMPLE** | | **RIESGO** | | |
| INDICADOR | **ASPECTO A EVALUAR** | **SI** | **NO** | **BAJO** | **MEDIO** | **ALTO** |
| 35 | Cuenta con políticas de seguridad de los equipos respecto al consumo de alimentos bebidas | | X | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| 36 | Cuenta con planes de capacitación al personal sobre seguridad informática | | X | | X | |
| 37 | Se dispone de un plan de manejo seguro de datos críticos | X | | X | | |
| 38 | Se destruyen discos duros catalogados como dañados | | X | | | X |
| 39 | El personal de la empresa se conduce y aplica hábitos seguros de manejo de la información | X | | X | | |
| 40 | En general la actitud hacia la aplicación de normas de seguridad es positiva | X | | X | | |

**Formato de validación**

**Anexos 2**

| |
|---|
| Nombres: Diego Endara |
| Título profesional: Mg. Tecnologías de la Información y Comunicación |
| Correo: dendara@uisrael.edu.ec |
| Celular: 0985710699 |
| Cargo laboral: Asistente de Recursos Tecnológicos |
| Indique una vez leído el documento por favor le parece funcional y aporte a la Universidad Tecnológica Israel |
| La propuesta de monitorización de estos eventos es funcional en la Universidad Tecnológica Israel, en especial en el servidor AD institucional que a la vez funciona como DNS, si nos planteamos esto la Universidad Tecnológica Israel al momento de perder este servidor por un ataque de seguridad no detectado a tiempo, dejaría a las autoridades, personal administrativo, docentes y estudiantes sin servicio de Internet, y sin poder autenticarse a nivel local, perdiendo la posibilidad de avanzar con cualquier tipo de trabajo dentro de la institución, es por eso que la propuesta es funcional y se adapta a las necesidades actuales en cuanto a tecnología.<br>Se debe tomar en consideración que WAZUH es una herramienta de código abierto con posibilidades de análisis, detección y corrección de amenazas, dando un plus a la parte financiera a un proyecto de estas dimensiones. |
| Firma:  |

**Formato de validación**

**Anexos 2**

| |
|---|
| Nombres: Mg. Edwin Lagos Lara |
| Título profesional: Ingeniero en Sistemas |
| Correo: elagos@uisrael.edu.ec |
| Celular: 0995024666 |
| Cargo laboral: Director de Recursos Tecnológicos |
| Indique una vez leído el documento por favor le parece funcional y aporte a la Universidad Tecnológica Israel |
| La implementación de Wazuh en la UISRAEL, es de gran ayuda ya que contiene:<br>✓ Detección de amenazas<br>✓ Integración con Elasticsearch y Kibana<br>✓ Monitorización en tiempo real<br>✓ Automatización de respuestas<br>✓ Integración con otros sistemas<br><br>Todo esto, permitirá detectar comportamientos maliciosos y actividades sospechosas en el tráfico de nuestra red en tiempo real, para que el administrador de Seguridad de la UISRAEL, pueda responder rápidamente a incidentes de seguridad.<br><br>Además, permite la automatización de respuestas a eventos de seguridad mediante acciones predefinidas, como bloquear direcciones IP sospechosas o tomar medidas específicas en función del tipo de amenaza detectada.<br><br>Sin duda la implementación de esta herramienta Wazuh, brindará seguridad a nuestra infraestructura digital, mejorando la administración y disponiendo de un mecanismo de defensa ante un sin número de ataques que ocurren diariamente en el mundo. |
| Firma:<br>  |

**Formato de validación**

**Anexos 2**

| |
|---|
| Nombres: Juan Francisco Pabón Alajo |
| Título profesional: Máster en Inteligencia Artificial |
| Correo: jfpabon@uisrael.edu.ec |
| Celular:0997177712 |
| Cargo laboral: Asistente del DRT |
| Indique una vez leído el documento por favor le parece funcional y aporte a la Universidad Tecnológica Israel |
| El sistema Wazuh es una solución altamente funcional que desempeña un papel fundamental en la seguridad y monitorización, siendo ampliamente adoptado por organizaciones con el propósito de detectar, analizar y responder eficazmente a las amenazas de seguridad en sus entornos informáticos.<br><br>Dentro de este contexto, el proyecto de tesis llevado a cabo por el Ingeniero Fernández Danny, titulado 'Propuesta de Monitoreo de Eventos de Seguridad con Wazuh para Instituciones de Educación Superior', destaca por su notable funcionalidad y su aporte sumamente significativo en lo que respecta al monitoreo y control de amenazas en el Data Center de la institución en la cual ha sido implementado. |
| Firma: JUAN FRANCISCO PABON ALAJO |