

TECNICATURA UNIVERSITARIA EN

CIBERSEGURIDAD



**SISTEMAS DE GESTIÓN DE SEGURIDAD
DE LA INFORMACIÓN (MARCOS
NORMATIVOS)**

Trabajo práctico final de la materia
**Universidad del
Gran Rosario**

**Profesor: Lic. Juan Pablo Villalba
Tec. Tomás Navarro**

**Alumno: Balbuena Atar Dante Gabriel
Tucumán, Tafí Viejo – noviembre 2024**

Índice

Introducción	3
• Contexto de la ciberseguridad para PyMEs en Argentina	
• Importancia de las herramientas de código abierto en la seguridad	
• Objetivo del trabajo	
Resumen de Herramientas	6
Wazuh	6
• Funcionalidades	
• Rol en el cumplimiento normativo	
Graylog	6
• Gestión y análisis de registros	
• Integración con Wazuh	
Snort/Suricata	6
• Detección y prevención de intrusiones	
• Relevancia para la seguridad de red	
Yara	6
• Detección de malware	
• Uso en combinación con Wazuh	
VirusTotal	6
• Análisis de archivos y URLs sospechosas	

- Integración con otras herramientas

MITRE ATT&CK 7

- Marco de referencia de tácticas y técnicas de ataque
- Uso para mejorar la respuesta ante incidentes

MikroTik 7

- Control de accesos y seguridad en red
- Integración con Wazuh y Graylog

Integración de Herramientas 11

- Centralización y visualización de eventos: Wazuh y Graylog
- Detección y alerta de intrusiones: Wazuh y Snort/Suricata
- Análisis y verificación de malware: Yara y VirusTotal
- Correlación de técnicas de ataque: Wazuh y MITRE ATT&CK
- Monitoreo de red y control de accesos: dispositivos MikroTik

Cumplimiento Normativo 19

- GDPR (Reglamento General de Protección de Datos)
- PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago)
- ISO 27001 (Sistema de Gestión de Seguridad de la Información)
- CIS Controls
- NIST (Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología)
- Ley Argentina 25.326 de Protección de Datos Personales

Matriz de Cumplimiento Normativo 21

Ejemplo Hipotético de Respuesta a un Ataque de Fuerza Bruta 21

- Escenario del ataque
- Flujo de alertas y respuesta
- Análisis y mapeo con MITRE ATT&CK
- Respuesta y medidas de mitigación

Propuestas de Mejora para la Integración de Seguridad 23

- Sincronización de alertas
- Actualización de reglas de detección
- Automatización de bloqueos de IP

Conclusiones 24

- Resumen de beneficios de la integración
- Áreas de mejora para el cumplimiento total

Referencias 24

1. Introducción

En un contexto de economía fluctuante como el de Argentina, las pequeñas y medianas empresas (PyMEs) deben afrontar el desafío de mantenerse a flote y competitivas sin perder de vista la protección de sus activos digitales. Estas empresas, debido a sus limitaciones de recursos, se ven particularmente expuestas a riesgos de ciberseguridad que pueden afectar su operatividad y dañar su reputación en el mercado.

Dada esta situación, las soluciones de ciberseguridad accesibles resultan fundamentales para que las PyMEs puedan resguardar su información sin incurrir en elevados costos. Herramientas de código abierto como Wazuh, Graylog y Snort ofrecen capacidades avanzadas para el monitoreo y la detección de amenazas a costos significativamente menores en comparación con alternativas comerciales, lo que permite a estas empresas establecer un sistema de seguridad adecuado y accesible.

Entre estas herramientas, Wazuh se posiciona como un elemento central en el esquema de seguridad de las PyMEs, ya que permite monitorear logs, detectar intrusiones y facilitar el cumplimiento normativo en una plataforma unificada. Al integrarse con otras soluciones de seguridad, permite una respuesta coordinada ante posibles amenazas, lo que resulta crucial para empresas que deben optimizar sus recursos.

El uso combinado de herramientas de seguridad de código abierto permite a las PyMEs implementar un sistema de monitoreo y protección continuo, que abarca diferentes capas de defensa. Por ejemplo, Graylog facilita la gestión y visualización de registros, mientras que Snort se enfoca en la detección y prevención de intrusiones en tiempo real. Además, Yara permite identificar patrones de malware en archivos, y VirusTotal realiza comprobaciones de URLs y archivos sospechosos en busca de posibles amenazas.

También, el marco MITRE ATT&CK ofrece una guía para identificar y entender técnicas de ataque, y MikroTik permite controlar los accesos en la red, contribuyendo cada herramienta a un enfoque de seguridad integral.

Este trabajo se propone investigar cómo la adopción de herramientas de seguridad de código abierto ayuda a las PyMEs a cumplir con diversas normativas, como GDPR, PCI DSS, ISO 27001 y la Ley de Protección de Datos Personales en Argentina. También se plantearán recomendaciones para mejorar la detección y mitigación de amenazas en entornos con recursos limitados.

2. Desarrollo

1. Resumen de Herramientas

Para implementar un sistema integral de seguridad que permita a las PyMEs proteger sus activos digitales y cumplir con normativas clave, se han seleccionado varias herramientas de código abierto con roles específicos y bien definidos. A continuación, se presenta un resumen técnico de cada una:

Wazuh

Wazuh es una plataforma open-source de monitoreo y análisis de seguridad, que permite gestionar registros, detectar intrusiones y asegurar el cumplimiento de normativas de seguridad. Su arquitectura distribuida facilita el análisis en tiempo real de grandes volúmenes de datos de diferentes sistemas, ayudando a las organizaciones a monitorear su infraestructura de TI y a responder proactivamente ante amenazas. Con funciones avanzadas como la detección de cambios en archivos (FIM), gestión de vulnerabilidades y monitoreo de integridad, Wazuh es compatible con normativas como GDPR, PCI DSS e ISO 27001, proporcionando informes detallados que simplifican las auditorías de seguridad.

Graylog

Graylog es una potente plataforma para la gestión y análisis de registros, ideal para centralizar, procesar y visualizar grandes cantidades de datos en tiempo real desde dispositivos, aplicaciones y sistemas de red. Su utilidad en la investigación de problemas de seguridad y en la detección de patrones sospechosos es invaluable, permitiendo a los equipos de TI realizar consultas complejas y personalizar tableros de control. Graylog se complementa eficazmente con otras herramientas, como Wazuh, facilitando la correlación de eventos y una respuesta más eficiente a las amenazas.

Snort/Suricata

Snort y Suricata son sistemas de detección y prevención de intrusiones (IDS/IPS) que permiten identificar y, en algunos casos, bloquear actividades maliciosas en tiempo real mediante la inspección profunda de paquetes (DPI). Snort es uno de los IDS más utilizados por su amplia biblioteca de reglas, mientras que Suricata destaca por su capacidad para analizar tráfico en múltiples hilos, ideal en entornos de alto volumen. Ambas herramientas son esenciales para detectar amenazas de red, como ataques de fuerza bruta o tráfico malicioso, reforzando la defensa en profundidad de la organización.

Yara

Yara es una herramienta de código abierto diseñada para identificar y clasificar archivos sospechosos mediante reglas definidas por el usuario, siendo ampliamente utilizada en la investigación de malware. Cada regla en Yara permite definir patrones específicos para detectar amenazas en archivos y procesos del sistema, convirtiéndola en una herramienta flexible y poderosa para identificar variantes de malware. Integrada en sistemas de monitoreo como Wazuh, Yara facilita la detección temprana de archivos potencialmente maliciosos, crucial para la defensa contra amenazas avanzadas (APT).

VirusTotal

VirusTotal es una plataforma que permite analizar archivos y URLs sospechosas usando múltiples motores antivirus y herramientas de detección. Es particularmente útil para validar la detección de archivos sospechosos en tiempo real, verificando si estos han sido identificados como maliciosos

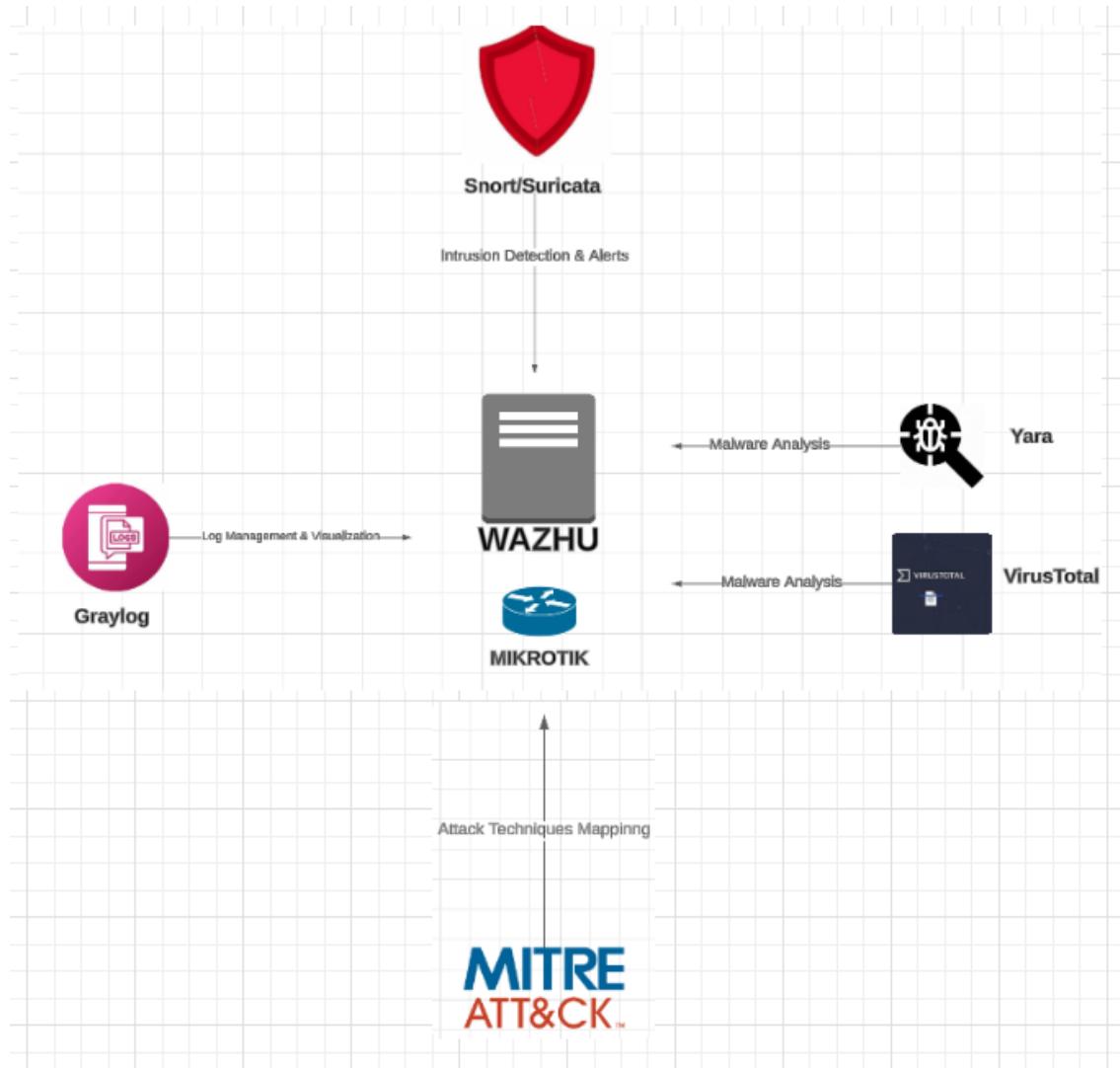
en otros sistemas. Integrar VirusTotal con herramientas como Yara o Wazuh mejora la capacidad de respuesta ante amenazas al añadir una capa adicional de verificación para los equipos de TI.

MITRE ATT&CK

MITRE ATT&CK es un marco de referencia que documenta tácticas, técnicas y procedimientos (TTPs) utilizados en ciberataques, organizando amenazas por patrones de ataque. Al integrar MITRE ATT&CK con herramientas como Wazuh y Graylog, se facilita la correlación de eventos y el mapeo de actividades maliciosas, proporcionando una comprensión detallada de los patrones del atacante y ayudando a predecir posibles vectores de ataque. Este marco permite planificar respuestas basadas en amenazas conocidas, fortaleciendo las estrategias de defensa.

MikroTik

MikroTik es una línea de dispositivos de red, como routers y firewalls, que ofrecen rendimiento y accesibilidad. Monitorizar dispositivos MikroTik mediante decodificadores personalizados en Wazuh permite registrar accesos y cambios en la configuración, mejorando la seguridad de la red al rastrear intentos de acceso no autorizados. La integración de estos registros con Graylog permite correlacionar eventos de seguridad y detectar amenazas en tiempo real, ofreciendo a las PyMEs un nivel de visibilidad y protección comparables a los de infraestructuras mayores.



2. Integración de Herramientas

Para implementar un sistema de seguridad eficaz y coherente en entornos de PyMEs, es crucial integrar herramientas de seguridad open-source que trabajen en sincronía, maximizando la detección de incidentes y la respuesta a amenazas. La configuración y el flujo de información entre herramientas como Wazuh, Graylog, Snort, Yara, VirusTotal y el marco MITRE ATT&CK aumentan la capacidad de monitoreo y facilitan el cumplimiento normativo.

Centralización y Visualización de Eventos: Wazuh y Graylog

Wazuh y Graylog son piezas clave para centralizar y analizar los registros de seguridad. Wazuh recopila datos de distintas fuentes, generando alertas ante eventos de seguridad como accesos no autorizados o modificaciones de archivos críticos. Estas alertas se envían a Graylog, que permite visualizarlas y analizarlas a través de su interfaz gráfica en tiempo real. Gracias a esta integración, los administradores pueden centralizar eventos, filtrar alertas mediante búsquedas personalizadas y detectar patrones de amenazas. La correlación de eventos resulta esencial para reconocer incidentes complejos, reduciendo el tiempo de respuesta y facilitando la identificación de anomalías en la red.

Integración de Wazuh con Graylog

Configuración de salida de logs en Wazuh: Para enviar logs de Wazuh a Graylog, puedes configurar Wazuh para que utilice el protocolo Syslog y dirija sus registros hacia el puerto donde Graylog escucha mensajes de Syslog (por defecto, el puerto 514).

Ejemplo de configuración en Wazuh:

```
# Archivo de configuración en Wazuh (/var/ossec/etc/ossec.conf)

<output>

    <syslog>
        <server>IP_GRAYLOG_SERVER</server>
        <port>514</port>
        <format>json</format>
    </syslog>
</output>
```

Configuración de entrada en Graylog: En Graylog, crea una entrada Syslog para recibir los logs.

1. Ve a *System > Inputs* y selecciona *Syslog UDP*.
2. Configura el puerto (514) y cualquier filtro o tag adicional.

Beneficio: Esta configuración permite que los registros y alertas de Wazuh se visualicen y analicen en Graylog, centralizando la gestión de eventos de seguridad.



Estos dos fragmentos de código que se mostraron tanto en la imagen (ossec.conf) como por texto (syslog) , cumplen funciones relacionadas. La diferencia principal entre los dos fragmentos de configuración en Wazuh, se encuentra en los detalles de la **configuración de salida de logs** y en **cómo se especifica el formato y protocolo de envío hacia Graylog**.

syslog

```
# Archivo de configuración en Wazuh (/var/ossec/etc/ossec.conf)

<output>

  <syslog>
    <server>IP_GRAYLOG_SERVER</server>
    <port>514</port>
    <format>json</format>
  </syslog>
</output>
```

Explicación

1. Este bloque define la **salida de logs de Wazuh en formato Syslog**.
2. Especifica que el servidor de destino (Graylog) está en IP_GRAYLOG_SERVER y que los logs se envían a través del **puerto 514**.
3. Se define el **formato de salida como JSON** (<format>json</format>), lo que significa que los logs se estructurarán en formato JSON cuando se envíen a Graylog.
4. **Protocolo:** Aquí no se especifica explícitamente si el protocolo es UDP o TCP, pero por defecto, Syslog suele usar UDP si no se especifica otro protocolo.

Este fragmento es ideal cuando quieras que los logs se envíen a Graylog en un formato estructurado como JSON, facilitando el procesamiento y análisis en Graylog.

Ossec.config

```
<ossec_config>  
  <remote>  
    <connection>  
      <protocol>udp</protocol>  
      <address>Graylog_IP_address</address>  
      <port>514</port>  
    </connection>  
  </remote>  
</ossec_config>
```

Explicación

1. Este bloque también define una **conexión remota desde Wazuh hacia Graylog**, pero está configurando más directamente el **protocolo de envío de logs (UDP)**.
2. Aquí, el protocolo está explícitamente definido como **UDP** (<protocol>udp</protocol>), lo que garantiza que Wazuh utilizará UDP para enviar los logs.
3. El servidor de destino es Graylog_IP_address, y el **puerto es el 514**, que es el puerto estándar de Syslog.
4. **Formato:** En este caso, no se especifica un formato de log (como JSON). Por lo tanto, los logs se envían en el formato predeterminado de Syslog, que suele ser texto plano.

Este segundo fragmento es adecuado si prefieres que los logs se envíen en texto plano y deseas especificar explícitamente el protocolo (UDP o TCP).



Detección y Alerta de Intrusiones: Wazuh y Snort/Suricata

Snort y Suricata, como sistemas de detección y prevención de intrusiones (IDS/IPS), monitorean el tráfico de red en busca de patrones asociados a ataques conocidos, como fuerza bruta o intentos de explotación de vulnerabilidades. Al detectar un evento sospechoso, Snort genera una alerta que se envía a Wazuh, donde se almacena y se correlaciona con otros eventos del sistema. Esta colaboración permite analizar estos eventos de red en conjunto con otros registros de seguridad, mejorando la identificación de ataques avanzados y permitiendo que el equipo de seguridad actúe rápidamente ante amenazas.

Integración de Snort con Wazuh

Instalación de Snort: Instala Snort y configura sus reglas en /etc/snort/snort.conf.

Enviar alertas de Snort a Wazuh:

1. Configura Snort para guardar alertas en formato JSON y permite que Wazuh lea estos archivos.
2. Edita el archivo de configuración de Wazuh para habilitar la decodificación de alertas de Snort.

Ejemplo de configuración en Wazuh:

```
# Configuración en /var/ossec/etc/ossec.conf para monitorear las alertas de Snort

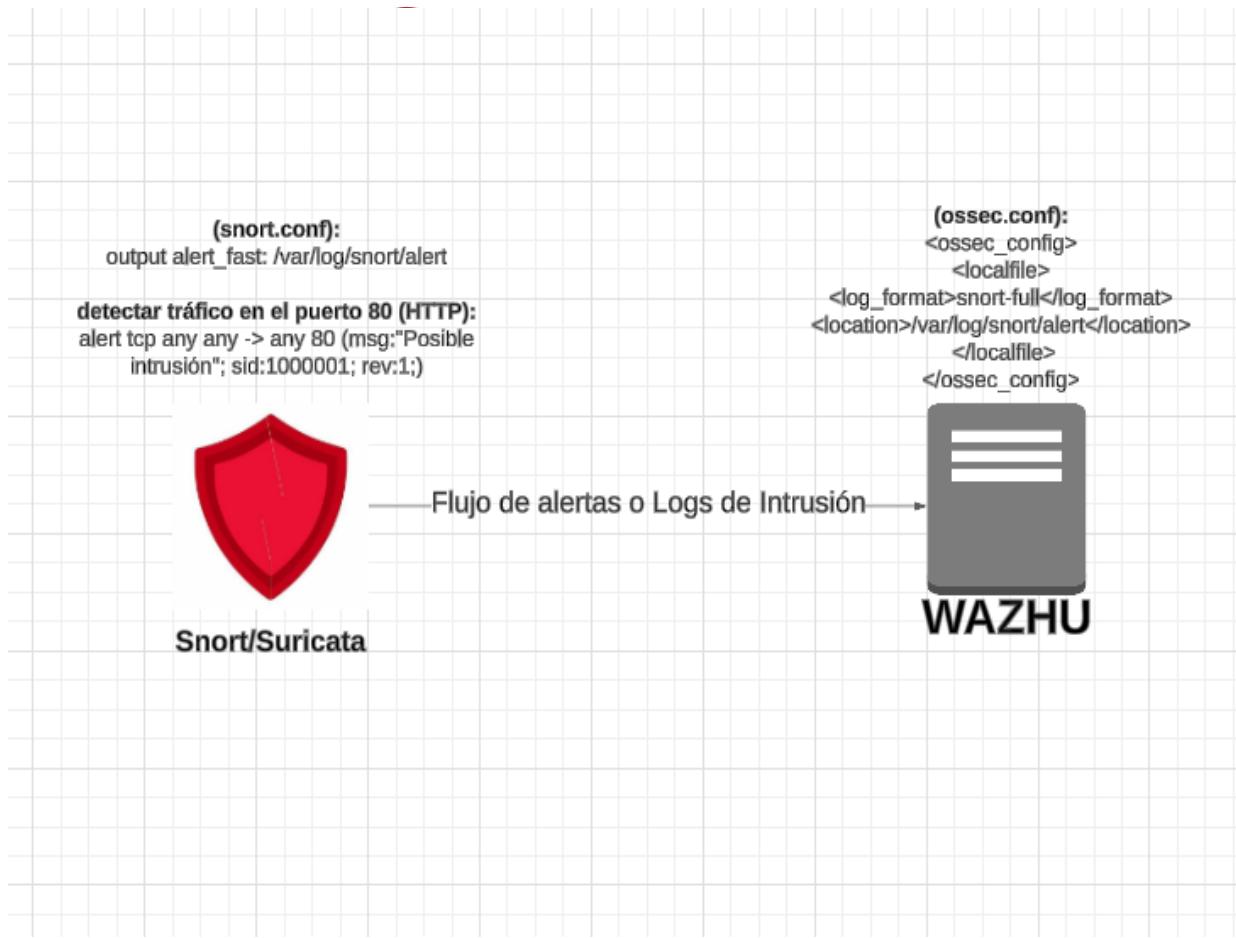
<localfile>

    <log_format>snort-full</log_format>

    <location>/var/log/snort/alert</location>

</localfile>
```

Beneficio: Al integrarse, Wazuh correlaciona las alertas de Snort con otros eventos del sistema, brindando un contexto más amplio para cada alerta.



Análisis y Verificación de Malware: Yara y VirusTotal

Yara y VirusTotal son herramientas especializadas en la detección de malware que complementan a Wazuh en la identificación de archivos maliciosos. Yara permite definir patrones de búsqueda que detectan variantes de malware específicas en archivos o procesos. Al detectar un archivo sospechoso, se genera una alerta que se envía a Wazuh. Luego, para una verificación adicional, el archivo puede enviarse a VirusTotal, donde es evaluado por múltiples motores antivirus. La respuesta de VirusTotal se almacena en Wazuh, permitiendo una evaluación más precisa del riesgo. Este proceso asegura que los administradores puedan identificar y mitigar amenazas con mayor precisión y evitar la propagación de malware en la red.

Integración de Yara con Wazuh

Configuración de reglas en Yara: Define reglas personalizadas en Yara para detectar patrones específicos de malware y almacénalas en `/etc/yara_rules`.

Integración con Wazuh:

1. Configura Wazuh para que ejecute Yara en los archivos del sistema o en directorios específicos.
2. En el archivo de configuración de Wazuh, agrega la ruta de las reglas de Yara y especifica los directorios a escanear.

Ejemplo de configuración en Wazuh:

```
# En /var/ossec/etc/ossec.conf

<syscheck>

    <directories check_all="yes">/etc,/var/www</directories>

    <yara_rules_path>/etc/yara_rules</yara_rules_path>

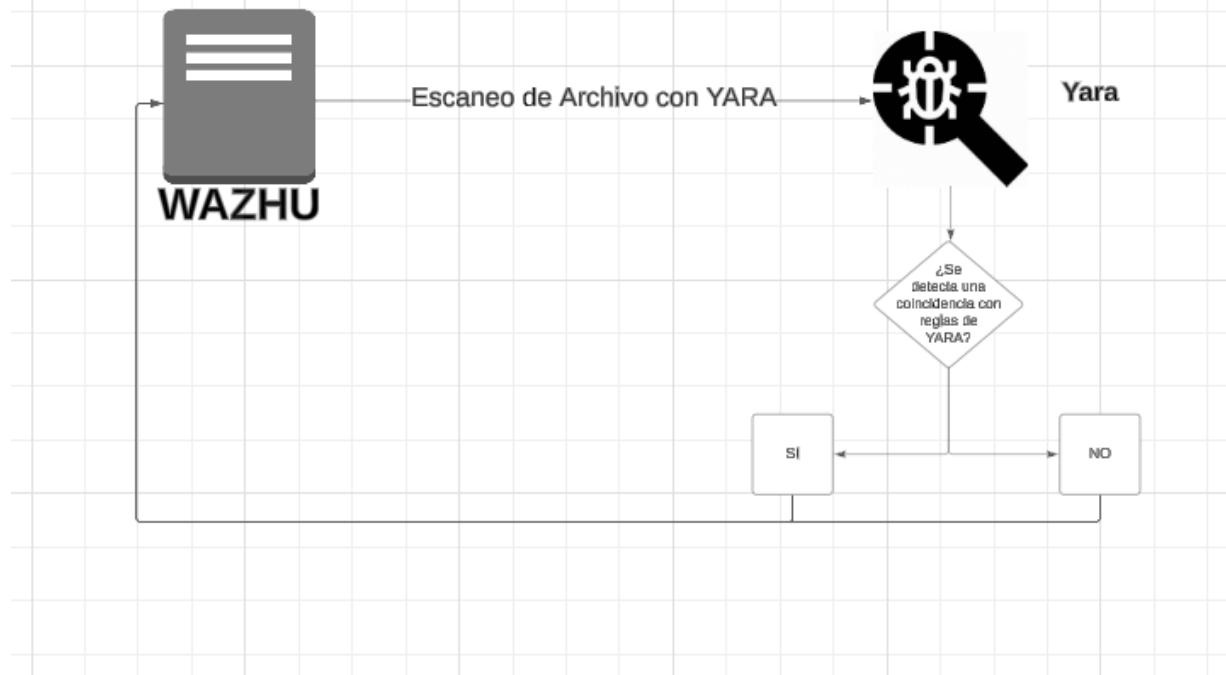
</syscheck>
```

Beneficio: Esto permite que Wazuh detecte archivos sospechosos y los marque según las reglas de Yara, reforzando la detección de malware.

```
script en Python o bash que ejecuta la
detección con YARA:
import yara
# Ruta del archivo y de las reglas de YARA
file_path = 'ruta/al/archivo_sospechoso'
rule_path = 'ruta/a/las/reglas.yara'

# Compilar y ejecutar reglas
rules = yara.compile(filepath=rule_path)
matches = rules.match(file_path)

if matches:
    print("Amenaza detectada:", matches)
    # Enviar resultado de vuelta a Wazuh o
    # tomar acción
else:
    print("No se detectó ninguna amenaza.")
```



Estos dos fragmentos de código que se mostraron tanto en la imagen como por texto, cumplen funciones relacionadas con la detección de amenazas, pero su enfoque y alcance son diferentes:

1. Configuración en Wazuh (ossec.conf)

```
# En /var/ossec/etc/ossec.conf

<syscheck>

    <directories check_all="yes">/etc,/var/www</directories>

    <yara_rules_path>/etc/yara_rules</yara_rules_path>

</syscheck>
```

Este código es una configuración para el archivo ossec.conf de Wazuh. Aquí, Wazuh utiliza la integración con YARA para escanear directorios específicos (/etc y /var/www) en busca de archivos sospechosos basados en reglas de YARA.

Propósito: Configura el monitoreo continuo de los directorios especificados. Cada archivo en estos directorios se escanea usando las reglas definidas en la ruta de yara_rules_path.

Automatización: Wazuh ejecutará el escaneo según las reglas de syscheck de manera automática en intervalos establecidos, generando alertas si detecta coincidencias con las reglas de YARA.

Contexto de Uso: Es parte de un sistema de monitoreo de seguridad (Wazuh) que mantiene un control constante y envía alertas en caso de amenazas.

2. Script en Python usando YARA directamente

```
import yara

# Ruta del archivo y de las reglas de YARA

file_path = 'ruta/al/archivo_sospechoso'

rule_path = 'ruta/a/las/reglas.yara'

# Compilar y ejecutar reglas

rules = yara.compile(filepath=rule_path)

matches = rules.match(file_path)

if matches:

    print("Amenaza detectada:", matches)
```

```
# Enviar resultado de vuelta a Wazuh o tomar acción
```

```
else:
```

```
    print("No se detectó ninguna amenaza.")
```

Este código es un script en Python que utiliza la biblioteca de YARA para escanear un archivo específico (`file_path`) en busca de coincidencias con las reglas definidas en `rule_path`.

Propósito: Ejecuta un escaneo manual y específico en un archivo concreto, utilizando YARA desde un script independiente.

Automatización y Flexibilidad: Es una ejecución manual o puede integrarse en un flujo de trabajo automatizado. Este script es flexible y permite adaptarse para escanear cualquier archivo, pero no tiene el monitoreo continuo de Wazuh.

Contexto de Uso: Se utiliza fuera del entorno de Wazuh o como una herramienta puntual para analizar archivos específicos, siendo útil para tareas de análisis forense o escaneos personalizados.

Integración de VirusTotal con Wazuh

Automatizar la verificación en VirusTotal:

1. Configura un script en Wazuh para enviar hashes de archivos sospechosos a la API de VirusTotal y verificar si están registrados como maliciosos.

Ejemplo de script en Python:

```
import requests

def check_virustotal(api_key, file_hash):

    url = f'https://www.virustotal.com/api/v3/files/{file_hash}'

    headers = {'x-apikey': api_key}

    response = requests.get(url, headers=headers)

    return response.json()

# Uso del script con el hash del archivo y la clave de API
```

Integración con Wazuh: Configura Wazuh para ejecutar este script cada vez que detecte un archivo sospechoso, generando una alerta adicional si VirusTotal confirma la amenaza.

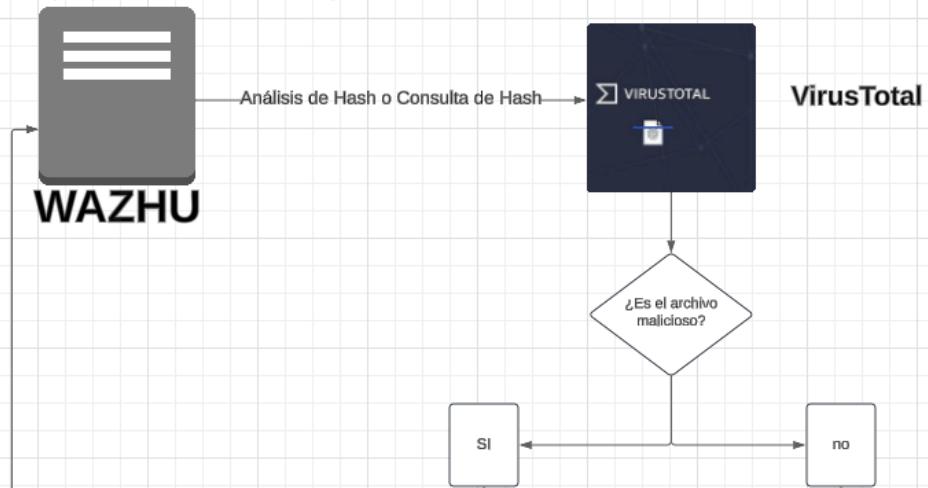
Beneficio: La integración permite una verificación más robusta, confirmando amenazas con información de múltiples motores antivirus.

```
script en Python o bash que ejecuta la consulta en VirusTotal:
import requests
API_KEY = 'YOUR_VIRUSTOTAL_API_KEY' file_hash
= 'HASH_DEL_ARCHIVO'

url = f"https://www.virustotal.com/api/v3/files/{file_hash}"
headers = {"x-apikey": API_KEY}

response = requests.get(url, headers=headers)

if response.status_code == 200:
    result = response.json()
    # Análisis de resultado y envío de vuelta a Wazuh o
    toma de acción
else:
    print("Error al consultar VirusTotal")
```



Los códigos anteriormente mostrados dan a entender que son diferentes, pero pueden cumplir con el mismo objetivo por lo cual se utiliza solo que pueden tener algunas diferencias. Por lo tanto, para aclarar esas diferencias se mostrará continuación la Definición de Función vs. Código Directo.

Función vs. Código Directo:

Código Directo: Es un bloque directo de código que ejecuta una consulta específica a la API de VirusTotal para un archivo en particular.

Función: Define check_virustotal, una función que recibe dos parámetros (api_key y file_hash). Esto permite reutilizar el código con diferentes claves y hashes, facilitando su integración en otros sistemas o scripts.

Uso de Variables:

Código Directo: Define API_KEY y file_hash como variables globales en el código. Estos valores están "fijos" en el script.

Función: Usa parámetros de entrada para la API y el hash del archivo, lo que hace que el script sea más flexible y adaptable a múltiples casos.



Manejo de Errores:

Código Directo: Incluye una verificación de estado (`response.status_code == 200`) para manejar errores en la respuesta. Si la solicitud falla, imprime un mensaje de error, ayudando a diagnosticar problemas.

Función: No maneja errores explícitamente; simplemente retorna el resultado en formato JSON. Esto podría ser mejorado añadiendo un manejo de errores similar al código directo.

Flexibilidad y Reutilización:

Código Directo: Es menos modular y está pensado para una consulta única. No es fácilmente reutilizable sin modificar las variables `API_KEY` y `file_hash`.

Función: Es independiente y puede llamarse en cualquier parte del código con diferentes argumentos, facilitando su integración en un programa más grande.

Combinación de los 2 códigos:

para tener una función reutilizable con manejo de errores se puede usar el siguiente código:

```
import requests

def check_virustotal(api_key, file_hash):

    url = f'https://www.virustotal.com/api/v3/files/{file_hash}'

    headers = {'x-apikey': api_key}

    response = requests.get(url, headers=headers)

    if response.status_code == 200:

        return response.json() # Devuelve el resultado en caso de éxito

    else:

        print("Error al consultar VirusTotal:", response.status_code)

        return None # Maneja el error devolviendo None o un mensaje
```

Correlación de Técnicas de Ataque: Wazuh y MITRE ATT&CK

MITRE ATT&CK es un marco que documenta técnicas y tácticas comunes de ataque, permitiendo mapear el comportamiento de los atacantes en fases específicas del ataque. Wazuh puede integrarse con MITRE ATT&CK para correlacionar eventos de seguridad con tácticas documentadas. Esto ayuda a identificar patrones avanzados de ataque, proporcionando una comprensión detallada de la actividad maliciosa y ayudando a anticipar los pasos del atacante.

Los analistas de seguridad pueden así tomar medidas preventivas, optimizando las estrategias de defensa.

Integración de MITRE ATT&CK con Wazuh

Mapeo de TTPs: Configura Wazuh para correlacionar eventos con tácticas, técnicas y procedimientos (TTPs) del marco MITRE ATT&CK.

Configuración de reglas en Wazuh: Crea reglas de correlación que etiqueten eventos según las técnicas de MITRE ATT&CK.

Ejemplo:

```
<rule id="100001" level="10">
    <decoded_as>json</decoded_as>
    <field name="event_id">100</field>
    <description>Possible brute force attempt</description>
    <mitre_technique>T1110</mitre_technique>
    <mitre_tactic>Credential Access</mitre_tactic>
</rule>
```

Beneficio: El mapeo a MITRE ATT&CK permite una mejor comprensión de los ataques y la anticipación de posibles movimientos del atacante.

Monitoreo de Red y Control de Accesos: Dispositivos MikroTik

Los dispositivos MikroTik, como routers y firewalls, son habituales en entornos PyME por su rendimiento y accesibilidad. Wazuh puede configurarse con decodificadores personalizados para monitorear estos dispositivos, registrando accesos y cambios de configuración en tiempo real. Al integrar los registros de MikroTik en Wazuh y Graylog, se facilita la detección de accesos no autorizados y se mejora el control de la infraestructura de red. Además, el monitoreo de estos dispositivos ayuda a cumplir con los requisitos de control de acceso y auditoría de varias normativas de seguridad.

Monitoreo de MikroTik con Wazuh y Graylog

Configuración en MikroTik: Configura el dispositivo para enviar logs al servidor de Wazuh/Graylog a través de Syslog.

Ejemplo de configuración en MikroTik:

En un dispositivo MikroTik, estos comandos se ejecutan en el terminal del router MikroTik o a través de la interfaz gráfica (Winbox) para configurar el envío de logs a un servidor remoto, como Wazuh.

Para ejecutarlo en MikroTik:

1. Abre la terminal de MikroTik o accede a la interfaz Winbox.
2. Introduce los comandos directamente en la terminal del router MikroTik para configurar la acción de log y especificar el envío de logs a la IP del servidor Wazuh en el puerto 514.

```
/system logging action add name="remote" target=remote remote=IP_WAZUH_SERVER remote-port=514
```

/system logging add topics=info action=remote

Integración en Wazuh y Graylog: Configura Wazuh para procesar estos logs y envíalos a Graylog para visualización.

Beneficio: La integración permite monitorear los accesos y cambios de configuración en MikroTik, mejorando el control sobre la infraestructura de red.

Importancia de la Correlación de Eventos en la Detección de Patrones Complejos

La correlación de eventos en Wazuh y su visualización en Graylog ofrecen una visión completa del entorno de seguridad, permitiendo detectar patrones de ataque avanzados que podrían pasar desapercibidos si los eventos se analizaran por separado. Este enfoque no solo aumenta la eficacia del sistema de seguridad, sino que también optimiza la eficiencia operativa al reducir el tiempo necesario para identificar y responder a amenazas, haciendo un uso más efectivo de los recursos en entornos de PyME con limitaciones de presupuesto.

Cumplimiento Normativo

La adopción de herramientas de seguridad de código abierto en un sistema de monitoreo continuo representa una ventaja significativa para las PyMEs, ayudándolas a cumplir con diversas normativas de seguridad en un contexto de recursos limitados. A continuación, se describe cómo estas herramientas contribuyen al cumplimiento de regulaciones clave y qué áreas requieren ajustes adicionales.

1. GDPR (Reglamento General de Protección de Datos)

Herramientas Principales: Wazuh y Graylog.

Contribución al Cumplimiento:

Wazuh facilita el cumplimiento de GDPR mediante el monitoreo continuo y la generación de alertas cuando ocurren accesos no autorizados a datos sensibles. Esto permite auditar quién accede a los datos personales y cuándo, proporcionando trazabilidad y transparencia en la gestión de datos.

Graylog centraliza los logs y permite realizar búsquedas en tiempo real, ayudando a identificar patrones de acceso a datos. Esto contribuye al cumplimiento de los principios de minimización y seguridad en el tratamiento de datos, como lo exige GDPR.

Apoyo Adicional Necesario:

Para un cumplimiento completo, se requiere implementar políticas de respuesta rápida y notificación de brechas de seguridad en un máximo de 72 horas. La integración de procedimientos claros para reportar brechas y evaluar su impacto en la privacidad de los datos sería beneficioso, así como implementar cifrado de datos para proteger la información personal.

2. PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago)

Herramientas Principales: Wazuh y Snort/Suricata.

Contribución al Cumplimiento:

Wazuh se utiliza para auditar el acceso a sistemas de pago, generar alertas en caso de intentos de acceso no autorizados y verificar la integridad de los archivos, cumpliendo así los requisitos de monitoreo y control de accesos establecidos en PCI DSS.

Snort/Suricata, como IDS/IPS, detecta intentos de ataques en la red, protegiendo los sistemas de pago contra amenazas como tráfico malicioso o ataques de fuerza bruta.

Apoyo Adicional Necesario: PCI DSS también exige el cifrado de datos sensibles y políticas de

retención de logs. Sería útil complementar estas herramientas con soluciones de cifrado para datos de tarjetas y definir políticas de retención y eliminación de registros antiguos para cumplir completamente con la normativa.

3. ISO 27001 (Sistema de Gestión de Seguridad de la Información)

Herramientas Principales: Wazuh y MITRE ATT&CK.

Contribución al Cumplimiento:

Wazuh permite gestionar incidentes y detectar vulnerabilidades, facilitando la generación de informes de auditoría que simplifican las revisiones periódicas exigidas por ISO 27001.

MITRE ATT&CK ayuda a identificar y clasificar tácticas y técnicas usadas en ataques cibernéticos, permitiendo que la organización adopte controles proactivos y desarrolle estrategias de mitigación específicas.

Apoyo Adicional Necesario: La norma ISO 27001 requiere una gestión continua del ciclo de vida de los riesgos y capacitaciones periódicas en ciberseguridad. Incluir entrenamientos regulares y evaluaciones anuales de riesgo sería fundamental para completar el cumplimiento.

4. CIS Controls (Controles de Seguridad del Centro para la Seguridad de Internet)

Herramientas Principales: Wazuh, Graylog y Snort/Suricata.

Contribución al Cumplimiento:

Wazuh y Graylog implementan controles como la protección contra malware, monitoreo de accesos y auditoría continua, manteniendo un registro detallado de accesos y actividad inusual en la red.

Snort/Suricata refuerza el control contra ataques a la red y permite configurar alertas personalizadas, cumpliendo con los controles específicos de protección de infraestructura.

Apoyo Adicional Necesario: Aunque estas herramientas cubren varios controles técnicos, los CIS Controls también enfatizan la necesidad de educar al personal en ciberseguridad. La implementación de programas de capacitación regulares y políticas de gestión de cambios mejorarían la eficacia del sistema en su conjunto.

5. NIST (Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología)

Herramientas Principales: Wazuh, Snort y Yara.

Contribución al Cumplimiento:

Wazuh y Snort permiten la identificación y respuesta a incidentes en tiempo real, cubriendo los requisitos de NIST relacionados con la protección de activos y la gestión de incidentes.

Yara ayuda a detectar patrones de malware, contribuyendo al cumplimiento de requisitos de protección y mitigación de amenazas.

Apoyo Adicional Necesario: NIST también sugiere implementar procesos avanzados de recuperación y planes de continuidad de negocio. La inclusión de políticas de recuperación de desastres y automatización en respaldo y restauración de datos mejoraría el cumplimiento.

6. Ley Argentina 25.326 de Protección de Datos Personales

Herramientas Principales: Wazuh, Graylog y MikroTik.

Contribución al Cumplimiento:

Wazuh y Graylog ayudan a cumplir con los requisitos de auditoría y trazabilidad de esta ley,

registrando quién accede a los datos sensibles y facilitando revisiones en caso de accesos indebidos.

MikroTik ofrece control de accesos en la red, permitiendo que solo usuarios autorizados tengan acceso a información sensible.

Apoyo Adicional Necesario: Esta ley exige no solo controles técnicos, sino también políticas organizacionales para la protección de datos. La designación de un responsable de protección de datos y el establecimiento de políticas de gestión de datos personales completarían el cumplimiento normativo.

Matriz de Cumplimiento Normativo

Normativa	Wazuh	Graylog	Snort/Suricata	Yara	VirusTotal	MITRE ATT&CK	MikroTik
GDPR	✓	✓	✓		✓		
PCI DSS	✓	✓	✓	✓	✓		✓
ISO 27001	✓	✓				✓	
CIS Controls	✓	✓	✓	✓			✓
NIST	✓	✓	✓				
Ley 25.326 de Protección de Datos (Argentina)	✓	✓	✓	✓			✓

3. Ejemplo Hipotético de Respuesta a un Ataque de Fuerza Bruta

Objetivo: Ilustrar cómo una PyME podría responder a un ataque de fuerza bruta utilizando herramientas de seguridad open-source, gestionando un flujo de alertas desde Snort hasta VirusTotal y apoyándose en el marco MITRE ATT&CK para coordinar una respuesta adecuada.

Escenario del Ataque

Imaginemos que un atacante está intentando acceder a un servidor de autenticación de la PyME mediante un ataque de fuerza bruta, probando repetidamente combinaciones de usuario y contraseña en un intento por obtener acceso no autorizado.

Flujo de Alertas y Respuesta

1. **Detección Inicial con Snort:** Snort, configurado para monitorear el tráfico de red en tiempo real, detecta una cantidad anormal de intentos de acceso fallidos hacia el servidor. Este comportamiento se clasifica como un posible ataque de fuerza bruta, generando una alerta que incluye detalles clave, como la dirección IP del atacante y el puerto de destino.
3. **Validación en VirusTotal:** La dirección IP identificada por Snort se envía a VirusTotal, que permite verificar si esa IP está asociada con actividades maliciosas conocidas. Esta validación ayuda a confirmar si la actividad es malintencionada o si puede tener otra explicación, lo que permite priorizar una respuesta adecuada.
4. **Análisis y Mapeo con MITRE ATT&CK:** Utilizando el marco MITRE ATT&CK, se mapea el ataque dentro de la categoría de “Acceso inicial” y se identifica la técnica de fuerza bruta. Este análisis permite entender mejor el contexto del ataque y ayuda a identificar patrones o tácticas que el atacante podría estar usando, lo que permite anticipar posibles movimientos.
5. **Respuesta y Medidas de Mitigación:** Con la información recopilada, se decide bloquear la IP del atacante en el firewall y activar monitoreo adicional sobre intentos de acceso al servidor. También se ajustan las políticas de seguridad para endurecer los controles de acceso y se configuran alertas adicionales que ayuden a identificar intentos similares en el futuro.
6. **Documentación y Mejora Continua:** Se registra todo el flujo del incidente, incluyendo la alerta de Snort, los datos obtenidos de VirusTotal y el mapeo de MITRE ATT&CK, en un informe interno. Esta documentación permite evaluar la efectividad de la respuesta, mejorar la política de seguridad y sirve como referencia para situaciones similares en el futuro.

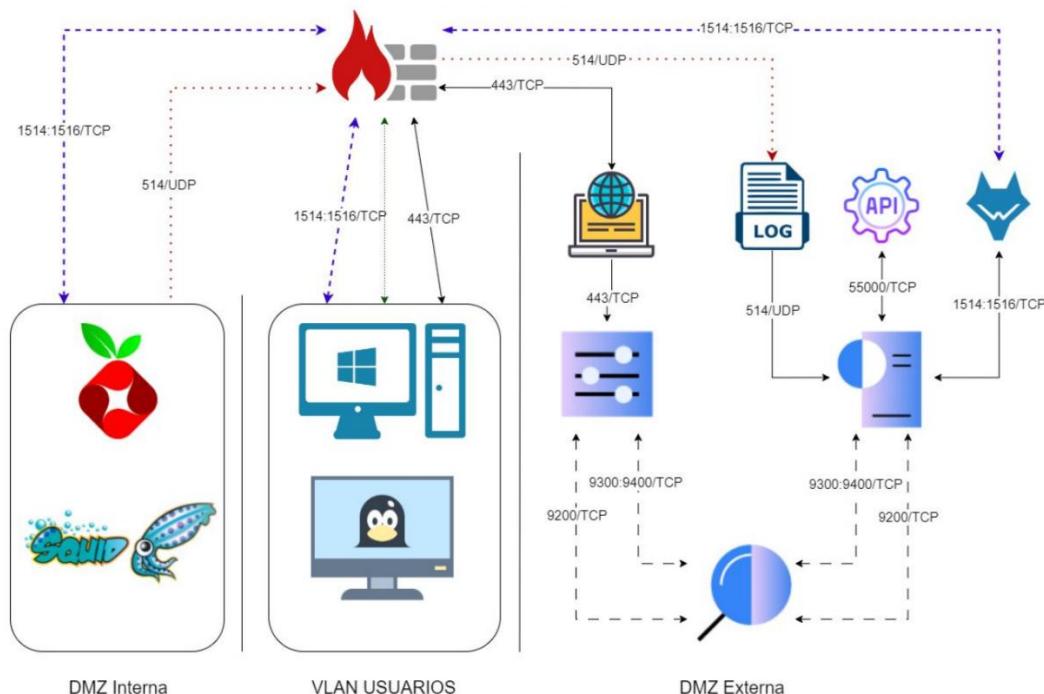


Diagrama de red para la detección y respuesta ante un ataque de fuerza bruta. Fuente: Profesor Lic. Juan Pablo Villalba, UGR Universidad del Gran Rosario,
https://virtual.ugr.edu.ar/pluginfile.php/496853/mod_resource/content/2/red%20wazuh.jpeg.

4. Propuestas de Mejora para la Integración de Seguridad

Para fortalecer la respuesta ante incidentes y optimizar la eficacia de las herramientas de seguridad open-source en el contexto de una PyME, se proponen las siguientes mejoras en sincronización de alertas, actualización de reglas de detección y automatización de bloqueos de IPs sospechosas.

1. Sincronización de Alertas

Una sincronización rápida entre herramientas permite responder a amenazas con mayor agilidad. Algunas recomendaciones para mejorar la velocidad de transmisión de alertas entre Snort, Graylog y otros sistemas son:

- **Protocolos de Baja Latencia:** Utilizar protocolos de baja latencia como UDP para el envío de alertas urgentes, lo que puede reducir el tiempo de transmisión en comparación con TCP.
- **Ajuste de la Configuración de Logs:** Simplificar las alertas para que incluyan solo la información más relevante, lo cual reduce el tamaño de los datos y optimiza el flujo de transmisión.
- **Orquestación de Eventos:** Implementar un orquestador de eventos, como Elastic Stack, que permita centralizar y coordinar las alertas de múltiples herramientas, mejorando la velocidad de respuesta y la visibilidad de eventos críticos.

2. Actualización de Reglas de Detección

Para mantener al sistema actualizado frente a nuevas amenazas, es clave revisar y ajustar las reglas en Snort y Yara. Algunas acciones recomendadas son:

- **Reglas Personalizadas Adaptadas al Entorno:** Crear reglas específicas en Snort y Yara basadas en el comportamiento y las necesidades de la PyME, lo cual mejora la precisión de la detección en función del contexto particular.
- **Fuentes Externas de Inteligencia de Amenazas:** Conectar Snort y Yara a fuentes de inteligencia que provean reglas actualizadas para amenazas emergentes, de manera que el sistema esté preparado para identificar patrones nuevos de actividad maliciosa.
- **Revisión y Optimización Periódica de Reglas:** Establecer un calendario de revisión de reglas que permita desactivar aquellas que ya no son relevantes y ajustar otras según los cambios en el entorno, mejorando así el rendimiento general del sistema.

3. Automatización de Bloqueos de IPs

Para agilizar la respuesta a accesos no autorizados, se sugiere implementar mecanismos de bloqueo automático de IPs sospechosas. Las siguientes medidas pueden ser efectivas:

- **Bloqueo Automático en Snort:** Configurar Snort para que aplique bloqueos automáticos a IPs que generen múltiples alertas en un corto periodo de tiempo, lo que puede indicar intentos de acceso no autorizados o ataques de fuerza bruta.
- **Scripts para Bloqueos en Firewall:** Desarrollar un script que, ante la activación de una alerta crítica, añada automáticamente la IP sospechosa a la lista de bloqueos del firewall, permitiendo una respuesta inmediata.
- **Uso de SIEM para la Gestión de Bloqueos:** Integrar un SIEM que centralice el manejo de alertas y permita ejecutar bloqueos automáticos en tiempo real, lo cual optimiza la gestión de incidentes y permite realizar un seguimiento detallado de las amenazas.

3. Conclusiones

Destaco la posibilidad de descubrir y utilizar una combinación valiosa de herramientas open-source para el cumplimiento normativo y, en consecuencia, la seguridad de una organización (PyMEs). A pesar de mi limitada experiencia práctica en la implementación técnica de estas herramientas, he podido incorporar su uso mediante un proceso de prueba y error, alcanzando el objetivo de mejorar varios aspectos de seguridad sin incurrir en costos de software, y con la opción de obtener soporte pago si así se requiere.

Aunque estas herramientas no son 100% efectivas, en un contexto donde la PyME no contaba con ninguna medida de seguridad, su implementación agrega un valor significativo a la empresa y, a su vez, reduce su nivel de riesgo. Familiarizarse con estas herramientas brinda una base importante para personas con poca experiencia en el área de ciberseguridad.

Durante la investigación, algunos puntos que pude descubrir incluyen que la integración de estas herramientas puede ser compleja y consumir tiempo. Además, las interfaces de usuario no son siempre intuitivas, lo cual puede representar un desafío para quienes no tienen experiencia. Asimismo, las actualizaciones periódicas son menos frecuentes en comparación con las herramientas comerciales, lo que limita la capacidad para corregir vulnerabilidades y aumenta el riesgo. Sin embargo, como mencioné anteriormente, pasar de no contar con ninguna medida de seguridad a implementar un conjunto de soluciones open-source es un gran avance para la protección de los datos de la empresa y, por ende, para su reputación y estabilidad económica.

Con el tiempo, el uso de herramientas open-source en seguridad sigue evolucionando, y se está

convirtiendo en una opción sólida para que las PyMEs protejan sus sistemas sin incurrir en altos costos. Gracias a las constantes mejoras y al respaldo de la comunidad de desarrolladores, estas herramientas son cada vez más efectivas para enfrentar nuevas amenazas. Al mismo tiempo, las normativas de ciberseguridad, como el GDPR y PCI DSS, también están cambiando continuamente, exigiendo que las organizaciones cumplan con estándares más estrictos. Esto plantea nuevos desafíos y exige que las herramientas open-source también se desarrollen para ayudar a las PyMEs a cumplir con estas normativas de manera eficiente.

Finalmente, considero necesario expresar mi agradecimiento por el enfoque práctico que se utilizó durante todo el curso, ya que facilitó el aprendizaje y la aplicación de los conocimientos. Esto merece ser mencionado nuevamente, especialmente al tratarse del último trabajo de la materia. En conclusión, las herramientas de código abierto ofrecen un futuro prometedor para la seguridad en las PyMEs, aunque será fundamental que estas empresas mantengan una actitud proactiva y se adapten tanto a las innovaciones tecnológicas como a los requisitos regulatorios para asegurar su protección en el tiempo.

4. Referencias:

Banco Central de la República Argentina. (s.f.). *Ciberseguridad*. Recuperado de <https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Ciberseguridad.asp>

- CIS. (2022). *CIS Controls v8* [Versión en español]. Recuperado de https://virtual.ugr.edu.ar/pluginfile.php/324015/mod_resource/content/1/CIS_Controls_v8_Spanish_ESP_ONLINE_2022_0411.pdf
- European Union. (s.f.). *UE GDPR Texto Original*. Recuperado de https://virtual.ugr.edu.ar/pluginfile.php/333372/mod_resource/content/1/UE%20GDPR%20Texto%20Original.pdf
- Lucidchart. (2024). *Diagrama de Integración de Herramientas*. Recuperado de https://lucid.app/lucidchart/7f07d4d8-feaa-4f6a-8d8b-529676733d14/edit?beaconFlowId=2C32DE9E780496F0&invitationId=inv_3b918e76-e3e4-4c8a-9eca-67f2ae50c1db&page=0_0#
- National Institute of Standards and Technology. (s.f.). *NIST vs. ISO 27001: Marcos de Ciberseguridad*. Recuperado de https://virtual.ugr.edu.ar/pluginfile.php/495705/mod_resource/content/4/NIST-vs-ISO-27001-Marcos-de-Ciberseguridad.pdf
- National Institute of Standards and Technology. (s.f.). *NIST Cybersecurity Framework*. Recuperado de <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf>
- PCI Security Standards Council. (2018). *PCI DSS v3.2.1*. Recuperado de https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI_DSS_v3-2-1-ES-LA.pdf
- BleepingComputer. (n.d.). *VirusTotal cheat sheet makes it easy to search for specific results*. Recuperado de <https://www.bleepingcomputer.com/news/security/virustotal-cheat-sheet-makes-it-easy-to-search-for-specific-results/>
- Vecteezy. (n.d.). *Logs icon style*. Recuperado de <https://www.vecteezy.com/vector-art/21799200-logs-icon-style>
- Freepik. (n.d.). *Icono de escudo rojo: Ilustración vectorial*. Recuperado de https://www.freepik.es/vector-premium/icono-escudo-rojo-ilustracion-vectorial_33059949.htm
- eCrimeLabs. (2020, abril 5). *MITRE ATT&CK for improved metrics and KPI on detection capabilities*. Recuperado de <https://www.ecrimelabs.com/blog/2020/4/5/mitre-attampck-for-improved-metrics-and-kpi-on-detection-capabilities>
- Wazuh, Inc. (2024). *Installation guide*. Recuperado el 14 de noviembre de 2024, de <https://documentation.wazuh.com/current/installation-guide/index.html>
- Este documento sigue las normas de citación y referencias de la *Publication Manual of the American Psychological Association* (7^a ed.).