COLEGIO DE CIENCIAS E INGENIERÍAS

INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

Entregable III del Proyecto Integrador

Tutor: Roberto Andrade

Autor: José Contreras

Quito – Ecuador

2025

1. Título del Proyecto:

   Orquestador de Agentes de IA para gestión de incidentes de ciberseguridad

2. Resumen de actividades realizadas:

   1. Afinación agente de monitoreo y automatización de alertas con Wazuh: En el agente de monitoreo se realizó una revisión nodo por nodo con el fin de robustecer el funcionamiento, estandarizar los mensajes de notificación e implementar el paradigma de MITTRE&Attack. En términos del funcionamiento se intervino especialmente al de investigación & resumen. El script en principio mantiene 2 prompts. El primero que ejecuta el MapReduce y el segundo que implementa un Summarization. Para el MapReduce se modificó el prompt con el fin de que tome en espcial consideración las siguientes variables:

Variable	Descripción
timestamp	Fecha y hora exacta en la que Wazuh registró el evento/alerta (normalmente en UTC).
rule.id	Identificador numérico único de la regla de Wazuh que se disparó.
rule.level	Nivel de severidad de la alerta (normalmente 0–15 en Wazuh).
rule.description	Texto descriptivo de la regla que resume qué se ha detectado (p. ej. “Multiple failed login attempts”).
rule.groups[]	Lista de “grupos” o categorías a las que pertenece la regla (auth, ssh, malware, windows, etc.).
rule.mitre.tactic[]	Tácticas MITRE ATT&CK asociadas a la regla (p. ej. Credential Access, Discovery).
rule.mitre.technique[]	Técnicas MITRE ATT&CK asociadas (p. ej. T1110 Brute Force, T1046 Network Service Discovery).
agent.name	Nombre del agente Wazuh que generó el evento (normalmente el hostname del endpoint).

Tabla 1. Variables de interés incluidas en flujo

El flujo toma en consideración rule.mitre.tactic[] y rule.mitre.technique[], valores entregados por el siem Wazuh para utilizarlos de enriquecimiento contextual. Sin embargo, el flujo implementa de forma independiente MITTRE, también genera valores de riesgo y los compara para presentar el mensaje de notificación en telegram. Por otra parte también se modifica ..

Dentro del prompt de summarization se consideró la estandarization de los mensajes para evitar la variablidad de contexto entregado por la IA para diferentes alertas. A continuación se muestran los prompts:

Finalmente se realizaron las configuraciones necesarias para: habilitar un url de producción en n8n con el fin de que el flujo se integre con el Siem Wazuh de tal forma que sea capaz de escuchar permanentemente por el puerto 5678, acoplar la escala de riesgo como Wazuh de 1-15 y procesar sus alertas acorde. También se incorporaron nuevos endpoints que ahora se reflejan en el dashboard, entre ellos se encuentra el ids-suricata, ideapad 110s bajo nombre DESKTOP-1NRCFTA y Acer win11. A continuación, se presenta una imagen con el estado actual del dashboard Wazuh.

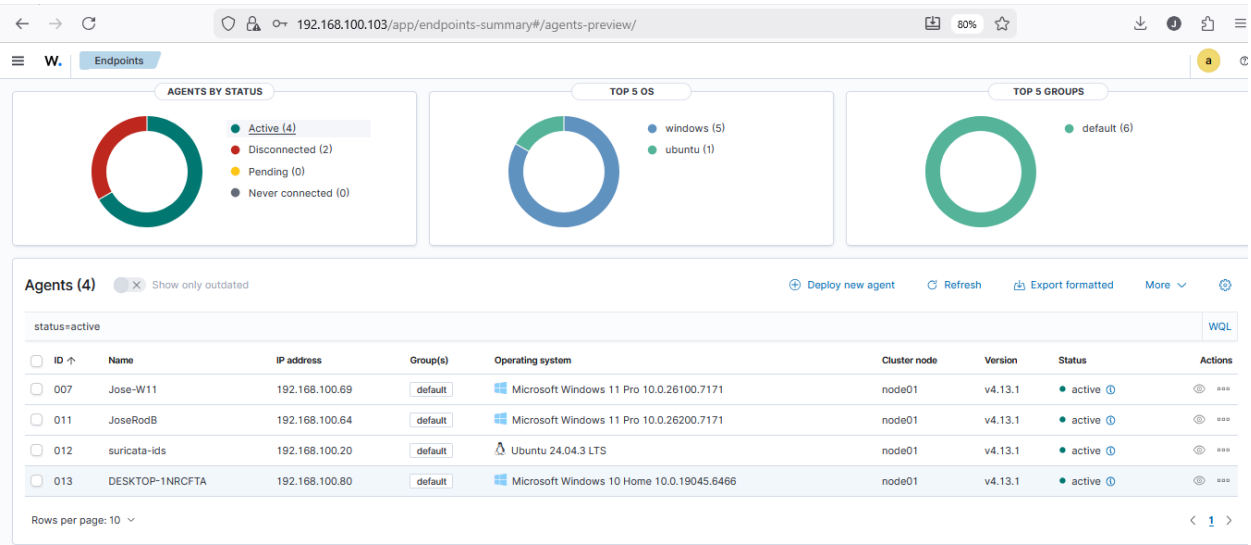


Figura 1. Estado actual del Dashboard

A continuación, se presenta un resumen de ejecuciones en N8N y 1 mensajes de alerta con formato estándarizado:

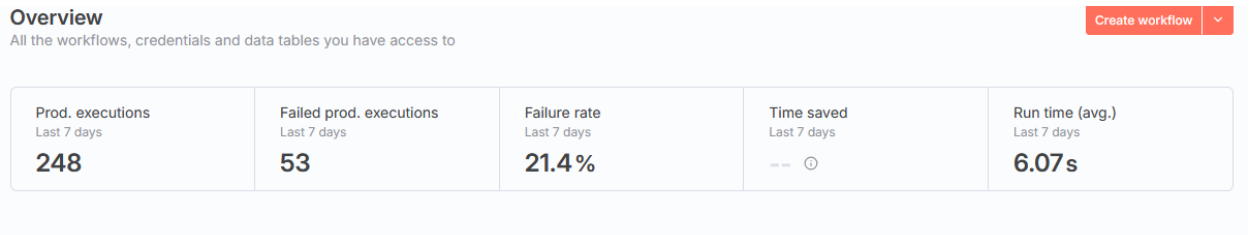


Figura 2. Resumen de Ejecuciones

Se han realizado 248 ejecuciones, de las cuáles en el chat de mensajería de telegram llamado Namebot se encuentran alrededor de 200 alertas analizadas por el agente.

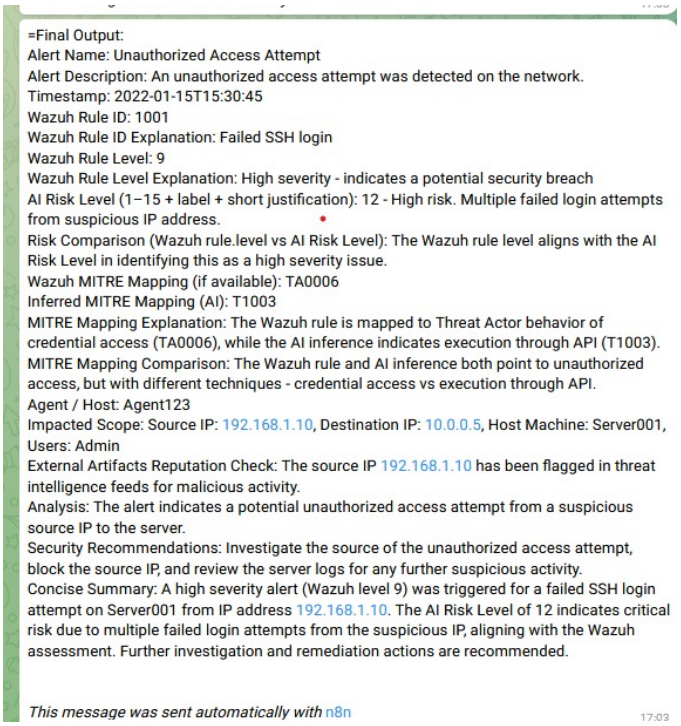


Figura 3. Mensaje de alerta con formato estándarizado

Como se observa en la imagen se ha complementado el formato inicial con algunos cambios como comparaciones en el nivel de riesgo entre el flujo y Wazuh como también en Mapeo MITTRE. También se busca con la configuración del prompt proveer una mayor explicación sobre las características del ataque y el detalle de las sugerencias que el sistema realiza para mitigar el riesgo. En este ejemplo, se trata de una alerta generada luego de múltiples intentos de loggeo mediante ssh hacia el usuario administrador del manager Wazuh. La explicación provista por el nodo detalla sobre múltiples intentos de loggeo desde una ip desconocida, en este caso 192.168.1.10 siendo externa a su red. El nivel de riesgo se clasifica como considerable alto, designándolo con 12 dentro de la escala de 1-15. En cuánto a las sugerencias el sistema sugiere mayor investigación acerca de la ip de origen realizando una revisión el los log del servidor.

2. Implementación de Laboratorio SOC: Dentro del SOC se realizaron una variedad de configuraciones entre ellas de AD/Windows Server 2025 e IDS/Suricata. A continuación, se presenta una tabla de direcciones ip de la topología de laboratorio SOC finalizada:

Nodo	Ip
Subred	192.168.100.0/24
Gateway Router Wifi	192.168.100.1
SG300 Gestión	192.168.100.2
AD-SOCLAB	192.168.100.10
Suricata	192.168.100.20
Wazuh-Manager	192.168.100.103
n8n-endpoint	192.168.100.64

Kali	192.168.100.200
Endpoint Lenovo	192.168.100.69
Enpoint Acer	192.168.100.64
Endpoint Ideapad	192.168.100.80

Tabla 2. Direcciones Ip Laboratorio SOC

Con esta designación de ips se procedió a implementar las repestivas configuraciones con el fin de implementar la siguiente topología:

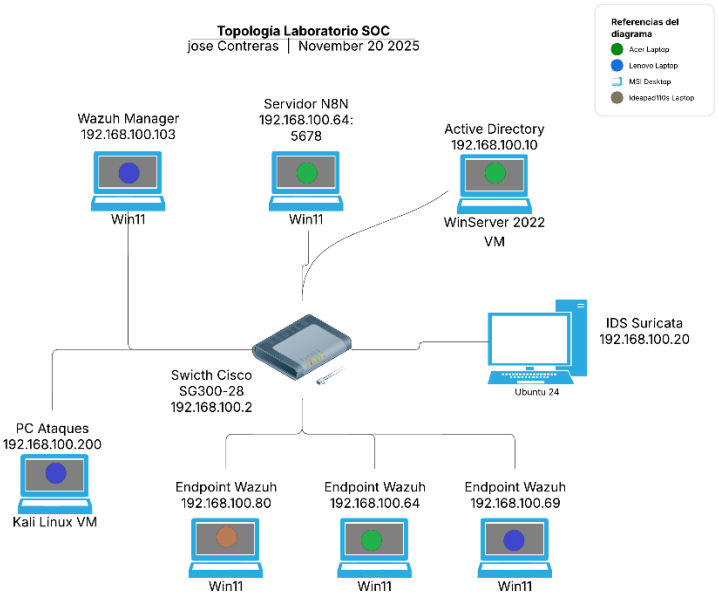


Figura 4. Topología final de Laboratorio SOC

Descripción de la topología y de los ataques que nos permite hacer con la integración que tenemos:

La topología del laboratorio SOC está organizada en torno a un switch Cisco SG300-28 que actúa como núcleo de la red cableada, al que se conectan todos los nodos críticos: el servidor Wazuh Manager en Windows 11, que centraliza los logs y las alertas; el servidor N8N en otro Windows 11, que orquesta las automatizaciones y notificaciones; el controlador de dominio y servidor DNS Active Directory sobre Windows Server 2022; y el sensor IDS Suricata desplegado en Ubuntu 24, encargado de inspeccionar el tráfico en modo espejo desde el switch. Desde este núcleo, se ramifican tres endpoints Windows 11 con el agente de Wazuh instalado (Acer, Lenovo y el Ideapad), que representan estaciones de trabajo de usuario final y sirven como blanco de pruebas de seguridad, mientras que una máquina Kali Linux funciona como PC de ataques para generar escaneos, intentos de intrusión y malware de prueba. Toda la infraestructura comparte el mismo segmento de red 192.168.100.0/24 con direcciones IP fijas para los servicios principales, lo que facilita la correlación de eventos y la medición de métricas de ataque y respuesta dentro del entorno controlado de laboratorio.

A continuación, se presenta la topología en hardware:

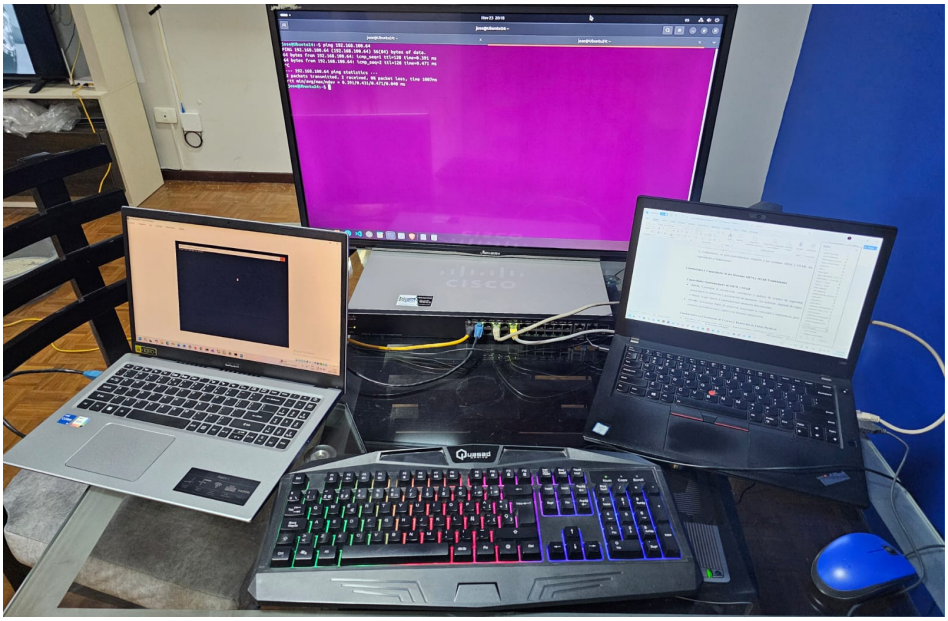
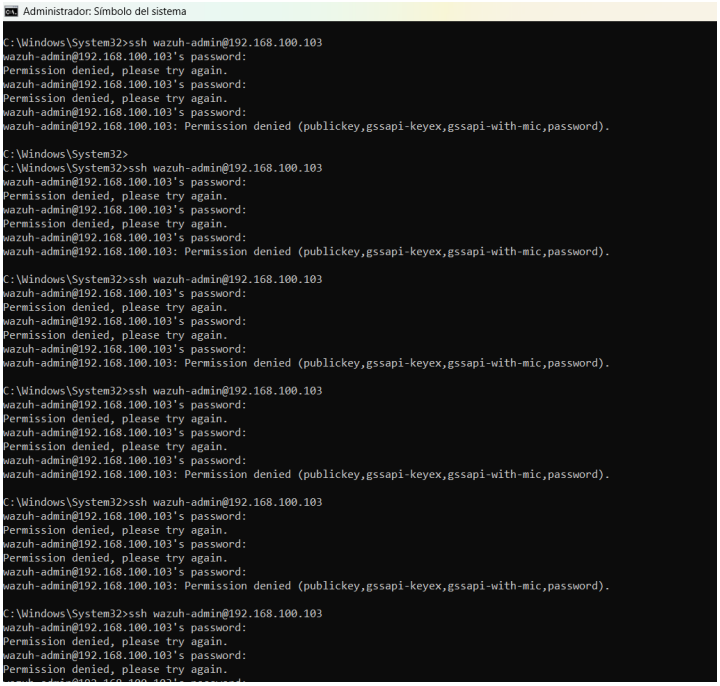


Figura 5. Topología de Laboratorio SOC

3. Elaboración de Ataques y campaña de pruebas:

   Ataque de prueba 1: Intento de autenticación fallido – Wazuh Manager

   En este caso se utilizará la línea de comandos y el protocolo ssh para realizar un intento de ingreso bajo fuerza bruta con claves incorrectas. Desde la terminal con ip: 192.168.100.64 se corren llamadas ssh hacia el Manager Wazuh con ip 192.168.100.103. A continuación, se presenta una imagen con algunos de los intentos:



```
C:\Windows\System32>ssh wazuh-admin@192.168.100.103
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
wazuh-admin@192.168.100.103: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Windows\System32>
C:\Windows\System32>ssh wazuh-admin@192.168.100.103
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
wazuh-admin@192.168.100.103: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Windows\System32>ssh wazuh-admin@192.168.100.103
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
wazuh-admin@192.168.100.103: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Windows\System32>ssh wazuh-admin@192.168.100.103
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
wazuh-admin@192.168.100.103: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Windows\System32>ssh wazuh-admin@192.168.100.103
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
wazuh-admin@192.168.100.103: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Windows\System32>ssh wazuh-admin@192.168.100.103
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
wazuh-admin@192.168.100.103's password:
Permission denied, please try again.
```

Figura 5: Intentos de loggeo SSH a Wazuh Manager

En la figura se observa las llamadas ssh que se realizan

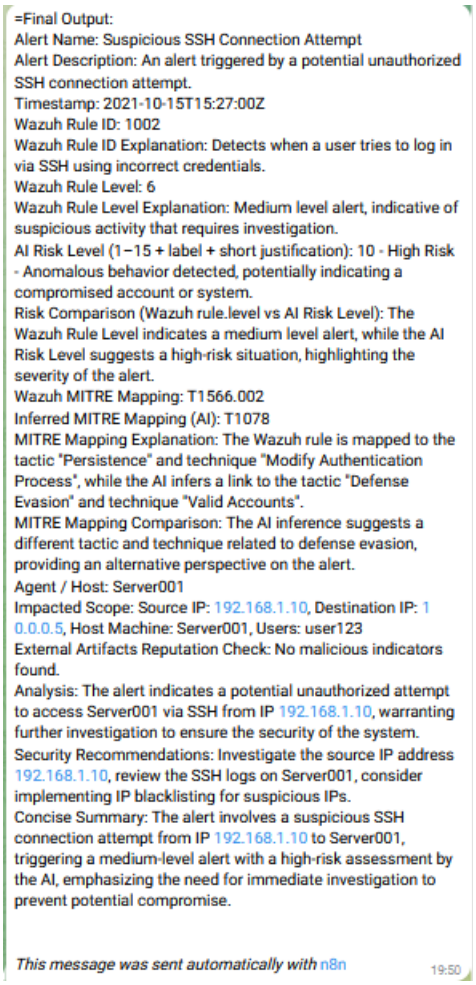


Figura 6: Mensaje alerta SOC telegram

Descripción en detalle del mensaje en narrativa continua

Ataque 2: Descarga y locación de archivo dañino EICAR

Luego de descargar, desde la url: https://www.eicar.org/download-anti-malware-testfile/ el programa EICAR para Windows 11. Al descomprimirlo y guardar estos cambios en el sistema operativo se generó una alerta de un troyano de red detectado además de la alerta de Windows defender. A continuación se muestra el mensaje:

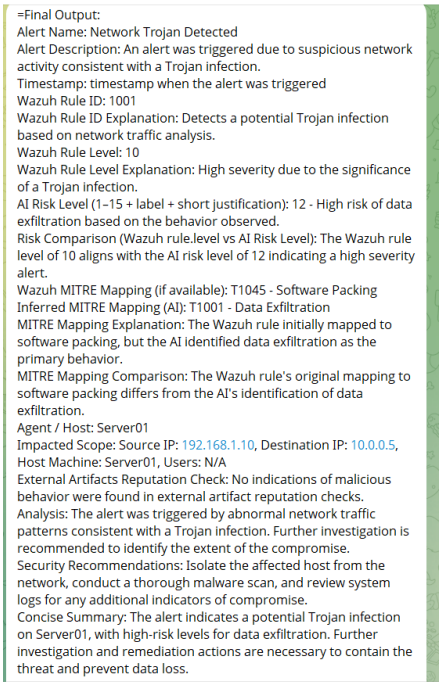


Figura 7: Mensaje de alerta EICAR al SOC.

3. Secciones o capítulos del documento final desarrollados

    1. Desarrollo del prototipo
    2. Ataques y pruebas de campaña

4. Revisión y firma del tutor del proyecto

    Yo, Roberto Andrade, profesor de la carrera de Ingeniería en Ciencias de la Computación, hago constar que he revisado y, por lo tanto, apruebo las actividades realizadas durante este período de trabajo. Por otra parte, considero que el avance del proyecto integrador es adecuado y se corresponde con el cronograma definido en el documento de planificación.

Roberto Omar Andrade Paredes
Time Stamping Security Data

Fdo: Roberto Andrade

Quito, 23 Noviembre de 2025