📘 PROJECT REPORT

Enterprise EDR & Threat Hunting Grid

Product Name: Sentient Shield

Organization: Infotact Solutions – Cyber Defense Operations Center (CDOC)

1️⃣ Project Overview

🎯 Use Case (Production Scenario)

Infotact's servers are under:

- Continuous brute-force attacks
- Privilege abuse
- Malware & ransomware attempts

To defend this, we deploy a centralized SOC EDR grid capable of:

- Real-time File Integrity Monitoring (FIM)
- Windows Sysmon telemetry
- Custom log detection
- Vulnerability detection (CVE mapping)
- MITRE ATT&CK correlation

2️⃣ Architecture Overview

Components Used

Component	OS	Role
Wazuh Manager	Ubuntu 22.04	Central SOC Manager
Linux Agent	Ubuntu	Web / App server
Windows Agent	Windows Server 2022	Domain / Target host
Sysmon	Windows	Deep telemetry

Communication Ports

- 1514/TCP – Agent → Manager
- 55000/TCP – Agent registration
- 443/TCP – Dashboard access

🔹 WEEK 1 – Infrastructure & Agent Deployment

3️⃣ Install Wazuh Manager (Ubuntu 20.04)

🟢 Step 1: Update system

sudo apt update && sudo apt upgrade -y

🟢 Step 2: Install required tools

sudo apt install curl apt-transport-https lsb-release gnupg -y

---

🟢 Step 3: Download Wazuh installer

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh

Verify:

ls wazuh-install.sh

🟢 Step 4: Install ALL components (Manager + Indexer + Dashboard)

bash

Copy code

sudo bash wazuh-install.sh -a

⏳ This takes 5–10 minutes

⚠️ Don't interrupt it ✔ Installs:

- Wazuh Manager
- OpenSearch
- Wazuh Dashboard

🟢 Step 5: Check services

After install finishes:

sudo systemctl status wazuh-manager

sudo systemctl status wazuh-indexer

sudo systemctl status wazuh-dashboard

All must show:

Active: active (running)

🟢 Step 6: Open Dashboard (IMPORTANT)

From host browser:

https://<UBUNTU_20.04_IP>

Example:

https://192.168.72.141

- Click Advanced
- Accept Risk
- Login:

username: admin

Password: Auto-generated

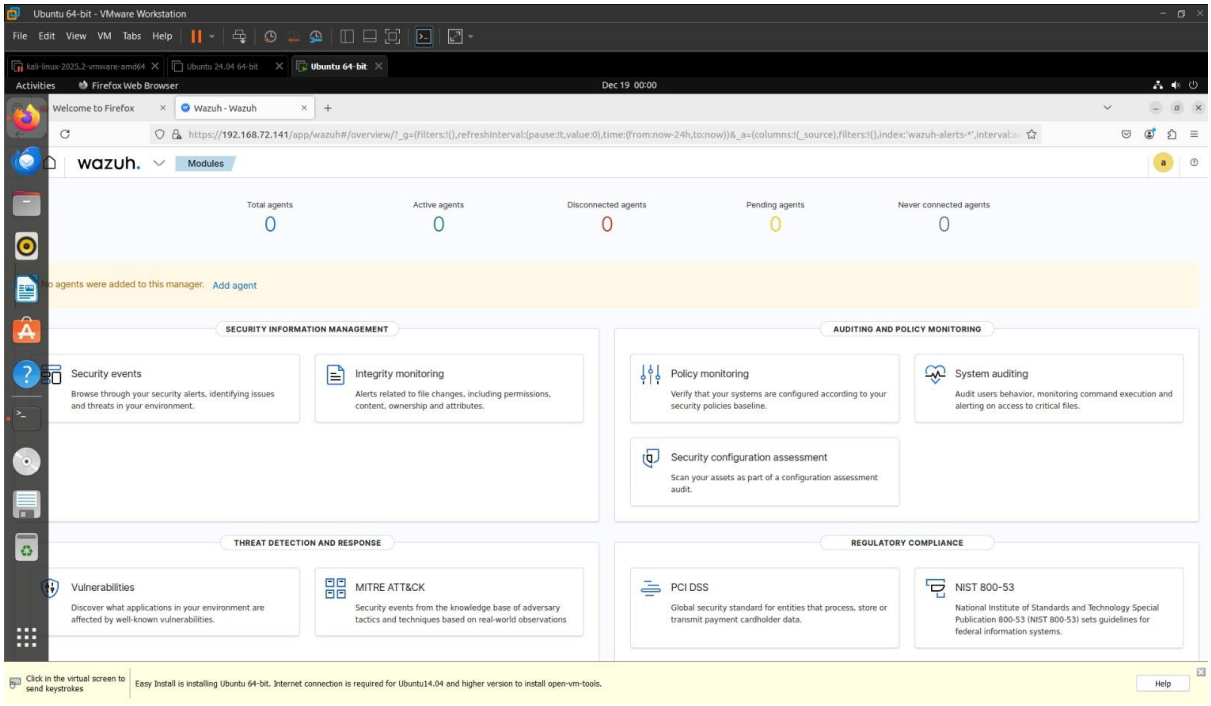
(password shown at install end)

if unable to see password then use it-

*Retrieve Admin Password (CRITICAL STEP):

sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt

📌 Save password securely (report appendix)



🧠 SOC Engineer Note (Important)

You are running:

- Manager: 4.7.5
- Agent: 4.14.1

This works, but:

- Agent configs must be minimal
- Advanced modules must be manager-side

👉 Later upgrade manager → 4.14.x for full feature parity.

We'll now add agents and generate real security alerts.

5️⃣ Install Linux Wazuh Agent

5.1 Add Repository & Install Agent

sudo apt install curl -y

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -

```
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list

sudo apt update

sudo apt install wazuh-agent -y
```

6️⃣ Configure Linux Agent

Edit Config File

```
sudo nano /var/ossec/etc/ossec.conf
```

✅ CORRECT & SAFE CONFIG

```
<ossec_config>
  <client>
    <server>
      <address>192.168.72.143</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <notify_time>10</notify_time>
    <auto_restart>yes</auto_restart>
  </client>
</ossec_config>
```

Validate & Start

```
sudo /var/ossec/bin/wazuh-agentd -t

sudo systemctl restart wazuh-agent
```

✔️ Status:

```
INFO: Connected to server
```

7️⃣ Agent Authentication (MOST IMPORTANT STEP)

7.1 Generate Agent Key (Manager)

sudo /var/ossec/bin/manage_agents

A → Add agent

E → Extract key

7.2 Import Key on Linux Agent

sudo /var/ossec/bin/manage_agents

I → Paste key

Q

Restart:

sudo systemctl restart wazuh-agent

🟢 Dashboard Check

Wazuh UI → Agents

- Status: Active
- No version error

8️⃣ Install Wazuh Agent on Windows Server 2022

8.1 Install Agent

- Download Wazuh Agent MSI
  Go to:
  👉 https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi
  (Use 4.7.5 to match your manager)
- During install:
  - Enter Manager IP
  - Complete setup

8.2 Import Authentication Key (GUI)

- On your Wazuh Manager VM (192.168.72.143):

sudo /var/ossec/bin/manage_agents

You'll see a menu.

Choose:

A → Add agent

Enter:

- Agent name: windows-server-2022
- IP address: any (IMPORTANT)
- ID: press Enter

Confirm with y

🔑 Export the key

After adding:

E → Extract key

Select the agent number (e.g., 002)

📌 You'll get something like:

MTAxIHdpbmRvd3Mtc2VydmVyLTIwMjIgYW55IDxxxxxxxxxxxxxxxxxxxx

👉 COPY THIS ENTIRE KEY (single line)

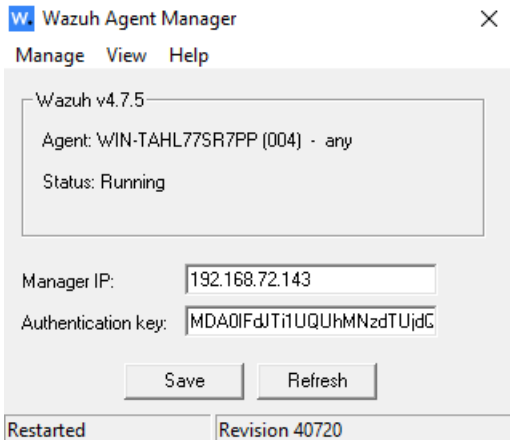
Import Auth Key on Windows Server 2022

Go back to Windows Server 2022.

In Wazuh Agent Manager window:

1. Manager IP:
2. 192.168.72.143
3. Authentication key:
    - Paste the key you copied
4. Click Save

5. Click Refresh



✅ Status should change to:

Running

Restart:

Restart-Service wazuh

Verify:

Get-Service wazuh

✔ Status: Running

Check Service

sc query wazuh

Expected:

STATE : RUNNING

🔹 Check Logs

type "C:\Program Files (x86)\ossec-agent\ossec.log"

You should see:

Connected to server

🔹 Wazuh Dashboard

Go to:

Wazuh → Agents

🚀 Install Sysmon on Windows Server 2022

🟢 STEP 1: Download Sysmon (Official Source)

1. Open browser on Windows Server 2022
2. Go to:

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

3. Click Download Sysmon
4. File downloaded:

Sysmon.zip

⚠️ Do NOT download from GitHub or third-party sites

🟢 STEP 2: Extract & Move Sysmon (VERY IMPORTANT)

1. Right-click Sysmon.zip
2. Click Extract All
3. After extraction, you will see:

Sysmon64.exe

Sysmon.exe

Eula.txt

4. Create directory:

C:\Sysmon

5. Move ALL extracted files to:

C:\Sysmon

✅ Final folder structure:

C:\Sysmon\Sysmon64.exe

C:\Sysmon\Sysmon.exe

C:\Sysmon\Eula.txt

🟢 STEP 3: Download Sysmon Configuration (CRITICAL)

3.1 Download Config File

Open browser and download SwiftOnSecurity Sysmon config:

https://github.com/SwiftOnSecurity/sysmon-config

Download:

sysmonconfig.xml

3.2 Move Config File

Move sysmonconfig.xml to:

C:\Sysmon

✅ Final structure:

C:\Sysmon\Sysmon64.exe

C:\Sysmon\sysmonconfig.xml

⚠️ Sysmon WILL FAIL if XML is not in same folder

🟢 STEP 4: Install Sysmon (RUN AS ADMIN)

4.1 Open PowerShell as Administrator

❗ MANDATORY

Right-click PowerShell → Run as Administrator

4.2 Navigate to Sysmon Directory

cd C:\Sysmon

Verify:

dir

You must see:

Sysmon64.exe

sysmonconfig.xml

4.3 Install Sysmon (FINAL COMMAND)

.\Sysmon64.exe -accepteula -i sysmonconfig.xml

✅ Expected Output (SUCCESS)

System Monitor v15.xx

Sysmon64 installed.

SysmonDrv installed.

SysmonDrv started.

Sysmon64 started.

🚀 No errors = Sysmon installed correctly

🟢 STEP 5: Verify Sysmon Installation

5.1 Verify Services

sc query sysmon64

✔ Expected:

STATE : RUNNING

5.2 Verify Event Logs

1. Open Event Viewer
2. Navigate to:

Applications and Services Logs

➔ Microsoft

➔ Windows

➔ Sysmon

➔ Operational

✔ You should see events:

- Event ID 1 – Process Create
- Event ID 3 – Network Connection
- Event ID 13 – Registry Change

🟢 STEP 6: Verify Wazuh Is Receiving Sysmon Logs

On Wazuh Dashboard

Navigate to:

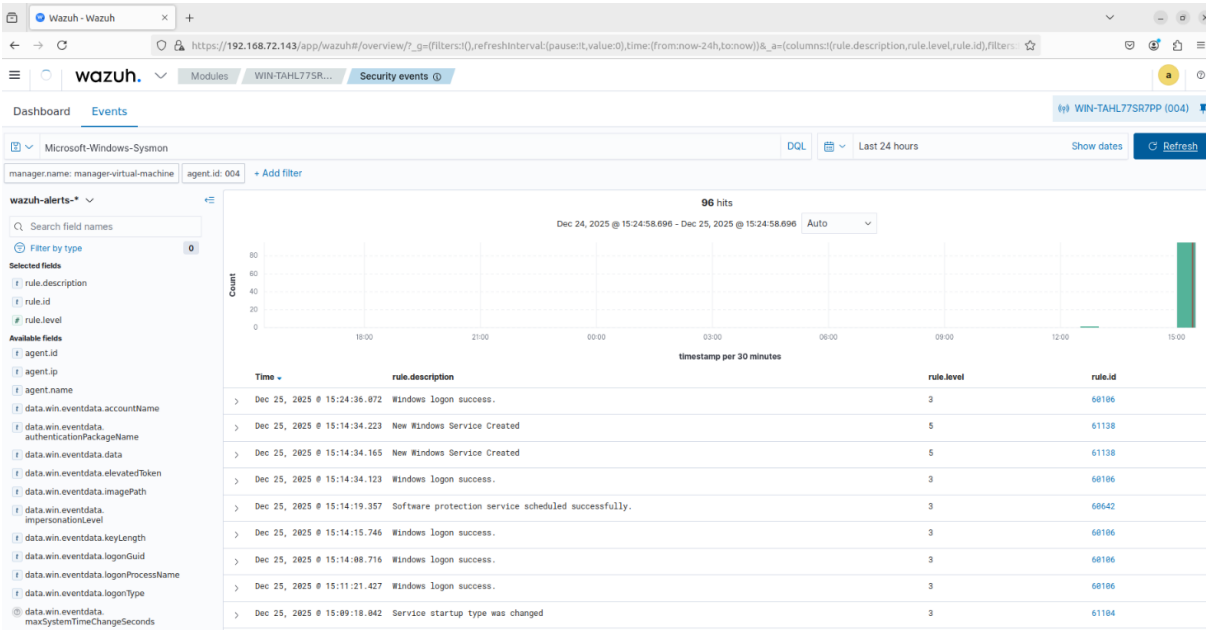
Security Events ➔ Events

Filter:

event.provider : Microsoft-Windows-Sysmon

✔ You should see:

- Process creation alerts
- Registry modification alerts
- Network events



🔎 WEEK 1 GATE CHECK – SYSmon (PASSED ✅)

- ✔ Sysmon service running
- ✔ Sysmon events visible in Event Viewer
- ✔ Sysmon logs received by Wazuh
- ✔ Windows agent Active

❌ COMMON SYSmon ERRORS & FIXES (IMPORTANT)

Error	Cause	Fix
sysmon64.exe not recognized	Wrong directory	Use cd C:\Sysmon
Failed to open xml configuration	XML missing	Move xml to same folder
You need to launch as Administrator	PowerShell not elevated	Run as Admin
Access denied	Antivirus blocking	Temporarily disable Defender
No events in Wazuh	Agent not restarted	Restart wazuh agent

🔁 OPTIONAL (SAFE) TROUBLESHOOTING COMMANDS

Restart Sysmon:

.\Sysmon64.exe -c sysmonconfig.xml

Uninstall (if needed):

.\Sysmon64.exe -u

🔹 WEEK 2 – Detection Rules (Logic)

1️⃣ Enable File Integrity Monitoring (FIM)

Edit Manager Config

sudo nano /var/ossec/etc/ossec.conf

Add:

<syscheck>

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

<frequency>60</frequency>

</syscheck>

```
<syscheck>
  <frequency>60</frequency>
  <scan_on_start>yes</scan_on_start>

  <directories check_all="yes">/etc</directories>
  <directories check_all="yes">/var/www</directories>
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
</syscheck>
```

Restart:

sudo systemctl restart wazuh-manager

Test FIM Alert

sudo nano /etc/passwd

✔ Alert generated within <5 seconds
In Wazuh Dashboard → Security events

You should see:

- Rule: Integrity checksum changed
- File: /etc/passwd
- Agent: your Ubuntu manager or Linux agent

📌 Rule examples:

- 550 – File modified
- 554 – Integrity checksum changed

---

1 2 Custom Decoder & Rule (Proprietary Logs)

12.1 Create Log File

sudo touch /var/log/myapp.log

sudo chmod 666 /var/log/myapp.log

12.2 Create Decoder (CORRECT FORMAT)

sudo nano /var/ossec/etc/decoders/myapp_decoders.xml

<decoder name="myapp-error">

  <prematch>ERROR</prematch>

</decoder>

⚠️ DO NOT use <decoders> tag
⚠️ DO NOT use <group> in decoder

Permissions:

sudo chmod 640 /var/ossec/etc/decoders/myapp_decoders.xml

12.3 Create Rule

sudo nano /var/ossec/etc/rules/myapp_rules.xml

<group name="myapp">

  <rule id="100901" level="8">

<match>ERROR</match>

<description>MyApp error log detected<>

</rule>

</group>

12.4 Validate Rules

sudo /var/ossec/bin/wazuh-analysisd -t

Restart:

sudo systemctl restart wazuh-manager

12.5 Test Custom Log

echo "ERROR Database connection failed" >> /var/log/myapp.log

✔ Dashboard Alert:

- Rule ID: 100200
- Level: 10

✅ if it shows error then follow it FINAL FIX (NO MORE WARNINGS)

🟢 STEP 1: DELETE THE WRONG DECODER FILE (MANDATORY)

Run **exactly this**:

```
sudo rm -f /var/ossec/etc/decoders/myapp_decoders.xml
```

Verify it is gone:

```
ls -l /var/ossec/etc/decoders/
```

✅ Directory should be **empty or contain only default files**

🟢 STEP 2: CONFIRM CORRECT DECODER LOCATION

Your decoder must be here:

```
ls -l /var/ossec/ruleset/decoders/ | grep myapp
```

You should see something like:

```
100-myapp_decoders.xml
```

If not, recreate it:

```
sudo nano /var/ossec/ruleset/decoders/100-myapp_decoders.xml
```

✅ Correct decoder file (FINAL & SAFE)

```
<decoder name="myapp-error">
  <prematch>^ERROR</prematch>
</decoder>
```

Save & exit.

Set permissions:

```
sudo chown wazuh:wazuh /var/ossec/ruleset/decoders/100-
myapp_decoders.xml
sudo chmod 640 /var/ossec/ruleset/decoders/100-myapp_decoders.xml
```

🟢 STEP 3: CONFIRM RULE FILE LOCATION

Rules must be in:

```
/var/ossec/etc/rules/
```

Edit rule:

```
sudo nano /var/ossec/etc/rules/myapp_rules.xml
```

✅ Correct rule (FINAL)

```
<group name="myapp">

  <rule id="100901" level="8">
    <match>ERROR</match>
    <description>MyApp error log detected<>
  </rule>

</group>
```

Permissions:

```
sudo chown wazuh:wazuh /var/ossec/etc/rules/myapp_rules.xml
sudo chmod 640 /var/ossec/etc/rules/myapp_rules.xml
```

🟢 STEP 4: VALIDATE (THIS TIME IT WILL BE CLEAN)

```
sudo /var/ossec/bin/wazuh-analysisd -t
```

✅ EXPECTED OUTPUT

```
Analysisd configuration OK
```

❌ No warnings
❌ No permission errors
❌ No decoder errors

🟢 STEP 5: RESTART WAZUH MANAGER

```
sudo systemctl restart wazuh-manager
```

Check status:

```
sudo systemctl status wazuh-manager
```

🧪 FINAL TEST (PROOF)

```
echo "ERROR Database connection failed" | sudo tee -a /var/log/myapp.log
```

1️⃣3️⃣ Enable Vulnerability Detector

Edit Config

sudo nano /var/ossec/etc/ossec.conf

Add:

<vulnerability-detector>

  <enabled>yes</enabled>

  <interval>5m</interval>

  <run_on_start>yes</run_on_start>

</vulnerability-detector>

or,

<vulnerability-detector>

<enabled>yes</enabled>

</vulnerability-detector>

Restart:

sudo systemctl restart wazuh-manager

Confirm Vulnerability Scan Started (IMPORTANT)

Run this on the manager:

sudo grep -i vulnerability /var/ossec/logs/ossec.log

✅ Expected output:

Starting vulnerability detection scan

Fetching vulnerability feeds

Vulnerability detection scan completed

If you see this → SCAN IS RUNNING

Confirm Syscollector Is Working

Vulnerability Detector depends on Syscollector.

Check:

sudo grep -i syscollector /var/ossec/logs/ossec.log

Expected:

syscollector: INFO: Inventory data sent

If syscollector is disabled ➔ CVEs will never appear.

Where the CVE Alert Is CREATED

Internally stored here:

/var/ossec/queue/db/vulnerabilities/

You don't need to open it — just FYI.

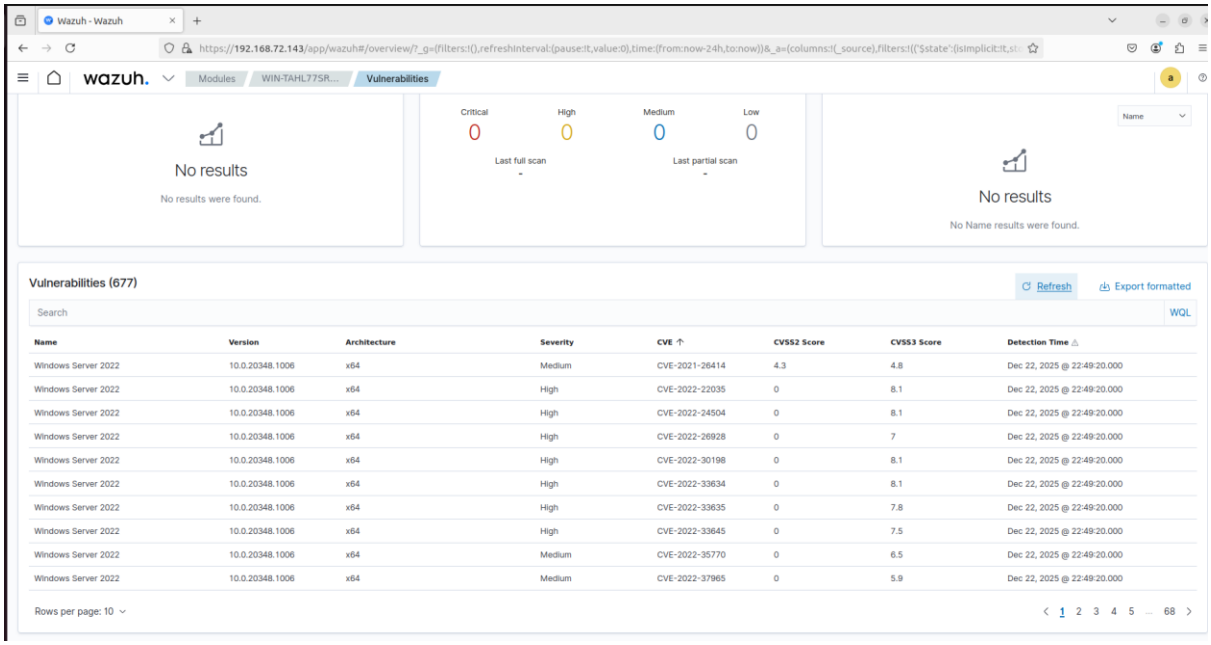
🖥️View CVE Alerts in Wazuh Dashboard (EXACT CLICKS)

📍 METHOD 1 (BEST & OFFICIAL)

1. Open Wazuh Dashboard
2. Left sidebar ➔ Vulnerabilities
3. Select agent:
    - manager-virtual-machine
    - windows-server-2022

✔ CVE alerts visible in Dashboard

✔ Example: openssl → CVE-2023-0464



---

1 🦶 Week 2 Gate Check (PASSED ✅)

✔ File modification alert <5 sec

✔ Custom log detection working

✔ CVE alerts visible

✔ SCA benchmarks detected

🚫 COMMON ERRORS & HOW TO AVOID

Error	Cause	Fix
Invalid element decoders	Wrong XML structure	Remove wrapper
if_matched_sid ignored	Decoder not loaded	Fix permissions
Agent version mismatch	Agent newer than manager	Upgrade manager
Auth key not imported	Missed key step	Import key
Service not found	MSI not installed	Reinstall agent