🛡️ Wazuh “Lazy” FIM Configuration

Version: 1.0 (Stable) **Date:** February 3, 2026 **Scope:** Windows Endpoints (Laptops/Desktops)

Overview

This configuration enables **Real-Time File Integrity Monitoring (FIM)** on critical Windows system folders. Unlike standard monitoring which scans every 12 hours, this configuration triggers an immediate alert the second a file is created, modified, or deleted in high-risk "persistence" locations often used by malware and attackers.

How It Works (The Logic)

A. The "Trigger" Explained

I selected these three locations because they align with the **MITRE ATT&CK** framework for "Persistence" (staying on the system after a reboot).

1. **Startup Folders:**
   - *The Threat:* Attackers drop a file here so their RAT (Remote Access Trojan) starts every morning when you turn on the PC.
   - *The Trap:* We monitor `C:\ProgramData\...\Startup` (All Users) and `C:\Users\*\...\Startup` (Individual Users).
2. **Scheduled Tasks (`System32\Tasks`):**
   - *The Threat:* Sophisticated malware hides as a "Windows Update" task that runs deeply in the background.
   - *The Trap:* Any new file created here is instantly flagged.
3. **Drivers/Etc (HOSTS File):**
   - *The Threat:* Attackers modify the `hosts` file to redirect your browser (e.g., `google.com` -> `malware-site.com`).
   - *The Trap:* Any modification to this folder is treated as a critical network tampering event.

B. Real-time vs. Periodic

- **Standard FIM:** Scans files every 12 hours(Wazuh). If a hacker enters at 1:00 PM and leaves at 2:00 PM, you won't know until the scan runs at midnight.
- **Our Configuration:** Uses Windows file system events. The operating system literally "pokes" the Wazuh Agent the millisecond a file is touched.

Deployment Instructions

We use a "One-Time Access" method to run the script. This tells Windows: *"Lower the security shields ONLY for this specific window, and raise them back up as soon as I close it."* This is the safest way to execute scripts.

Step 1: Prepare the Script

1. Copy the code into a text file and save it as **SetupWazuh.ps1**.
    - *Make sure you select "All Files" when saving so it doesn't become .txt.*
2. Place the file on the target computer (Desktop, USB, or Network Share).

Step 2: Run with "One-Time Access"

Since Windows blocks custom scripts by default, follow these exact steps to run it safely:

1. Open the **Start Menu** and type PowerShell.
2. **Right-click** "Windows PowerShell" and select **Run as Administrator**.
3. In the blue window, type the following command and hit **Enter**:
   PowerShell

```
None
    1.
       Set-ExecutionPolicy Bypass -Scope Process
```

4\.
   *(If asked for confirmation, type **A** or **Y** and hit Enter).*
   Why do we do this? The -Scope Process flag ensures this permission only lasts as long as this specific window is open. Once you close it, your security settings revert to normal.

5. Run the script by typing the path (or dragging the file into the window):
   PowerShell

```
None
    2.
       C:\Users\YourName\Desktop\SetupWazuh.ps1
```

6\.

Step 3: Follow the Prompts

1. **Path:** Press **Enter** to accept the default ossec.conf location.
2. **Server IP:** Enter your Wazuh Manager IP (e.g., 192.168.1.166).

3. **Extras:** Add any extra drives you want to monitor (e.g., E:\SecretFiles), or press Enter to skip.
4. **Finish:** The script will automatically backup your old config, apply the Hacker Traps, and restart the agent.

Success: You will see a green message: SUCCESS: Agent is CONNECTED and MONITORING.

Note: If anything goes wrong or you want to revert to your default settings, the backup file is created at the start of auto-execution. Just go to the folder and rename it.

Testing & Validation

The "Fake Backdoor" Test

To ensure the "Burglar Alarm" is functional, perform this test after every deployment.

1. **Navigate to the Trap:**
   - Go to `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`.
   - *Note: If you cannot find `ProgramData`, paste the path directly into the Explorer address bar.*
2. **Trigger the Alarm:**
   - Create a text file named `HACKER_TEST.txt`.
   - *Tip:* If Windows prevents creation, create it on the Desktop and **drag-and-drop** it into the folder.
3. **Verify:**
   - Open Wazuh Dashboard.
   - Go to **Modules > Security events**.
   - **Success Criteria:** You see an alert: `"File added to the system"` with the path to your test file.

Troubleshooting

- **Alert didn't appear?** Check if you accidentally duplicated a folder path (e.g., `%PROGRAMDATA%` vs `C:\ProgramData`). Duplicates silently disable monitoring for that specific folder.
- **Service won't start?** Use `taskkill /F /IM wazuh-agent.exe` to kill any "zombie" processes and try starting again. Or simply open “Services”, track down wazuhsvc and restart it.