Project Title: Automated Malware Detection and Remediation System

Framework: Wazuh SIEM + YARA Engine + Custom Active Response

1. Executive Summary

Developed a real-time endpoint security solution that automates the lifecycle of malware detection and containment. By integrating Wazuh's File Integrity Monitoring (FIM) with the YARA signature-matching engine, the system achieves sub-second response times for identifying and quarantining malicious files, significantly reducing the window of vulnerability.

2. Core Architecture

The system operates on a "Detection-Analysis-Action" loop:

- **Detection (Wazuh FIM):** The agent monitors a specified directory (`/home/ubuntu/downloads`) using the Linux `inotify` kernel subsystem for real-time file creation or modification.
- **Analysis (YARA Engine):** Upon detection, the Wazuh Manager triggers an Active Response script on the agent. This script passes the file through YARA, using 4,000+ industry-standard signatures from Florian Roth's signature-base.
- **Action (Automated Remediation):** If YARA returns a positive match, the script instantly moves the file to a secure, root-owned quarantine directory (`/root/quarantine`) and appends a `.malware` extension.

3. Implementation Details

- **Custom Rules (Manager):** Created Rule `108001` (Level 12) to escalate YARA "Scan Results" to high-severity alerts.
- **Active Response Script (Agent):** A bash script (`yara-scan.sh`) that parses JSON input from Wazuh, executes YARA binaries, and handles file manipulation.
- **Centralized Configuration:** Managed agent policies via Wazuh Groups to ensure consistent monitoring across endpoints.

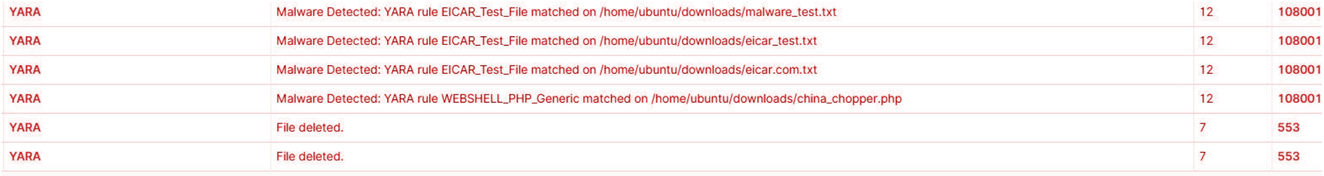
---

4. Verification & Results

A. The Dashboard View

This view confirms that the Wazuh Manager successfully processed the alerts and categorized them correctly.

- **Result:** Detected `EICAR_Test_File` and `WEBSHELL_PHP_Generic` (China Chopper).
- **Alert Level:** 12 (Critical).
- **Outcome:** Rule `553` (File deleted/moved) followed immediately after detection.

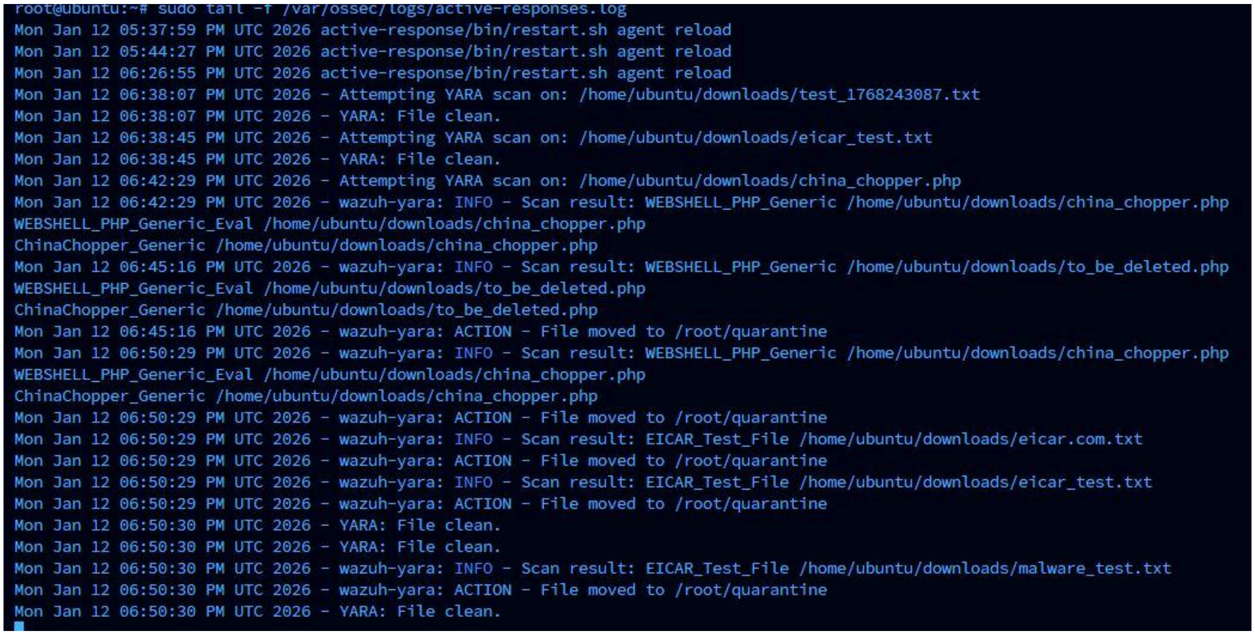


YARA	Malware Detected: YARA rule EICAR_Test_File matched on /home/ubuntu/downloads/malware_test.txt	12	108001
YARA	Malware Detected: YARA rule EICAR_Test_File matched on /home/ubuntu/downloads/eicar_test.txt	12	108001
YARA	Malware Detected: YARA rule EICAR_Test_File matched on /home/ubuntu/downloads/eicar.com.txt	12	108001
YARA	Malware Detected: YARA rule WEBSHELL_PHP_Generic matched on /home/ubuntu/downloads/china_chopper.php	12	108001
YARA	File deleted.	7	553
YARA	File deleted.	7	553

B. The Execution Log

The `active-responses.log` provides a forensic audit trail of the script's real-time performance.

- **Timeline:** At 06:50:29, the system processed four separate malware files in a single second.
- **Log Sequence:** `Attempting scan` -> `Scan result` -> `ACTION - File moved`.

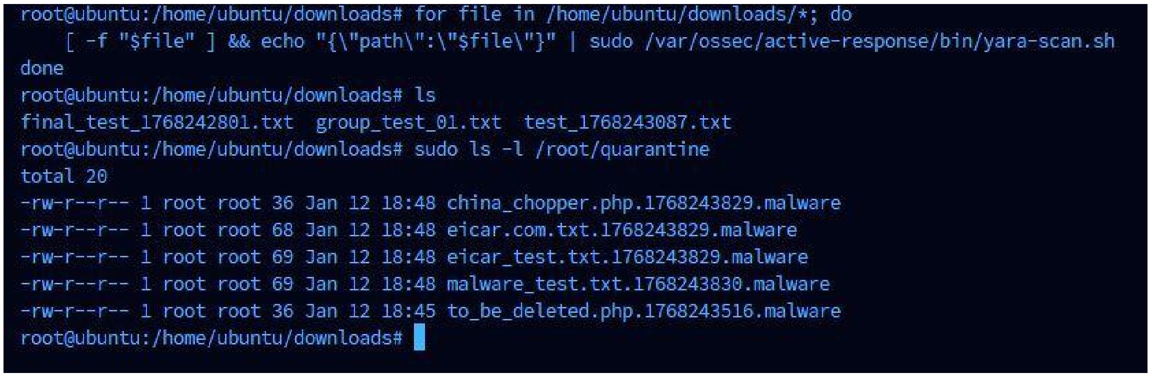


```
root@ubuntu:~# sudo tail -f /var/ossec/logs/active-responses.log
Mon Jan 12 05:37:59 PM UTC 2026 active-response/bin/restart.sh agent reload
Mon Jan 12 05:44:27 PM UTC 2026 active-response/bin/restart.sh agent reload
Mon Jan 12 06:26:55 PM UTC 2026 active-response/bin/restart.sh agent reload
Mon Jan 12 06:38:07 PM UTC 2026 - Attempting YARA scan on: /home/ubuntu/downloads/test_1768243087.txt
Mon Jan 12 06:38:07 PM UTC 2026 - YARA: File clean.
Mon Jan 12 06:38:45 PM UTC 2026 - Attempting YARA scan on: /home/ubuntu/downloads/eicar_test.txt
Mon Jan 12 06:38:45 PM UTC 2026 - YARA: File clean.
Mon Jan 12 06:42:29 PM UTC 2026 - Attempting YARA scan on: /home/ubuntu/downloads/china_chopper.php
Mon Jan 12 06:42:29 PM UTC 2026 - wazuh-yara: INFO - Scan result: WEBSHELL_PHP_Generic /home/ubuntu/downloads/china_chopper.php
WEBSHELL_PHP_Generic_Eval /home/ubuntu/downloads/china_chopper.php
ChinaChopper_Generic /home/ubuntu/downloads/china_chopper.php
Mon Jan 12 06:45:16 PM UTC 2026 - wazuh-yara: INFO - Scan result: WEBSHELL_PHP_Generic /home/ubuntu/downloads/to_be_deleted.php
WEBSHELL_PHP_Generic_Eval /home/ubuntu/downloads/to_be_deleted.php
ChinaChopper_Generic /home/ubuntu/downloads/to_be_deleted.php
Mon Jan 12 06:45:16 PM UTC 2026 - wazuh-yara: ACTION - File moved to /root/quarantine
Mon Jan 12 06:50:29 PM UTC 2026 - wazuh-yara: INFO - Scan result: WEBSHELL_PHP_Generic /home/ubuntu/downloads/china_chopper.php
WEBSHELL_PHP_Generic_Eval /home/ubuntu/downloads/china_chopper.php
ChinaChopper_Generic /home/ubuntu/downloads/china_chopper.php
Mon Jan 12 06:50:29 PM UTC 2026 - wazuh-yara: ACTION - File moved to /root/quarantine
Mon Jan 12 06:50:29 PM UTC 2026 - wazuh-yara: INFO - Scan result: EICAR_Test_File /home/ubuntu/downloads/eicar.com.txt
Mon Jan 12 06:50:29 PM UTC 2026 - wazuh-yara: ACTION - File moved to /root/quarantine
Mon Jan 12 06:50:29 PM UTC 2026 - wazuh-yara: INFO - Scan result: EICAR_Test_File /home/ubuntu/downloads/eicar_test.txt
Mon Jan 12 06:50:29 PM UTC 2026 - wazuh-yara: ACTION - File moved to /root/quarantine
Mon Jan 12 06:50:30 PM UTC 2026 - YARA: File clean.
Mon Jan 12 06:50:30 PM UTC 2026 - YARA: File clean.
Mon Jan 12 06:50:30 PM UTC 2026 - wazuh-yara: INFO - Scan result: EICAR_Test_File /home/ubuntu/downloads/malware_test.txt
Mon Jan 12 06:50:30 PM UTC 2026 - wazuh-yara: ACTION - File moved to /root/quarantine
Mon Jan 12 06:50:30 PM UTC 2026 - YARA: File clean.
```

C. The Quarantine Zone

This provides the "Ground Truth" that the threats were successfully isolated from the user environment.

- **Status:** The `/home/ubuntu/downloads` folder is verified clean of all threats.
- **Evidence:** The `/root/quarantine` folder contains the isolated binaries with timestamped metadata.



```
root@ubuntu:/home/ubuntu/downloads# for file in /home/ubuntu/downloads/*; do
    [ -f "$file" ] && echo "{\"path\":\"$file\"}" | sudo /var/ossec/active-response/bin/yara-scan.sh
done
root@ubuntu:/home/ubuntu/downloads# ls
final_test_1768242801.txt  group_test_01.txt  test_1768243087.txt
root@ubuntu:/home/ubuntu/downloads# sudo ls -l /root/quarantine
total 20
-rw-r--r-- 1 root root 36 Jan 12 18:48 china_chopper.php.1768243829.malware
-rw-r--r-- 1 root root 68 Jan 12 18:48 eicar.com.txt.1768243829.malware
-rw-r--r-- 1 root root 69 Jan 12 18:48 eicar_test.txt.1768243829.malware
-rw-r--r-- 1 root root 69 Jan 12 18:48 malware_test.txt.1768243830.malware
-rw-r--r-- 1 root root 36 Jan 12 18:45 to_be_deleted.php.1768243516.malware
root@ubuntu:/home/ubuntu/downloads# 
```

5. Key Achievements

- **Signature-Based Protection:** Implemented detection for APT-style webshells using community-driven threat intelligence.
- **Zero-Trust Directory:** Every file entering the monitored zone is automatically vetted before it can be accessed.
- **Incident Response Efficiency:** Automated the "Containment" phase, reducing response time from minutes to milliseconds.