

# Detecting the EICAR Test File with Wazuh SIEM

## Project Overview

This project demonstrates how to detect the EICAR test file using Wazuh SIEM. The goal is to showcase Wazuh's ability to capture malware events and file integrity changes from Windows endpoints.

## Objective

- Generate the EICAR test file on a Windows endpoint.
- Ensure the Wazuh agent collects Windows Defender and FIM logs.
- Detect and analyze the alerts in the Wazuh Dashboard.
- Map the detection to the MITRE ATT&CK framework.


## What is the EICAR Test File?

The EICAR test file is a harmless string of characters designed to trigger antivirus software.

It is not real malware, but a safe way to test detection pipelines.

### EICAR string:

[X5O!P%@AP\[4\PZX54\(P^\)7CC\)7}\\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\\$H+H\\*](#)

 Important: Do not rename it to `.exe` — the `.com` extension is enough for AV to detect it.


## Step 1: Generate the EICAR Test File

### PowerShell

```
Set-Content -Path "$env:USERPROFILE\Desktop\eicar.com" -Value 'X5O!P%  
@AP\[4\PZX54\(P^\)7CC\)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!  
$H+H*'
```

### Command Prompt

```
echo X5O!P%%@AP\[4\PZX54\(P^\)7CC\)7}\$EICAR-STANDARD-ANTIVIRUS-  
TEST-FILE!\$H+H\* > %USERPROFILE%\Desktop\eicar.com
```

 Result: The file is created on the Desktop.  
Windows Defender should immediately detect and quarantine it.

## Step 2: Configure Wazuh Agent to Monitor Defender Logs

Ensure your Windows agent's **ossec.conf** includes the Defender event channel:

**xml**

```
<localfile>
  <log_format>eventchannel</log_format>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
</localfile>
```

### Restart the agent:

```
net stop wazuh
net start wazuh
```

## Step 3: Detection in Wazuh

### File Integrity Monitoring (FIM)

When eicar.com is written to disk, Wazuh FIM triggers an alert:

```
{
  "rule.description": "File added to the system",
  "syscheck.path": "C:\\Users\\Public\\Desktop\\eicar.com",
  "syscheck.event": "added"
}
```

### Windows Defender Malware Detection

When Defender quarantines the file, Wazuh parses the Defender log:

```
{
  "rule.description": "Trojan detected (EICAR-Test-File)",
  "win.system.providerName": "Microsoft-Windows-Windows Defender",
  "win.system.eventID": "1116",
  "win.eventdata.ThreatName": "EICAR-Test-File",
  "win.eventdata.Action": "Quarantine"
}
```

## Step 4: Viewing Alerts in the Wazuh Dashboard

### Threat Hunting

- Search for: EICAR

### Security Events

- Set severity filter to **Critical**.
- Look for alerts with rule.description = "Trojan detected (EICAR-Test-File)".
- Example screenshot:

## **Alerts.json (Server-side)**

View raw alerts directly on the Wazuh server:

```
sudo tail -f /var/ossec/logs/alerts/alerts.json
```

## **MITRE ATT&CK Mapping**

Although EICAR is not a real threat, it can be mapped for training purposes:

- **T1105 – Ingress Tool Transfer** (malware/tool dropped into environment)
- **T1204 – User Execution** (user attempts to run malicious file)

## **Conclusion**

- The EICAR file provides a safe way to test malware detection.
- Wazuh FIM detects file creation.
- Windows Defender logs confirm malware detection.
- Alerts appear in both Threat Hunting and Security Events dashboards.

