

Detecting MITRE T1070.004 / T1485 Detected — File Deletion & Data Destruction using wazuh.

Objective:

Validate detection, alerting, and response capabilities for host-based file deletion (T1070.004) and data destruction (T1485) on the windows agent and identify gaps in logging, retention, and automated containment.

MITRE mapping:

- Technique: T1070.004 — *File Deletion* (sub-technique of T1070 — Indicator Removal on Host)
- Technique: T1485 — *Data Destruction*
- Tactics: Defense Evasion (primary for T1070.004) and Impact (primary for T1485)

Goals :

Confirm that Wazuh and SOC procedures detect and escalate file-deletion and destructive behavior, preserve sufficient forensic evidence, and enable timely recovery from data loss.

Before Alert Triggered:

Check if the timestamp 12:07 is the last attack that was triggered on the Wazuh manager before this alert.

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description
Nov 11, 2025 @ 12:07:52.7...	windows-wazuhh	T1070.004 T1485	Defense Evasion, Impact	File deleted.
Nov 11, 2025 @ 12:07:25.1...	windows-wazuhh	T1087	Discovery	Discovery activity executed
Nov 11, 2025 @ 12:07:25.0...	windows-wazuhh	T1087	Discovery	Discovery activity executed
Nov 11, 2025 @ 12:07:25.0...	windows-wazuhh	T1087	Discovery	Discovery activity executed
Nov 11, 2025 @ 12:07:25.0...	windows-wazuhh	T1087	Discovery	Discovery activity executed
Nov 11, 2025 @ 12:07:21.2...	windows-wazuhh	T1059.001	Execution	C:\Windows\SysWOW64\
Nov 11, 2025 @ 12:07:18.7...	windows-wazuhh	T1070.004	Defense Evasion	Powershell was used to de
Nov 11, 2025 @ 12:07:18.7...	windows-wazuhh	T1059.001	Execution	C:\Windows\SysWOW64\
Nov 11, 2025 @ 12:07:16.4...	windows-wazuhh	T1070.004	Defense Evasion	Powershell was used to de

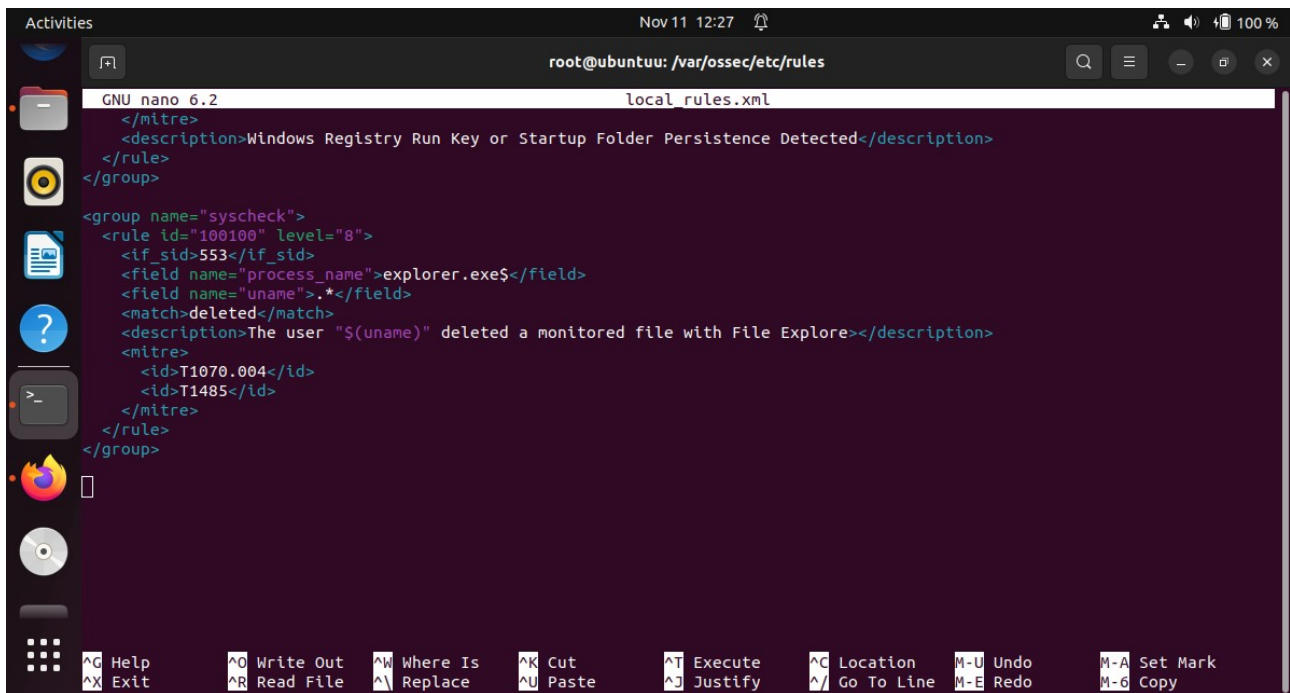
Steps to Reproduce :

Open this dir : `cd /var/ossec/etc/rules`

`$nano local_rules.xml`

Add below the rules on the local rules file :

```
<group name="syscheck">
  <rule id="100100" level="8">
    <if_sid>553</if_sid>
    <field name="process_name">explorer.exe$</field>
    <field name="uname">.*</field>
    <match>deleted</match>
    <description>The user "$(uname)" deleted a monitored file with File
Explore></description>
    <mitre>
      <id>T1070.004</id>
      <id>T1485</id>
    </mitre>
  </rule>
</group>
```



```
GNU nano 6.2 local_rules.xml
</mitre>
<description>Windows Registry Run Key or Startup Folder Persistence Detected</description>
</rule>
</group>

<group name="syscheck">
  <rule id="100100" level="8">
    <if_sid>553</if_sid>
    <field name="process_name">explorer.exe</field>
    <field name="uname">.*</field>
    <match>deleted</match>
    <description>The user "${uname}" deleted a monitored file with File Explore</description>
    <mitre>
      <id>T1070.004</id>
      <id>T1485</id>
    </mitre>
  </rule>
</group>
```

Restart the Wazuh server to apply the configuration changes:

\$ systemctl restart wazuh-manager

Windows Agent :

Perform the following steps to configure the Wazuh FIM module to monitor file deletion in the C:\test directory.

1. Create the C:\test directory on the endpoint:

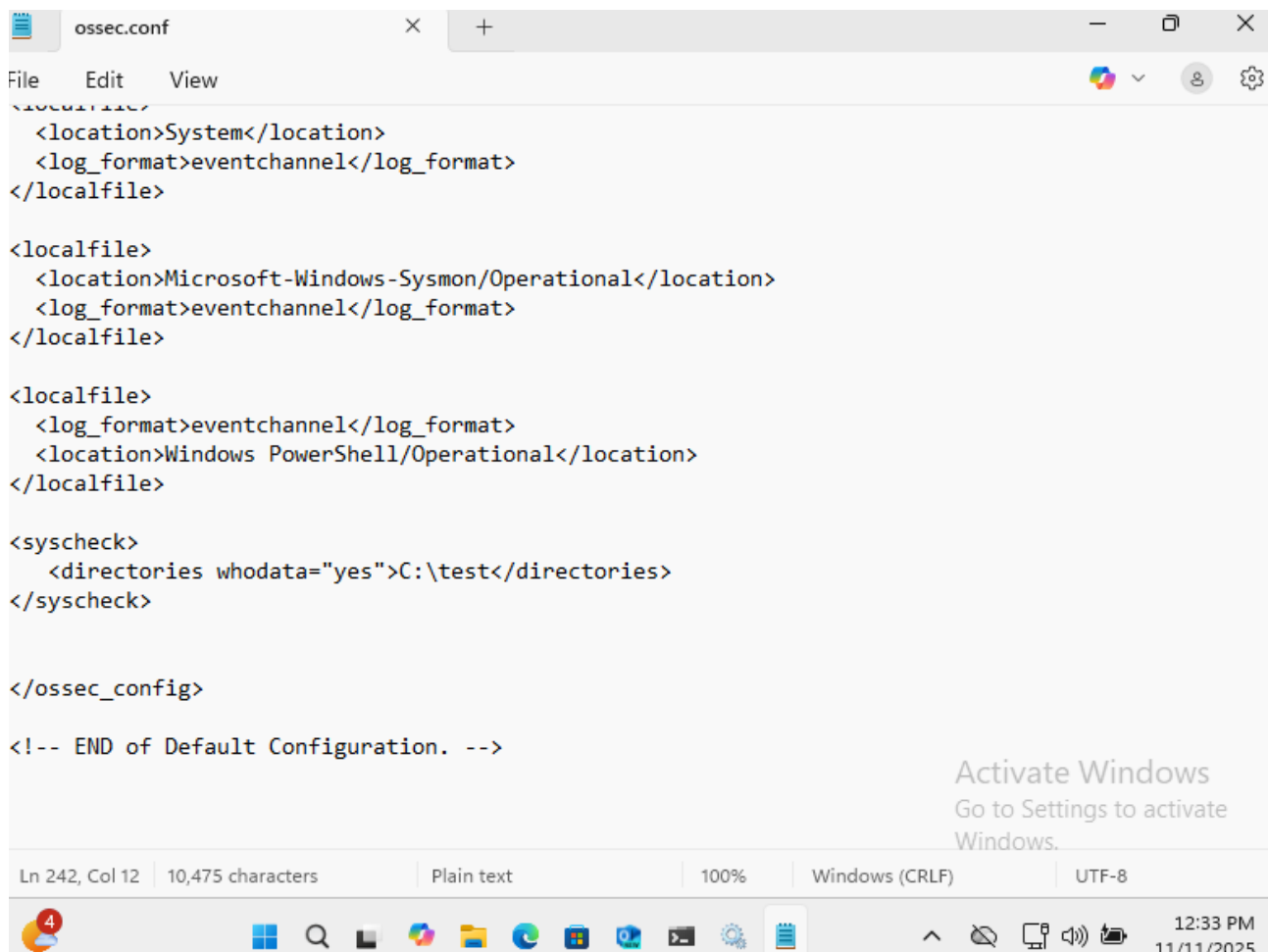
> mkdir C:\test

2 .Edit the Wazuh agent C:\Program Files (x86)\ossec-agent\ossec.conf configuration file of the Wazuh agent. Add the C:\test directory for monitoring:

<syscheck>

<directories whodata="yes">C:\test</directories>

</syscheck>

A screenshot of a Windows text editor window titled 'ossec.conf'. The window shows the configuration file content, which includes XML tags for localfile and syscheck. The localfile section has three entries with different locations and log formats. The syscheck section has a directory entry. The file ends with a comment indicating the end of the default configuration. The status bar at the bottom shows 'Ln 242, Col 12', '10,475 characters', 'Plain text', '100%', 'Windows (CRLF)', and 'UTF-8'. An 'Activate Windows' watermark is visible in the bottom right corner.

```
<!-- localfile -->
<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <log_format>eventchannel</log_format>
  <location>Windows PowerShell/Operational</location>
</localfile>

<syscheck>
  <directories whodata="yes">C:\test</directories>
</syscheck>

</ossec_config>

<!-- END of Default Configuration. -->
```

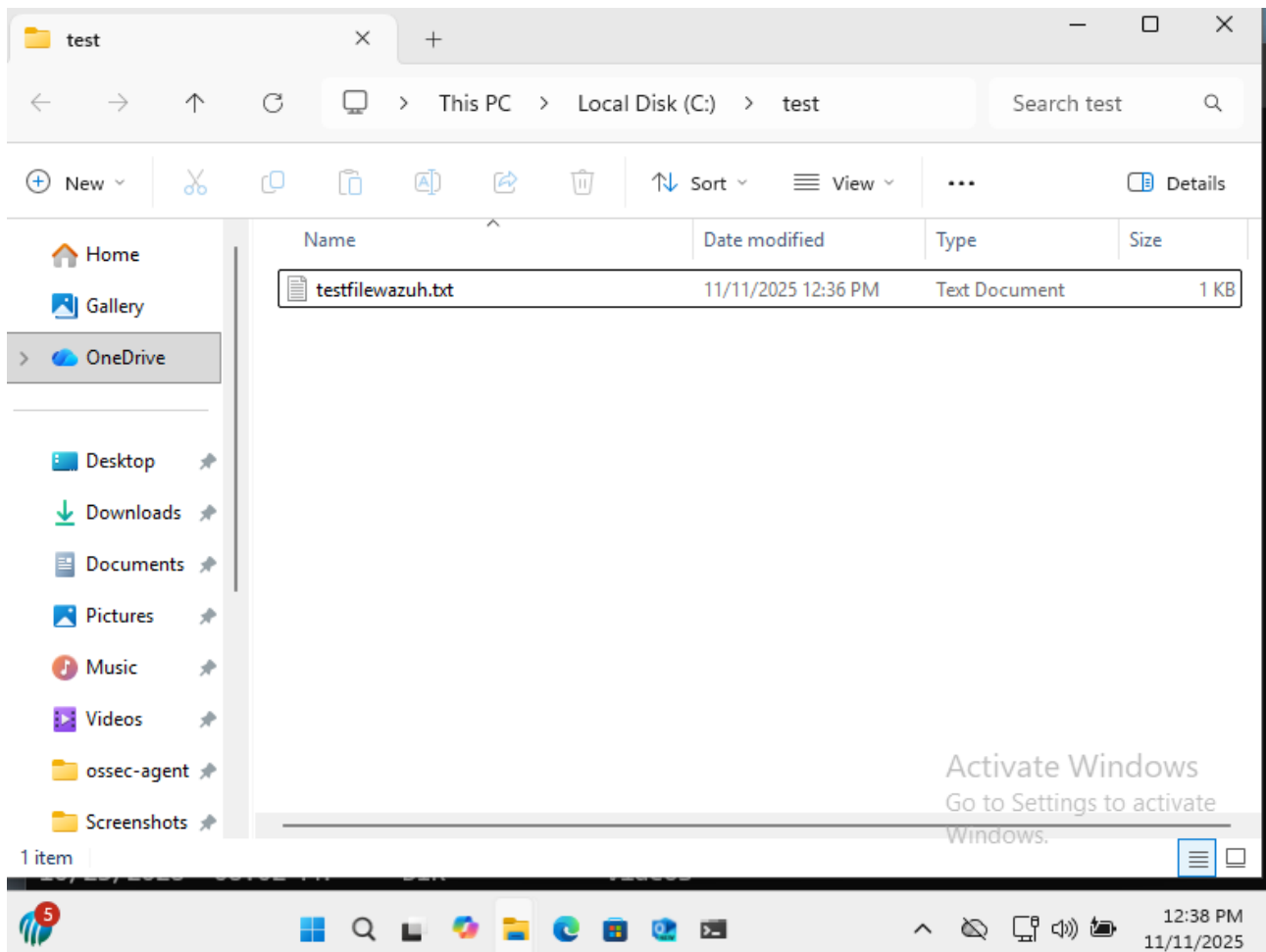
3. Restart the Wazuh agent using Powershell with administrator privilege to apply the changes:

> **Restart-Service -Name wazuh**

or service tab restart wazuh service.

Test the configuration

1. Create a text file with Notepad and save the file in the C:\test directory as testfilewazuh.txt.
2. Delete the testfilewazuh.txt file with Windows File Explorer.



I created the testfilewazuh.txt and i deleted the same file on triggering purpose .

Wazuh triggered alert on the wazuh manager :

Check the timestamp 12:40 the alert triggered file deletion and at the same time FIM (File Integrity Monitory) also triggered.

Activities Nov 11 12:40

Wazuh

192.168.1.49/app/mitre-attack#/overview/?tab=mitre&tabView=events&agentId=003

MITRE ATT&CK windows-wazuh

timestamp per 30 minutes

392 hits

Nov 10, 2025 @ 12:40:37.811 - Nov 11, 2025 @ 12:40:37.811

Export Formatted Reset view 770 available fields Columns Density 1 fields sorted Full screen

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description
Nov 11, 2025 @ 12:40:06.9...	windows-wazuhh	T1070.004 T1485	Defense Evasion, Impact	File deleted.
Nov 11, 2025 @ 12:40:00.8...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce
Nov 11, 2025 @ 12:40:00.6...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce
Nov 11, 2025 @ 12:39:53.8...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce
Nov 11, 2025 @ 12:39:53.6...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce
Nov 11, 2025 @ 12:39:03.8...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce
Nov 11, 2025 @ 12:39:03.8...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce
Nov 11, 2025 @ 12:39:00.5...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce
Nov 11, 2025 @ 12:39:00.5...	windows-wazuhh	T1055	Defense Evasion, Privil...	Sysmon - Suspicious Proce

Activities Nov 11 12:41

Wazuh

192.168.1.49/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&ag...

File Integrity M... windows-wazuh

timestamp per 30 minutes

6 hits

Nov 10, 2025 @ 12:41:23.981 - Nov 11, 2025 @ 12:41:23.981

Export Formatted Reset view 770 available fields Columns Density 1 fields sorted Full screen

mp	agent.name	syscheck.path	syscheck.event	rule.des...	rule
25 @ 12:40:06.9...	windows-wazuhh	c:\test\testfilewazuh.txt.txt	deleted	File deleted.	7
25 @ 12:36:11.4...	windows-wazuhh	c:\test\testfilewazuh.txt.txt	modified	Integrity ch...	7
25 @ 12:36:00.5...	windows-wazuhh	c:\test\new text document.txt	deleted	File deleted.	7
25 @ 12:36:00.5...	windows-wazuhh	c:\test\testfilewazuh.txt.txt	added	File added ...	5
25 @ 12:35:51.9...	windows-wazuhh	c:\test\new text document.txt	added	File added ...	5
25 @ 12:07:52.7...	windows-wazuhh	c:\test\new text document.txt.txt	deleted	File deleted.	7

Result :

The custom File Integrity Monitoring (FIM) rule successfully triggered in the Wazuh dashboard upon deletion of a monitored file via explorer.exe.

The alert matched MITRE ATT&CK techniques:

- **T1070.004** – Indicator Removal on Host: File Deletion
- **T1485** – Data Destruction

These techniques reflect adversary actions to remove or destroy files to conceal activities or cause damage. The alert included the deleting user and process details, confirming Wazuh's effective detection and attribution of file deletion events.