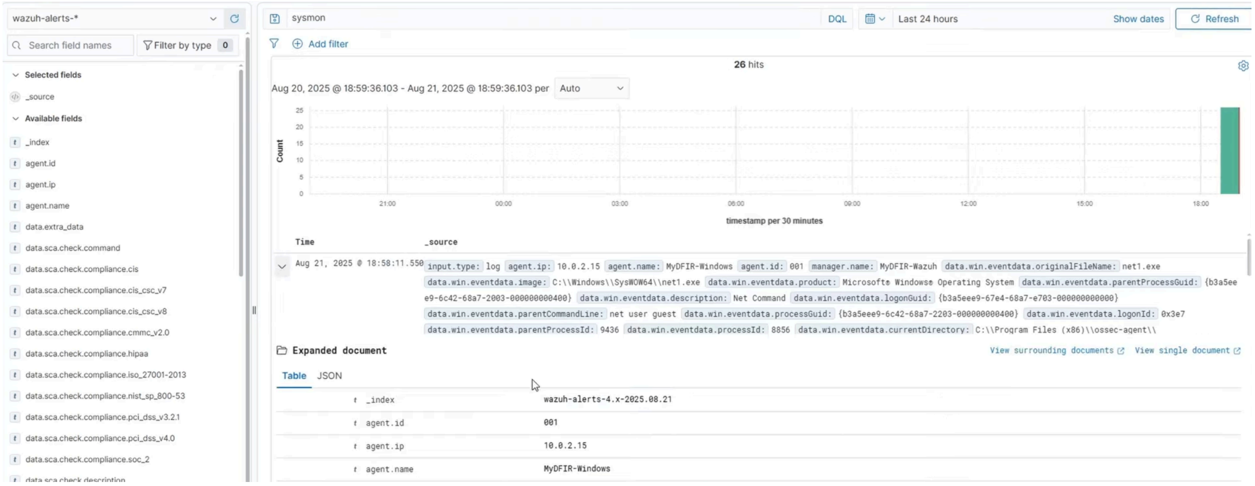
6. Configuring Wazuh Agent and Sysmon Forwarding


wazuh-alerts-*
sysmon
DQL
Last 24 hours
Show dates
Refresh
Search field names
Filter by type 0
Add filter
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.extra_data
data.sca.check.command
data.sca.check.compliance.cis
data.sca.check.compliance.cis_csc_v7
data.sca.check.compliance.cis_csc_v8
data.sca.check.compliance.cmmc_v2.0
data.sca.check.compliance.hipaa
data.sca.check.compliance.iso_27001-2013
data.sca.check.compliance.nist_sp_800-53
data.sca.check.compliance.pci_dss_v3.2.1
data.sca.check.compliance.pci_dss_v4.0
data.sca.check.compliance.soc_2
data.sca.check.description
26 hits
Aug 20, 2025 @ 18:59:36.103 - Aug 21, 2025 @ 18:59:36.103 per
Auto
Count
25
20
15
10
5
0
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
timestamp per 30 minutes
Expanded document
View surrounding documents
View single document
Table
JSON

```
Time                       _source
Aug 21, 2025 @ 18:58:11.550 input.type: log agent.ip: 10.0.2.15 agent.name: MyDFIR-Windows agent.id: 001 manager.name: MyDFIR-Wazuh data.win.eventdata.originalFileName: net1.exe
data.win.eventdata.image: C:\\Windows\\SysWOW64\\net1.exe data.win.eventdata.product: Microsoft® Windows® Operating System data.win.eventdata.parentProcessGuid: {b3a5ee
e9-6c42-68a7-2003-000000000400} data.win.eventdata.description: Net Command data.win.eventdata.logonGuid: {b3a5eee9-67e4-68a7-e703-000000000000}
data.win.eventdata.parentCommandLine: net user guest data.win.eventdata.processGuid: {b3a5eee9-6c42-68a7-2203-000000000400} data.win.eventdata.logonId: 0x3e7
data.win.eventdata.parentProcessId: 9436 data.win.eventdata.processId: 8856 data.win.eventdata.currentDirectory: C:\\Program Files (x86)\\ossec-agent\\
```

t _index	wazuh-alerts-4.x-2025.08.21
t agent.id	001
t agent.ip	10.0.2.15
t agent.name	MyDFIR-Windows

Steps:

1. From the Wazuh dashboard, deploy a Windows agent.

2. On the Windows 11 VM, install the agent using the provided command.

3. Edit ossec.conf to point log sources to Sysmon:

Original entries are removed or disabled.
Set location to:
Microsoft-Windows-Sysmon/Operational

4. Restart the Wazuh service.

5. Confirm in Wazuh dashboard under "Discover" that Sysmon logs are now indexed.