**Lab 6 Report: Sysmon Logging with Wazuh and Security Onion**

**Student Name:** Srivarsha Adla  
**Lab Title:** Using Wazuh to Add Sysmon Logging

**Objective**

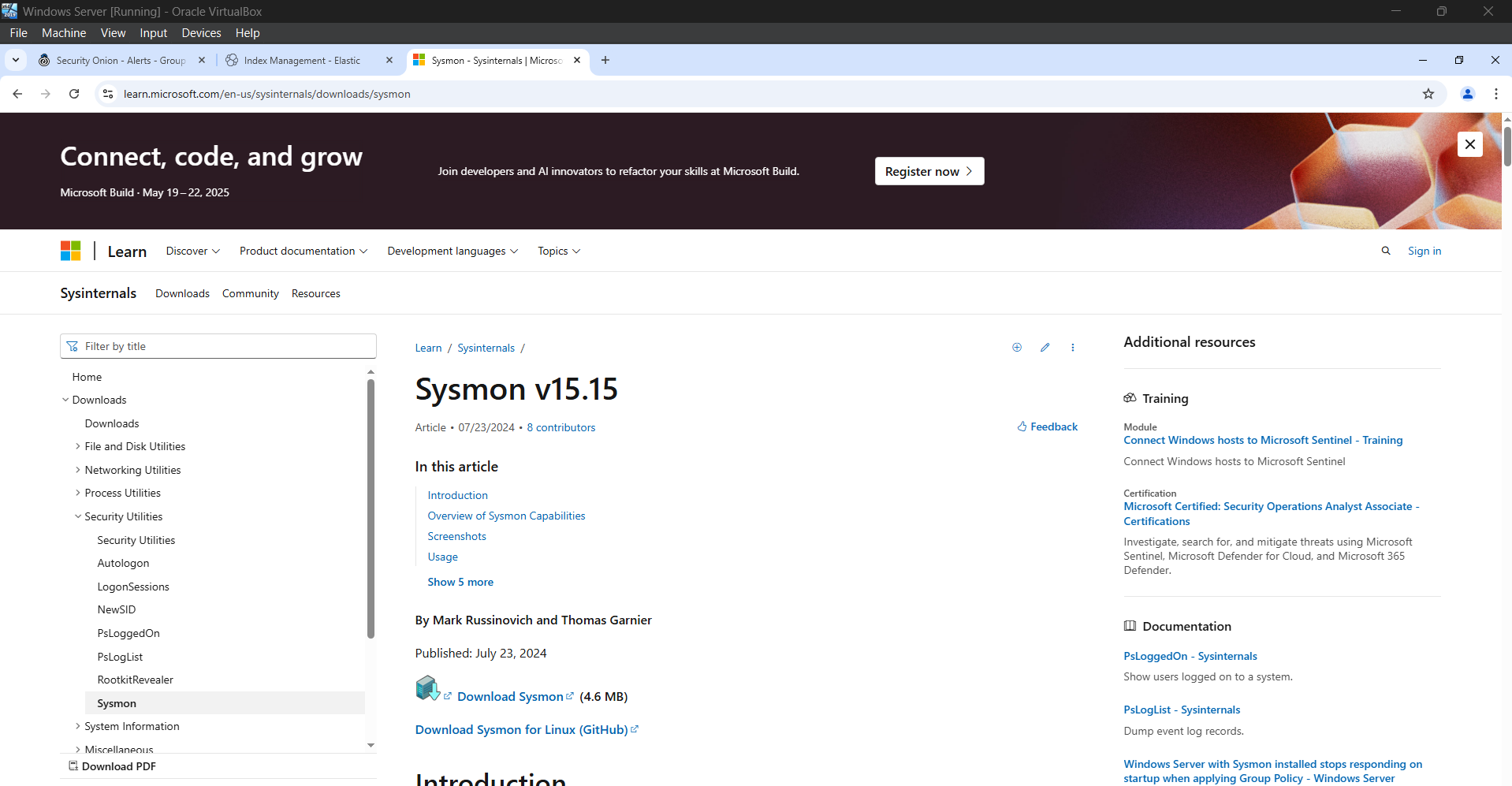
The purpose of this lab was to enhance Security Onion's event collection by integrating Sysmon-generated logs from a Windows endpoint. This was achieved by installing Sysmon, configuring it with a community-driven XML template, and ensuring logs were forwarded by the Wazuh agent to the Security Onion ELK stack. The lab also explored how to add other log sources such as FactoryTalk Diagnostics.

Step-by-Step Execution Summary

#### 1. ****Downloaded Sysmon from Microsoft Sysinternals****

Accessed: <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

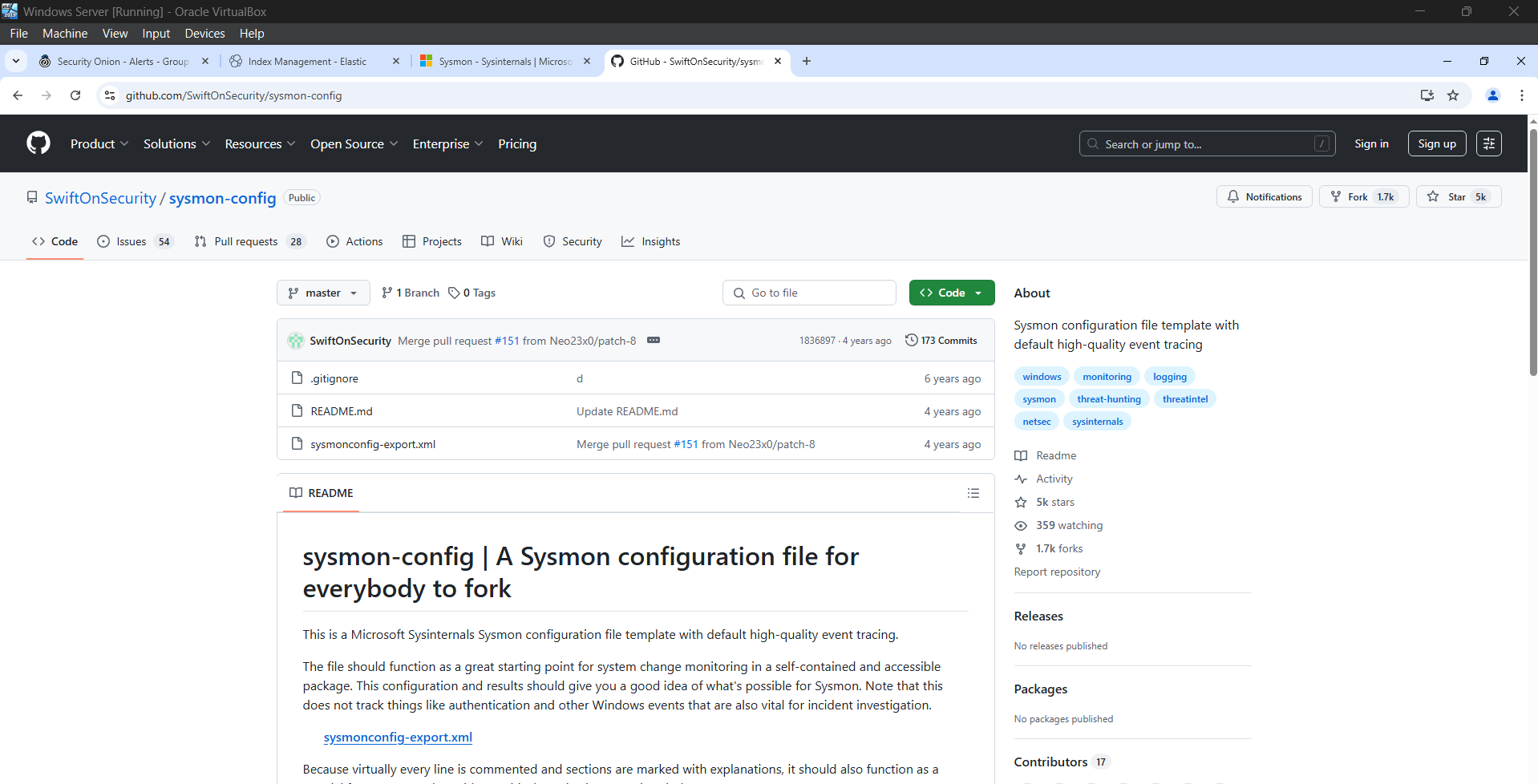
Extracted the ZIP which contains binaries for both x86 and x64 platforms.



2. **Downloaded Sysmon Configuration File**

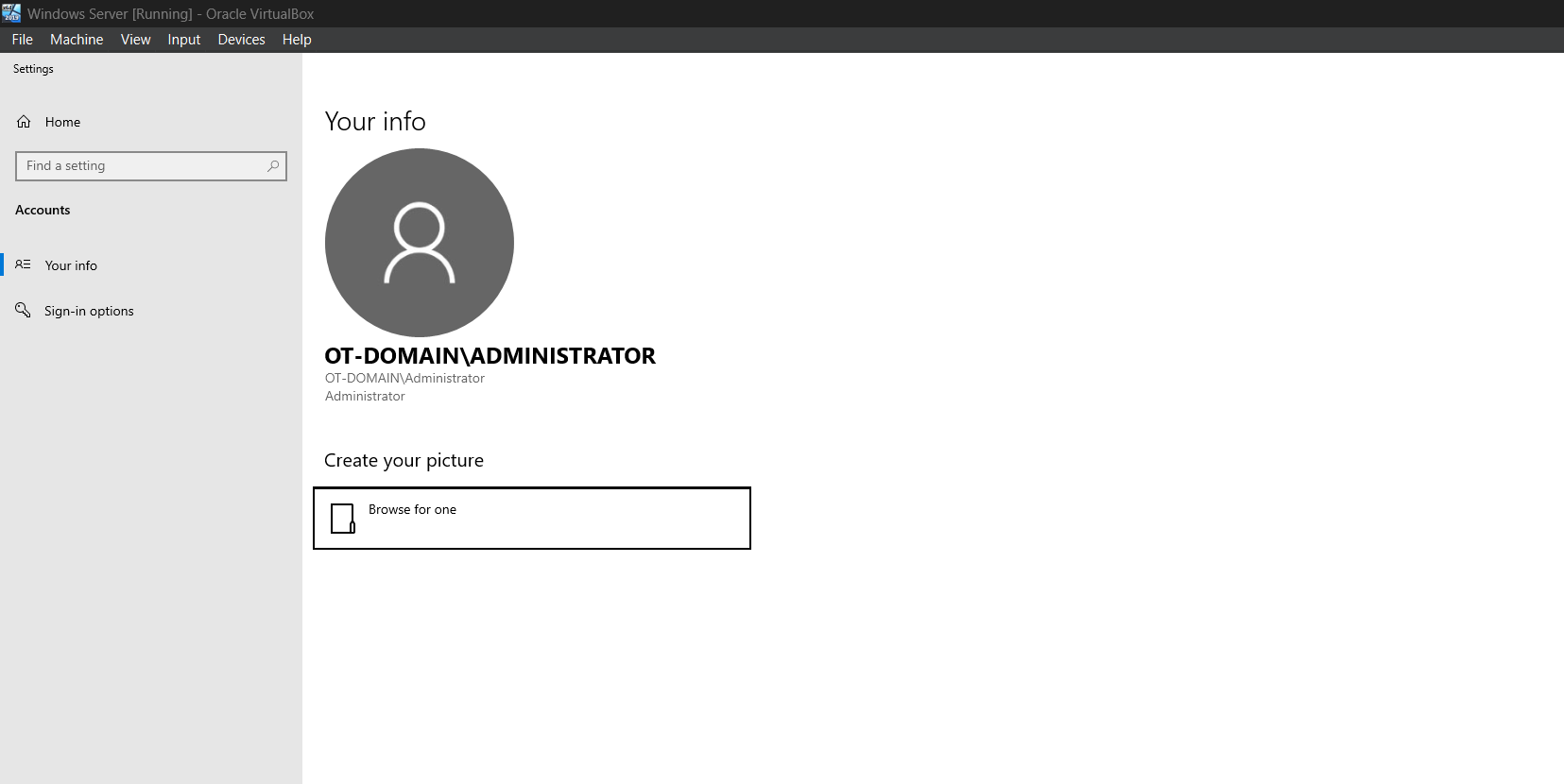
Config file source: [sysmonconfig-export.xml](https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml)

The configuration is designed for high compatibility with SIEM platforms.



3. **Logged into Windows Endpoint (OT-DC1)**

Selected OT-DC1 as the initial system for Sysmon installation.



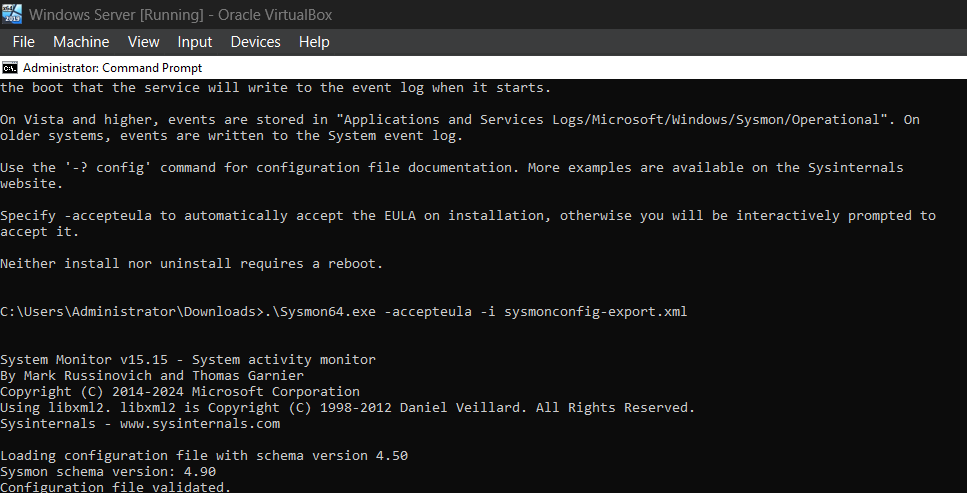
4. **Installed Sysmon Using Configuration File**

Opened PowerShell as Administrator.

Ran the following command:

sysmon.exe -accepteula -i sysmonconfig-export.xml

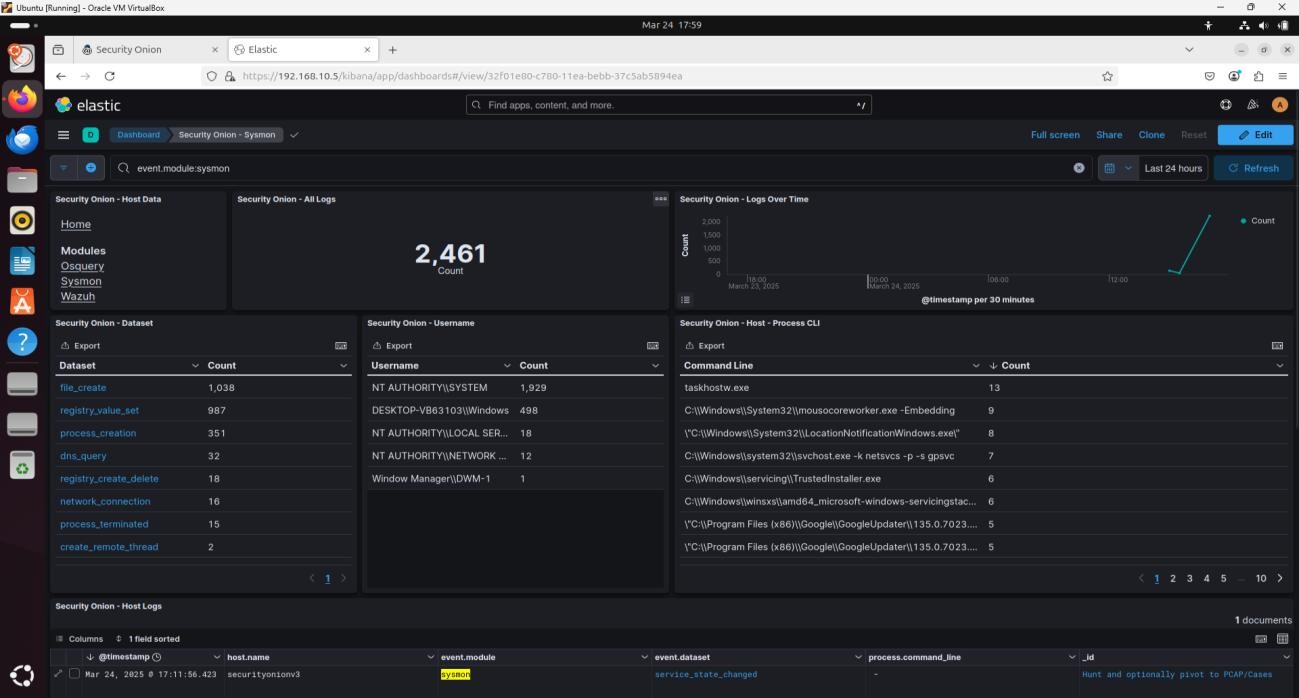
Confirmed Sysmon service was successfully installed and started.



5. **Validated Sysmon Logs via Kibana in Security Onion**

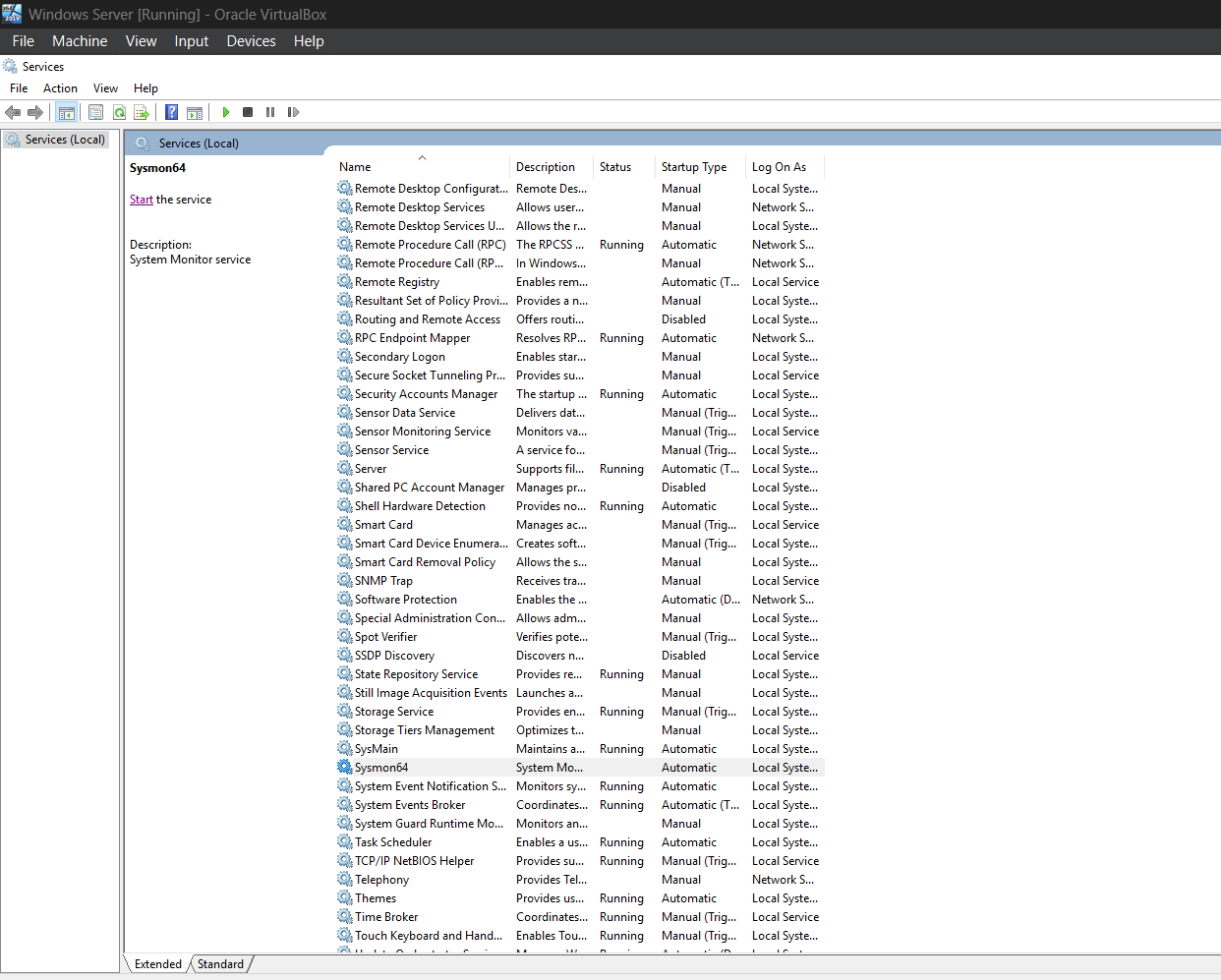
Navigated to: Home > Host > Sysmon dashboard

Verified logs for PowerShell startup event.



6. **Located Sysmon Logs in Windows Event Viewer**

Path: Applications and Services Logs > Microsoft > Windows > Sysmon > Operational

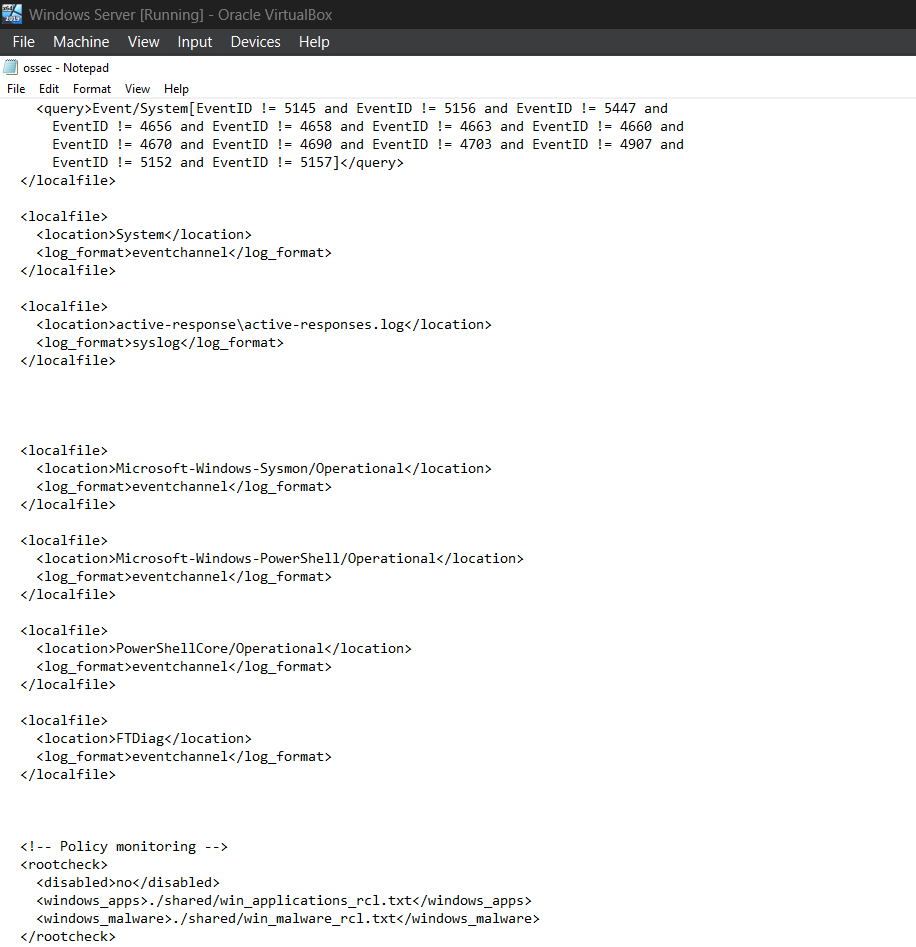


7. **Added FactoryTalk Diagnostics to Wazuh Configuration**

Identified log path: Applications and Services Logs > FactoryTalk Diagnostics

Right-clicked the log > Properties > Copied log name: FTDiag

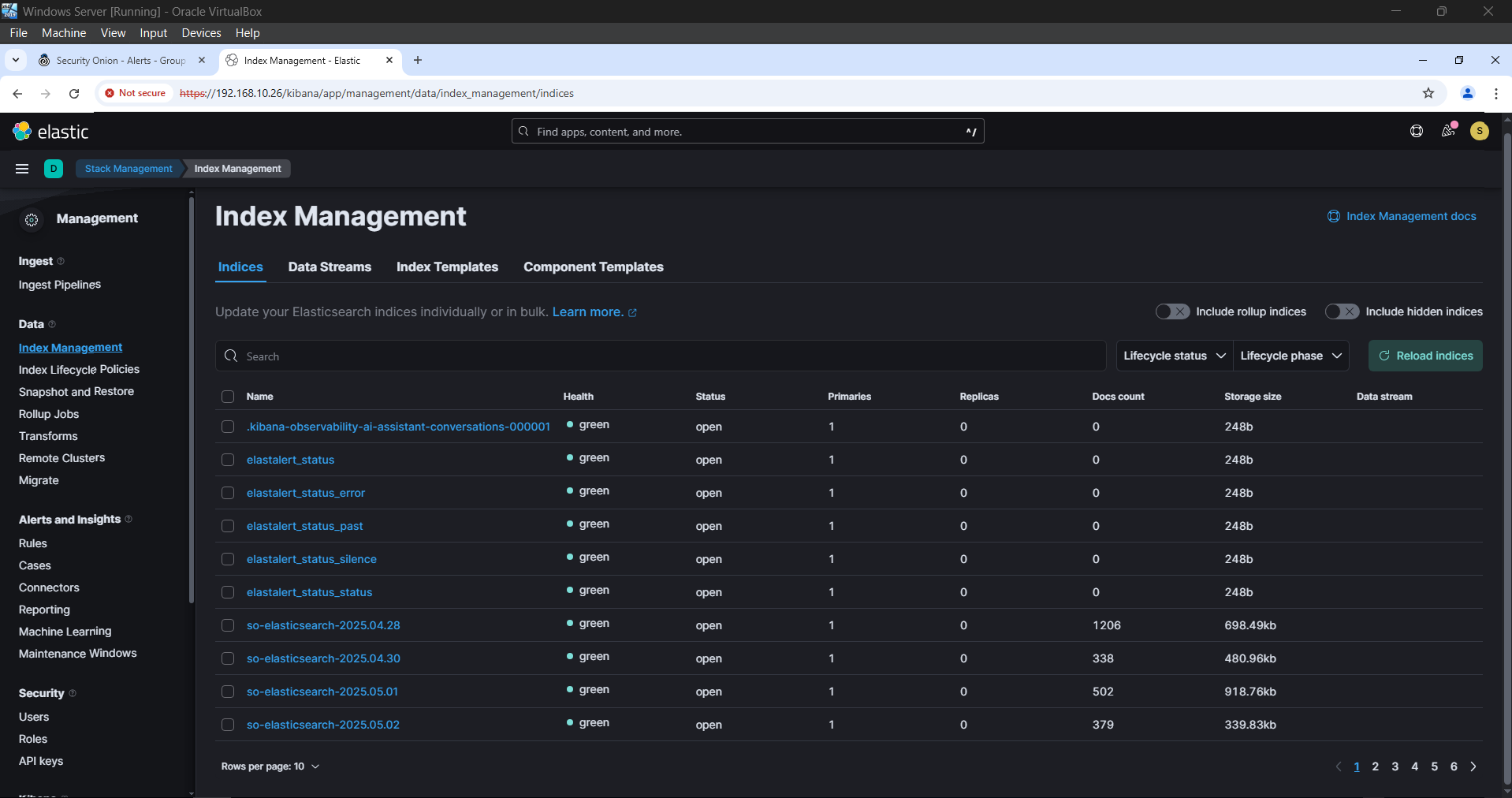
Edited Wazuh agent config to include this custom path.



8. **Refreshed Index Patterns in Elasticsearch via Kibana**

Path: Kibana > Menu > Stack Management > Index Patterns > \*:so-\*

Clicked **Refresh** and confirmed update.



**Conclusion**

This lab demonstrated how integrating Sysmon with Wazuh and Security Onion expands visibility across endpoints. By forwarding enriched logs to Elasticsearch, we now have the capability to investigate detailed process-level behavior and ICS application events. This integration improves threat detection, especially in operational technology environments.

The next section in the course will build upon this by enhancing PowerShell visibility in Security Onion.