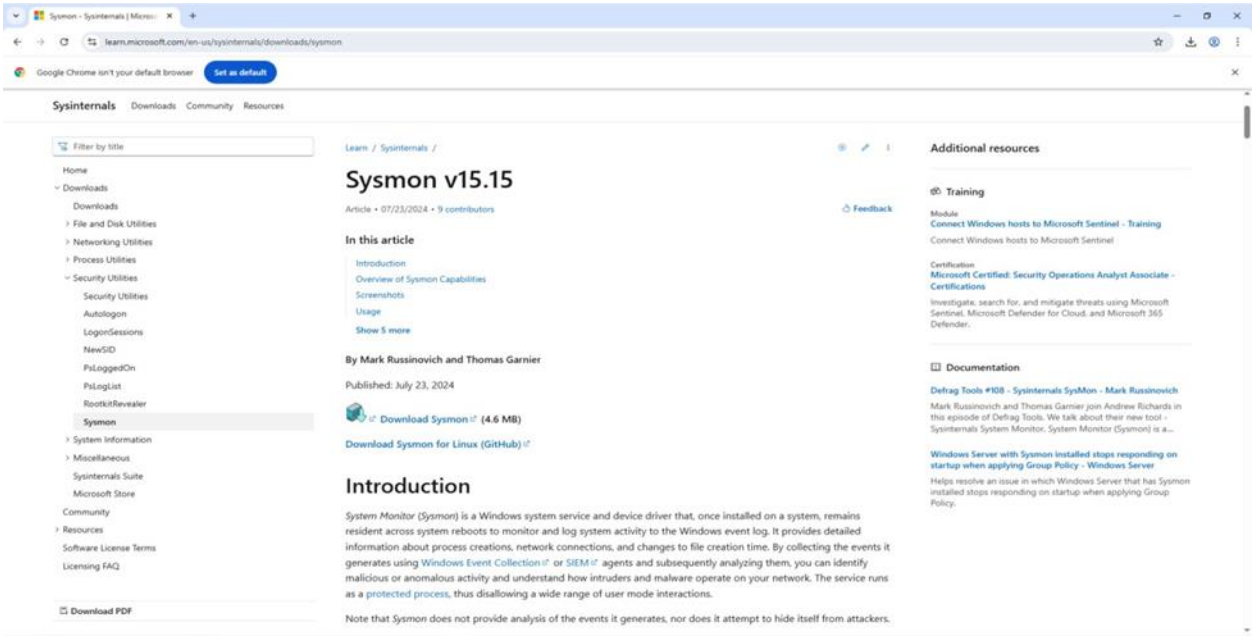
LAB Report 6 – using Wazuh to add Sysmon logging

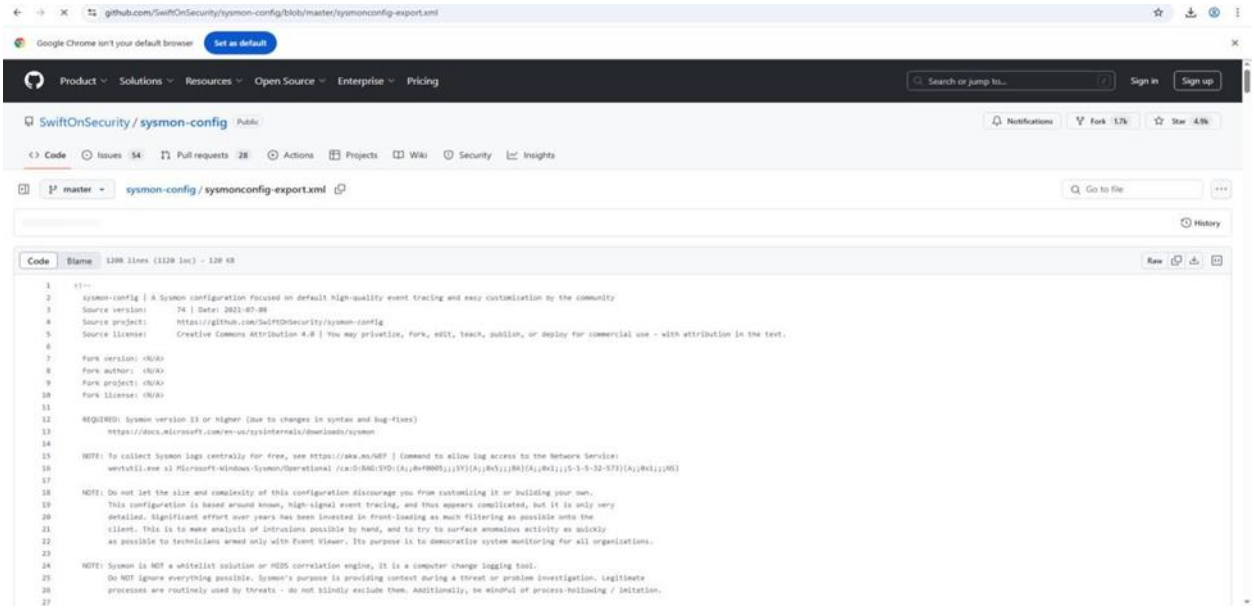
Name: Phanindhar Reddy Karnati
ID: 001667635

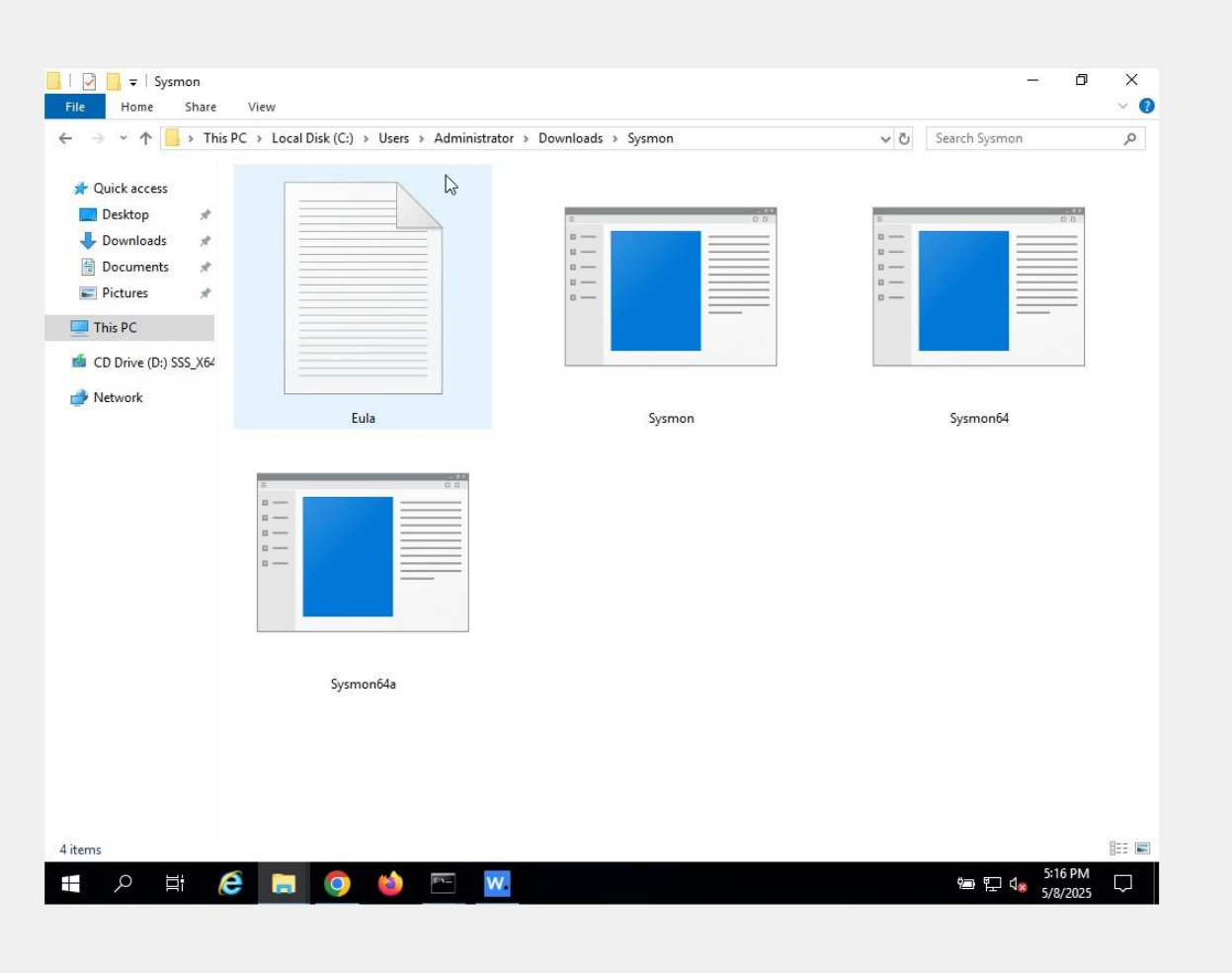
Date Submitted: 05/09/2025

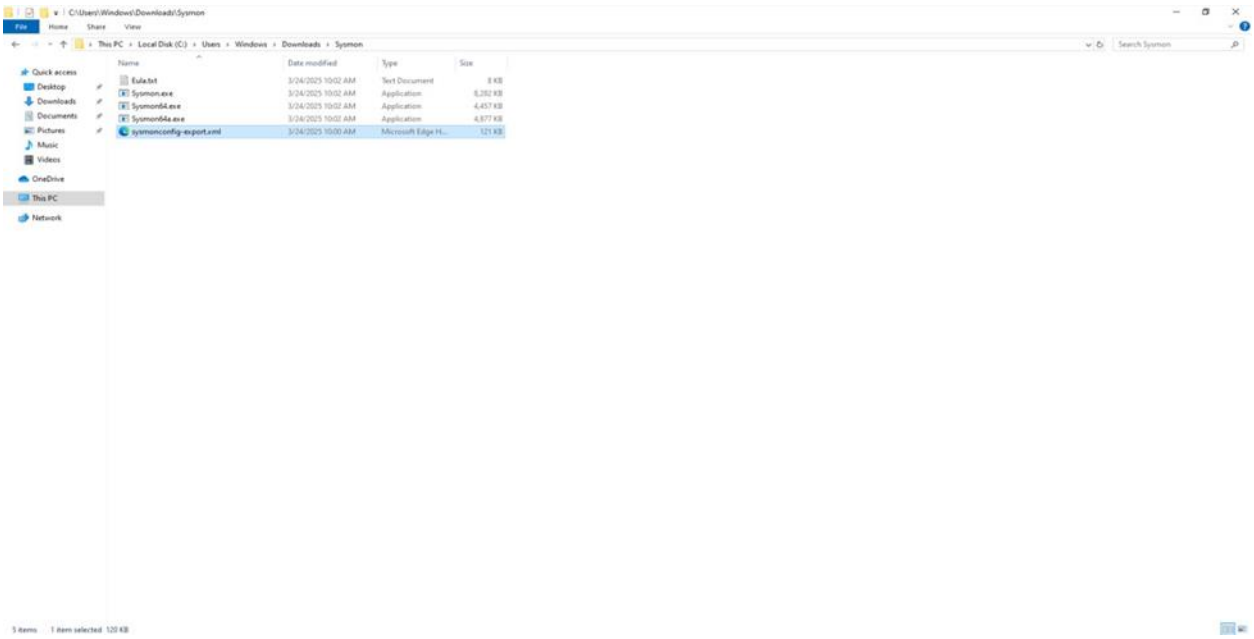
- I set up Sysmon on a Windows-based endpoint and set it up to collaborate with Wazuh for sophisticated event log forwarding in order to improve the monitoring capabilities of our Security Onion setup. A component of Microsoft Sysinternals, Sysmon (System Monitor) enables us to gather comprehensive data on system events like file modifications, network connections, and process creation. The objective was to use Wazuh's Sysmon integration to enhance the event data gathered in Security Onion.



I began by downloading the latest version of Sysmon from Microsoft's official Sysinternals site. The package came in a ZIP format containing executables for both 32-bit and 64-bit Windows systems. Alongside this, I also downloaded a pre-made configuration file (sysmonconfig-export.xml) from SwiftOnSecurity's GitHub repository, which includes rules optimized for compatibility with SIEM tools like the ELK stack used in Security Onion.



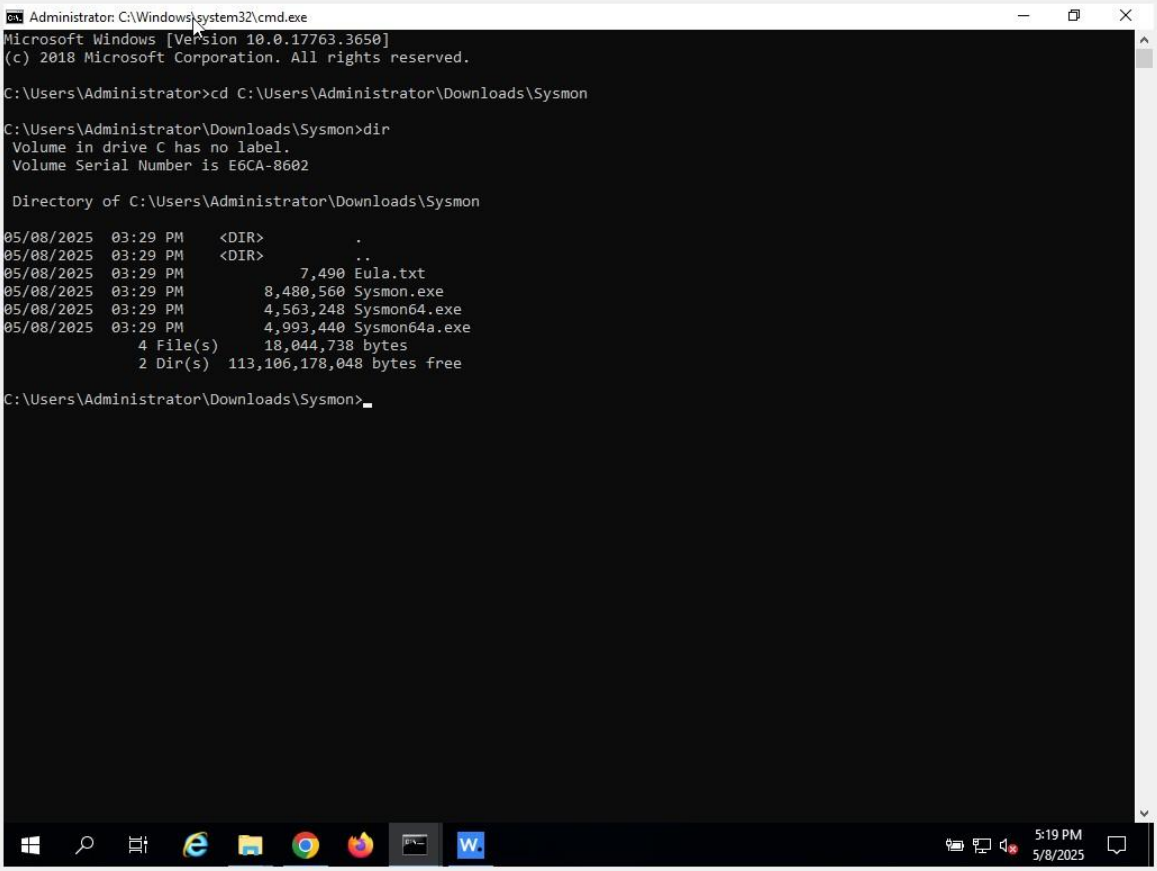

Sysmon
File
Home
Share
View
This PC › Local Disk (C:) › Users › Administrator › Downloads › Sysmon
Search Sysmon
Quick access
Desktop
Downloads
Documents
Pictures
This PC
CD Drive (D:) SSS_X64
Network
Eula
Sysmon
Sysmon64
Sysmon64a
4 items
5:16 PM
5/8/2025


C:\Users\Windows\Downloads\Sysmon
File
Home
Share
View
This PC › Local Disk (C:) › Users › Windows › Downloads › Sysmon
Search Sysmon
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Eula.txt
3/24/2025 10:02 AM
Text Document
8 KB
Sysmon.exe
3/24/2025 10:02 AM
Application
8,282 KB
Sysmon64.exe
3/24/2025 10:02 AM
Application
4,457 KB
Sysmon64a.exe
3/24/2025 10:02 AM
Application
4,977 KB
sysmonconfig-export.xml
3/24/2025 10:00 AM
Microsoft Edge H...
121 KB
5 items
1 item selected 120 KB


Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\Users\Windows\Downloads\Sysmon
C:\Users\Windows\Downloads\Sysmon>

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Windows\Downloads\Sysmon

C:\Users\Windows\Downloads\Sysmon>.\Sysmon64.exe -accepteula -i sysmonconfig-export.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Users\Windows\Downloads\Sysmon>
```



After copying both files to the Windows endpoint (in this case, **OT-DC1**), I launched a PowerShell terminal with administrator privileges. I navigated to the folder containing the Sysmon executable and configuration file, and then executed the installation command. This setup immediately activated the Sysmon driver, which began capturing events and logging them under the "Microsoft-Windows-Sysmon/Operational" log channel.

Administrator: C:\Windows\system32\cmd.exe

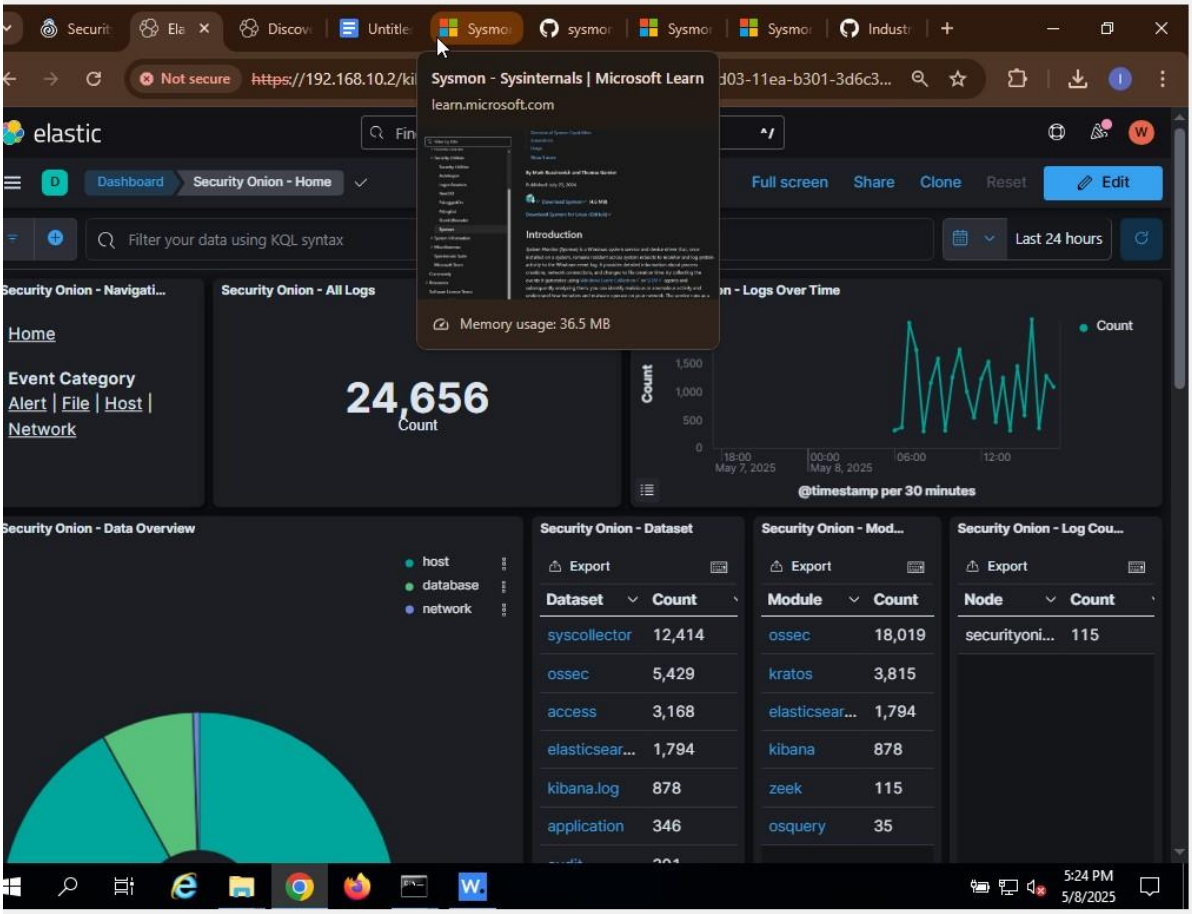
```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Users\Administrator\Downloads\Sysmon

C:\Users\Administrator\Downloads\Sysmon>dir
 Volume in drive C has no label.
 Volume Serial Number is E6CA-8602

 Directory of C:\Users\Administrator\Downloads\Sysmon

05/08/2025  03:29 PM    <DIR>          .
05/08/2025  03:29 PM    <DIR>          ..
05/08/2025  03:29 PM             7,490 Eula.txt
05/08/2025  03:29 PM         8,480,560 Sysmon.exe
05/08/2025  03:29 PM         4,563,248 Sysmon64.exe
05/08/2025  03:29 PM         4,993,440 Sysmon64a.exe
               4 File(s)     18,044,738 bytes
               2 Dir(s)  113,106,178,048 bytes free

C:\Users\Administrator\Downloads\Sysmon>dir
 Volume in drive C has no label.
 Volume Serial Number is E6CA-8602

 Directory of C:\Users\Administrator\Downloads\Sysmon

05/08/2025  05:20 PM    <DIR>          .
05/08/2025  05:20 PM    <DIR>          ..
05/08/2025  03:29 PM             7,490 Eula.txt
05/08/2025  03:29 PM         8,480,560 Sysmon.exe
05/08/2025  03:29 PM         4,563,248 Sysmon64.exe
05/08/2025  03:29 PM         4,993,440 Sysmon64a.exe
05/08/2025  03:30 PM           123,257 sysmonconfig-export.xml
               5 File(s)     18,167,995 bytes
               2 Dir(s)  113,106,071,552 bytes free

C:\Users\Administrator\Downloads\Sysmon>
```

5:20 PM
5/8/2025

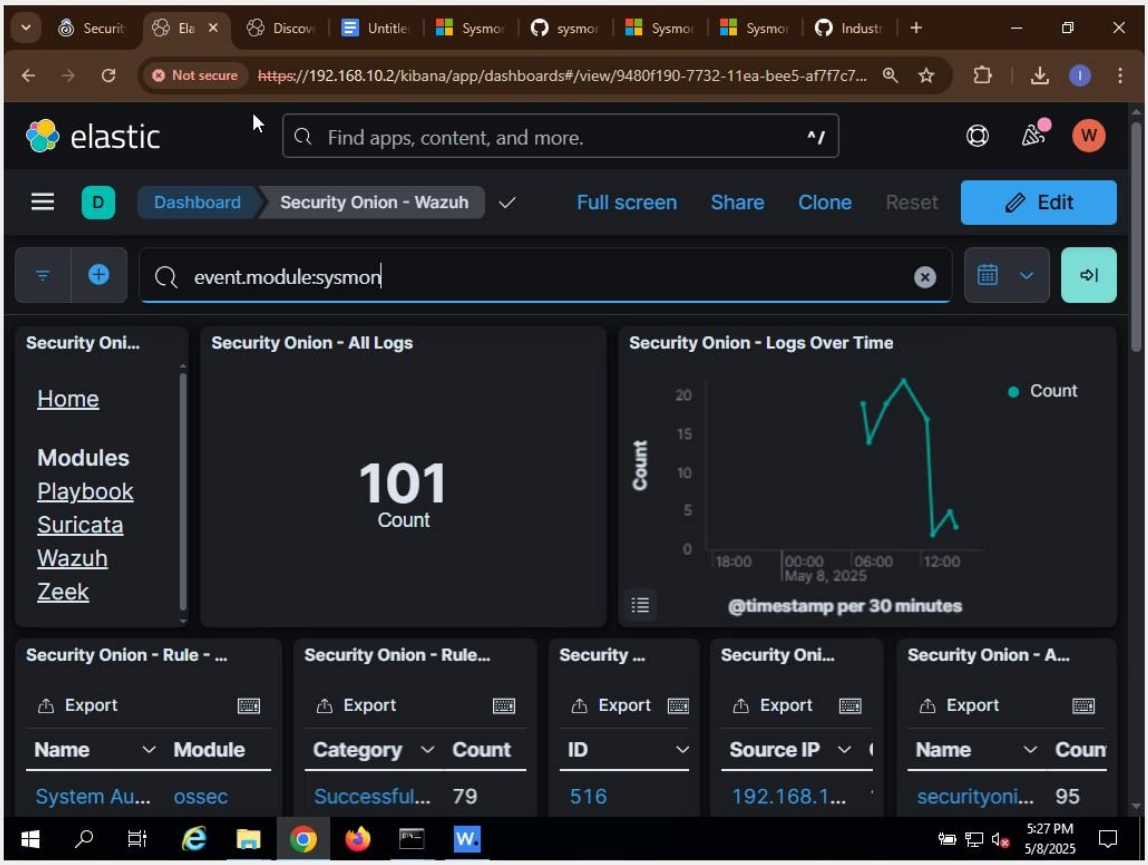
Administrator: C:\Windows\system32\cmd.exe

```
05/08/2025  03:29 PM    <DIR>          ..
05/08/2025  03:29 PM             7,490 Eula.txt
05/08/2025  03:29 PM         8,480,560 Sysmon.exe
05/08/2025  03:29 PM         4,563,248 Sysmon64.exe
05/08/2025  03:29 PM         4,993,440 Sysmon64a.exe
               4 File(s)     18,044,738 bytes
               2 Dir(s)  113,106,178,048 bytes free

C:\Users\Administrator\Downloads\Sysmon>dir
 Volume in drive C has no label.
 Volume Serial Number is E6CA-8602

 Directory of C:\Users\Administrator\Downloads\Sysmon

05/08/2025  05:20 PM    <DIR>          .
05/08/2025  05:20 PM    <DIR>          ..
05/08/2025  03:29 PM             7,490 Eula.txt
05/08/2025  03:29 PM         8,480,560 Sysmon.exe
05/08/2025  03:29 PM         4,563,248 Sysmon64.exe
05/08/2025  03:29 PM         4,993,440 Sysmon64a.exe
05/08/2025  03:30 PM           123,257 sysmonconfig-export.xml
               5 File(s)     18,167,995 bytes
               2 Dir(s)  113,106,071,552 bytes free

C:\Users\Administrator\Downloads\Sysmon>.\Sysmon64.exe -accepteula -i sysmonconfig-export.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Users\Administrator\Downloads\Sysmon>
```

5:21 PM
5/8/2025

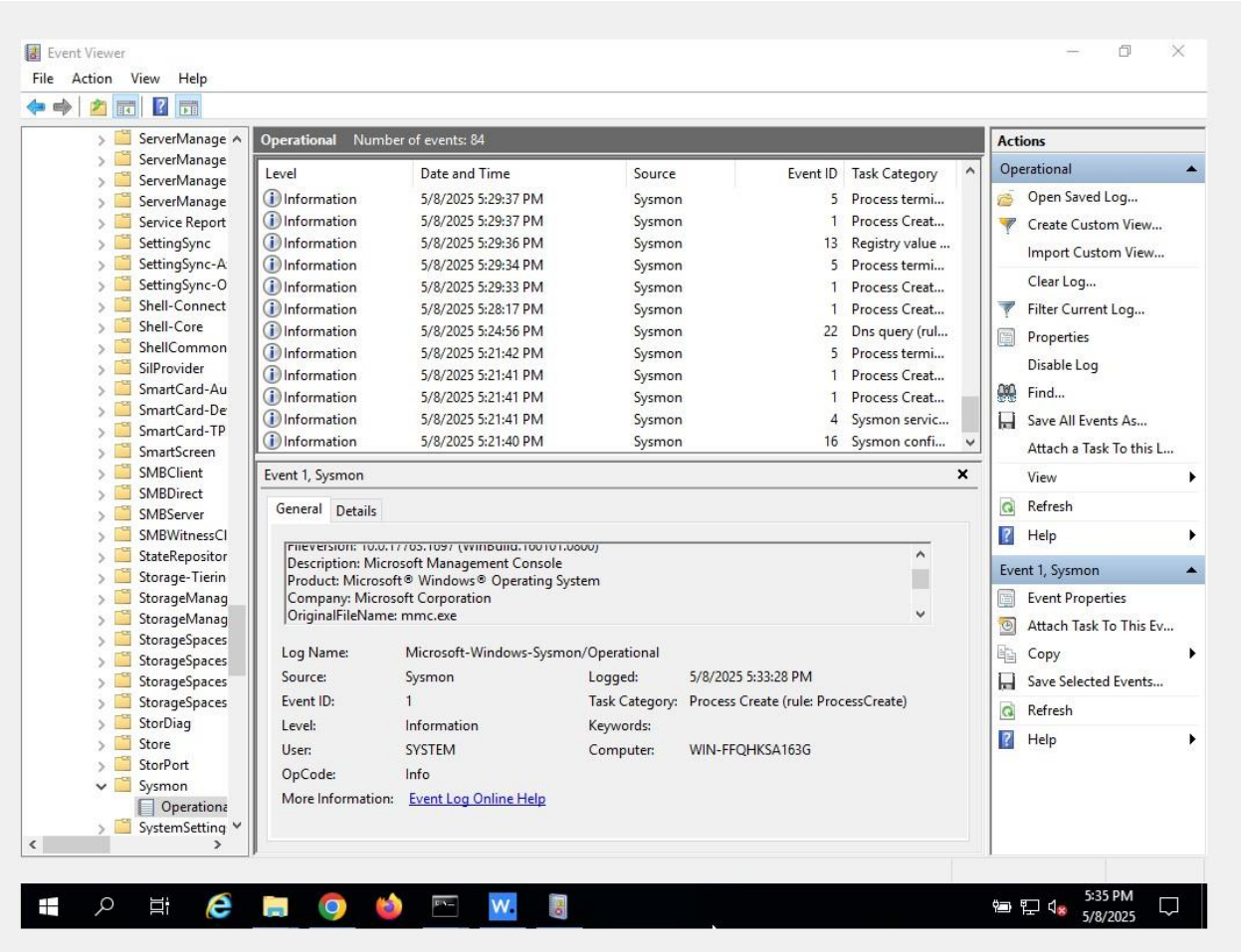


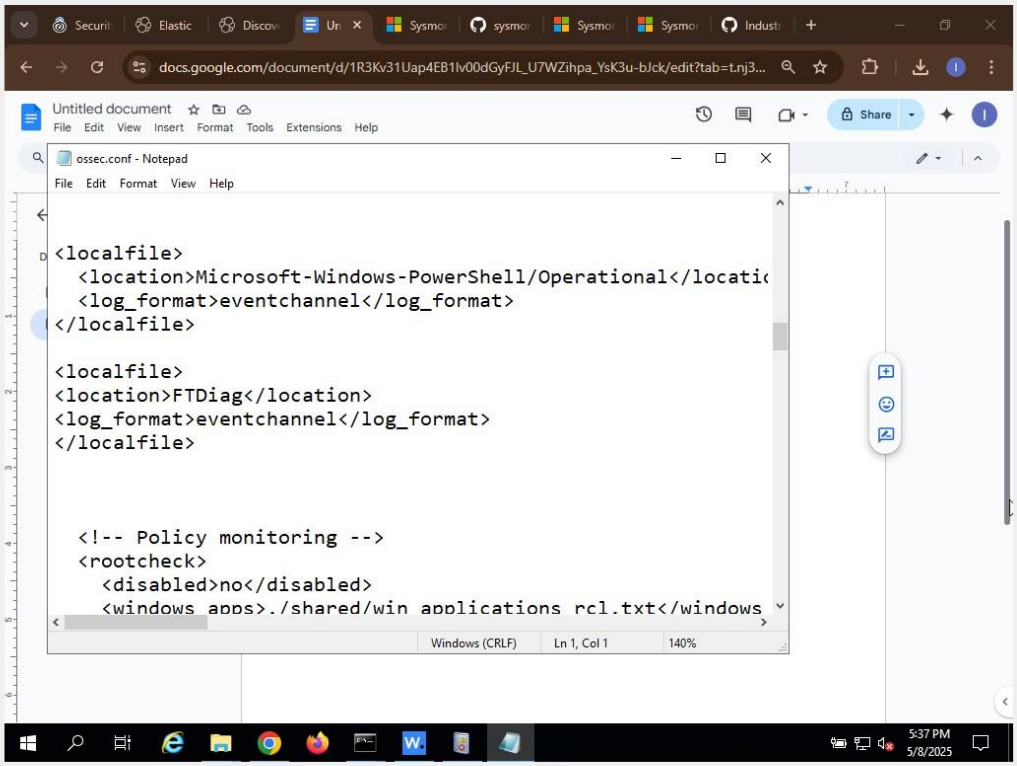
Once Sysmon was active, Wazuh — already installed and running on the endpoint — started monitoring the Sysmon logs. These entries were forwarded to Security Onion, where they became part of the Elasticsearch database.



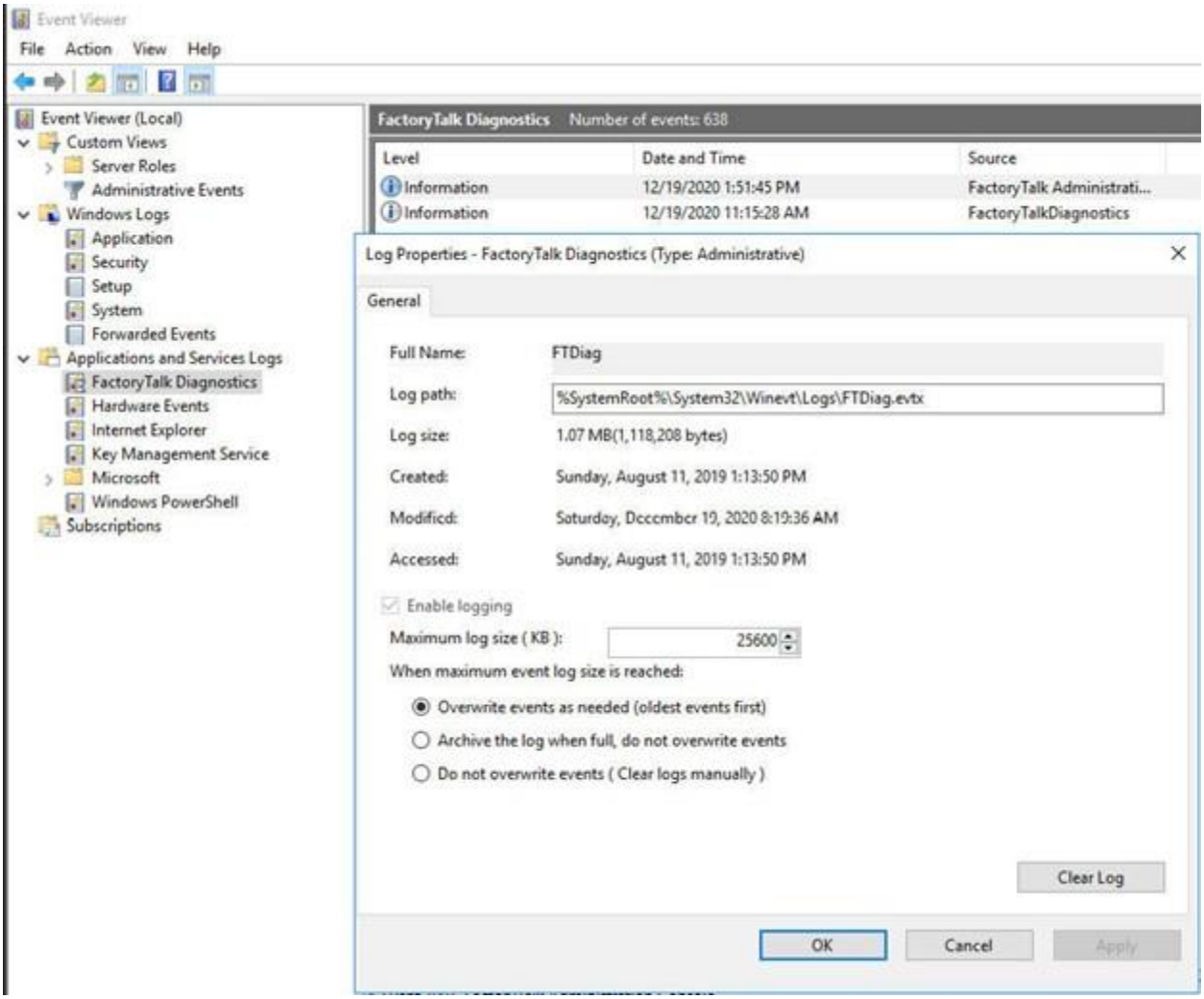
I verified this integration by accessing the Security Onion web portal, opening Kibana, and navigating to the “Sysmon” dashboard under the “Home” → “Host” section. There, I observed detailed logs such as PowerShell executions, including metadata like usernames, parent processes, file paths, command-line arguments, and process hashes.

process.command_line	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"
process.entity_id	{17B2E20D-F27D-5FF0-F300-000000003300}
process.executable	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
process.parent.command_line	C:\\Windows\\System32\\RuntimeBroker.exe -Embedding
process.parent.entity_id	{17B2E20D-D79E-5FF0-AC00-000000003300}
process.parent.executable	C:\\Windows\\System32\\RuntimeBroker.exe
process.pe.company	Microsoft Corporation
process.pe.description	Windows PowerShell
process.pe.file_version	10.0.14393.206 (rs1_release.160915-0644)
process.pe.original_file_name	PowerShell.EXE
process.pe.product	Microsoft® Windows® Operating System
process.ppid	4940
process.working_directory	C:\\Users\\Administrator\\
user.name	OT-DOMAIN\\Administrator
winlog.channel	Microsoft-Windows-Sysmon/Operational
winlog.computer	OT-DC1.OT-Domain.local
winlog.eventRecordID	2996
winlog.event_data.hashes	MD5=097CE5761C89434367598B34FE32893B,SHA256=BA4038FD20E474C047BE8AAD
winlog.event_data.integrityLevel	High
winlog.event_data.logonGuid	{17B2E20D-D79C-5FF0-BA3B-2D0000000000}
winlog.event_data.logonId	0x2d3bba
winlog.event_data.processId	1828

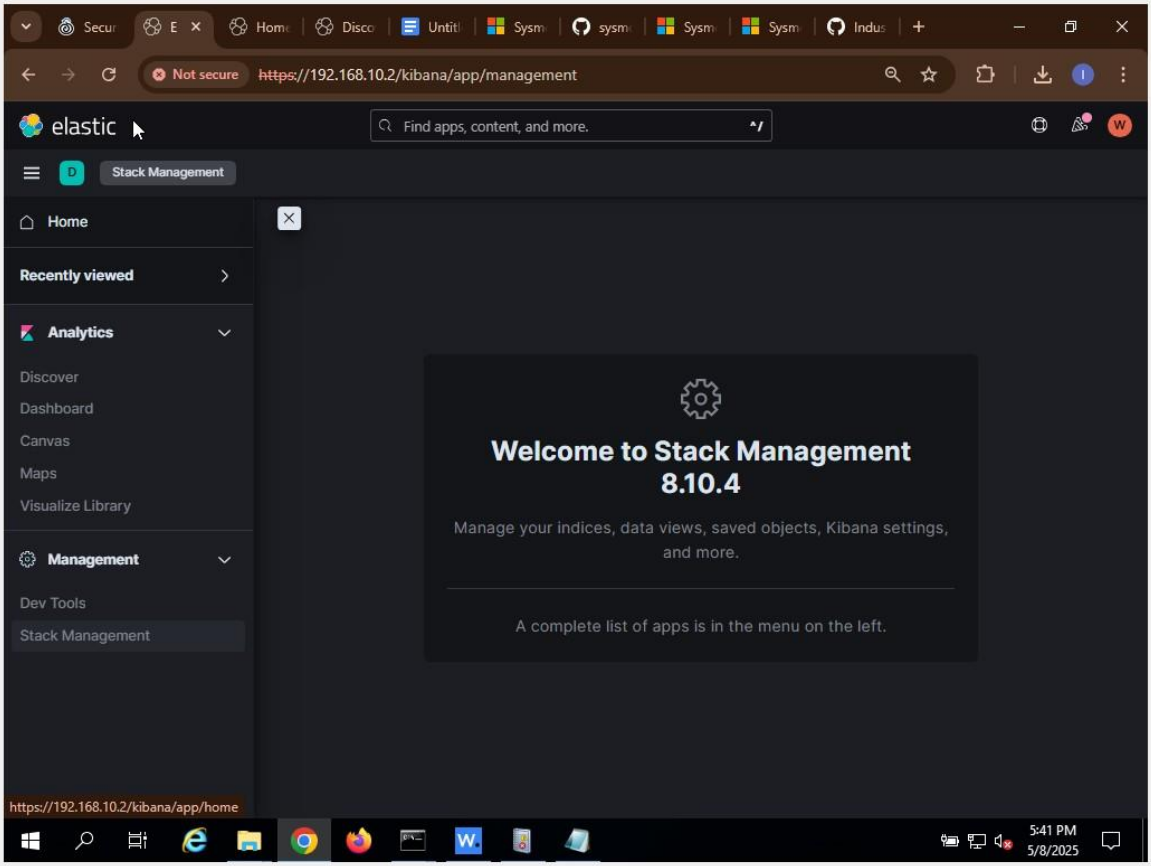

Event Viewer
File Action View Help
Operational Number of events: 84
Level Date and Time Source Event ID Task Category
Information 5/8/2025 5:29:37 PM Sysmon 5 Process termi...
Information 5/8/2025 5:29:37 PM Sysmon 1 Process Creat...
Information 5/8/2025 5:29:36 PM Sysmon 13 Registry value ...
Information 5/8/2025 5:29:34 PM Sysmon 5 Process termi...
Information 5/8/2025 5:29:33 PM Sysmon 1 Process Creat...
Information 5/8/2025 5:28:17 PM Sysmon 1 Process Creat...
Information 5/8/2025 5:24:56 PM Sysmon 22 Dns query (rul...
Information 5/8/2025 5:21:42 PM Sysmon 5 Process termi...
Information 5/8/2025 5:21:41 PM Sysmon 1 Process Creat...
Information 5/8/2025 5:21:41 PM Sysmon 1 Process Creat...
Information 5/8/2025 5:21:41 PM Sysmon 4 Sysmon servic...
Information 5/8/2025 5:21:40 PM Sysmon 16 Sysmon confi...
Event 1, Sysmon
General Details
Description: Microsoft Management Console
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: mmc.exe
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 5/8/2025 5:33:28 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: WIN-FFQHKSA163G
OpCode: Info
More Information: Event Log Online Help
Actions
Operational
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Disable Log
Find...
Save All Events As...
Attach a Task To this L...
View
Refresh
Help
Event 1, Sysmon
Event Properties
Attach Task To This Ev...
Copy
Save Selected Events...
Refresh
Help
5:35 PM
5/8/2025

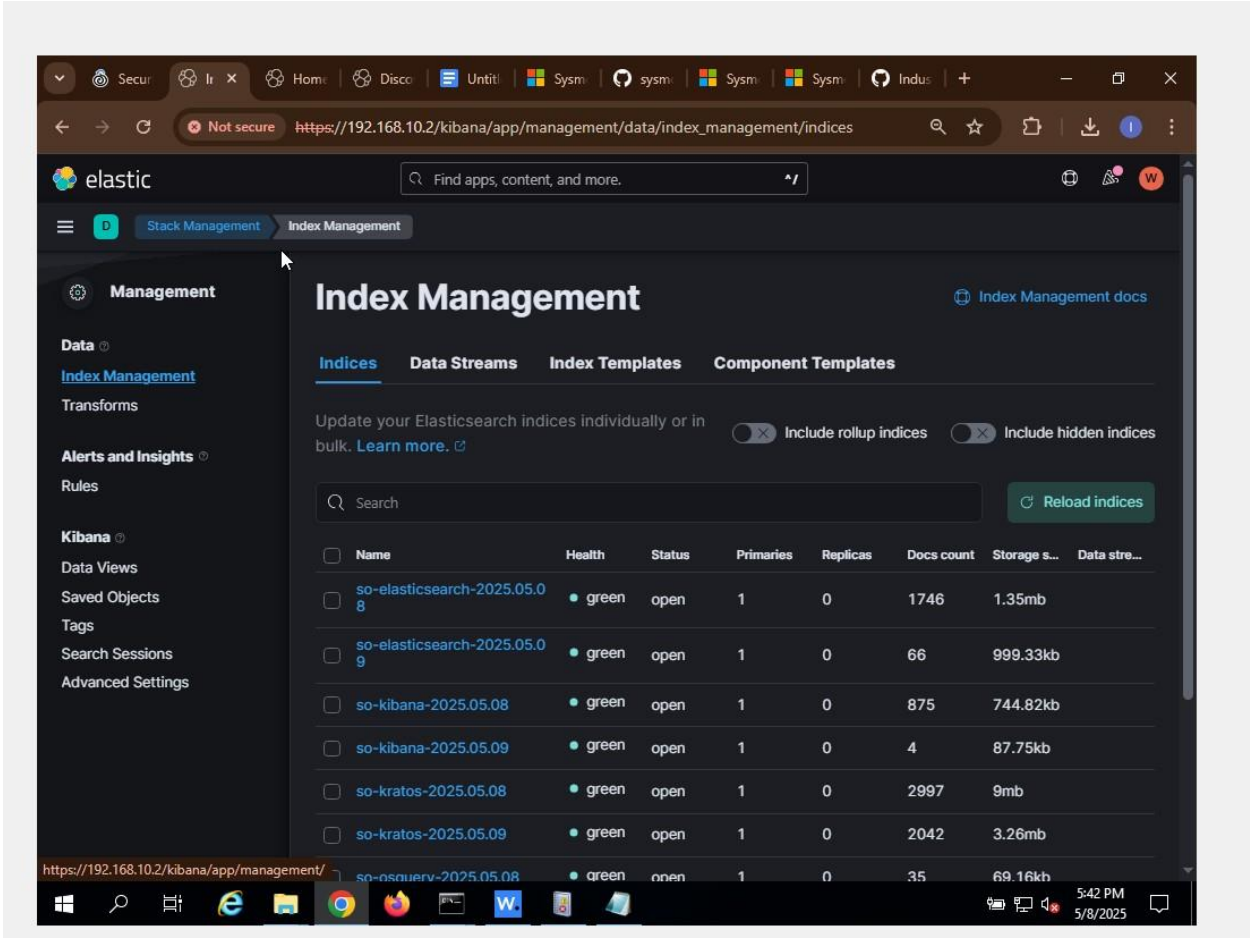


I verified this integration by accessing the Security Onion web portal, opening Kibana, and navigating to the “Sysmon” dashboard under the “Home” → “Host” section.

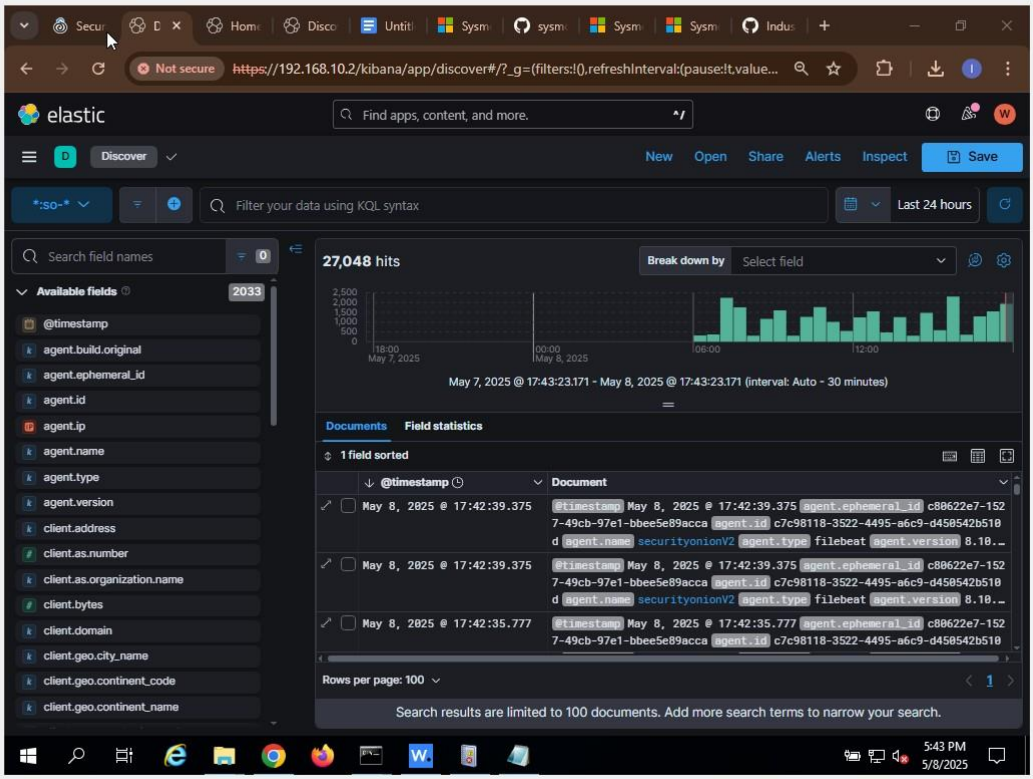


There, I observed detailed logs such as PowerShell executions, including metadata like usernames, parent processes, file paths, command-line arguments, and process hashes.

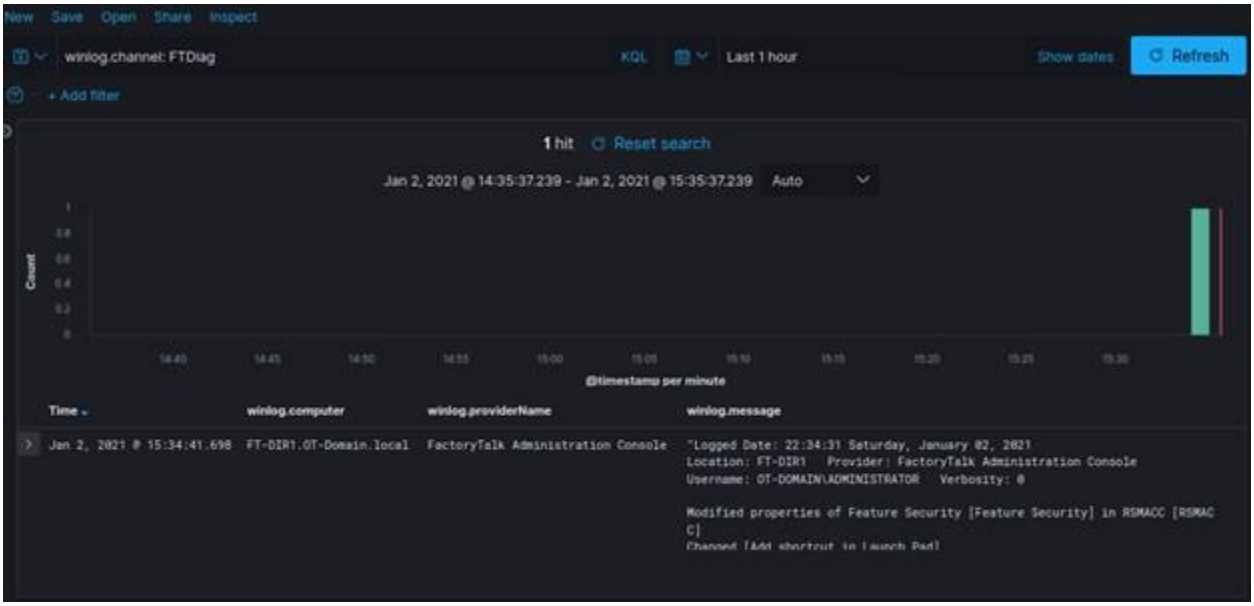

Not secure
https://192.168.10.2/kibana/app/management
elastic
Find apps, content, and more.
Stack Management
Home
Recently viewed
Analytics
Discover
Dashboard
Canvas
Maps
Visualize Library
Management
Dev Tools
Stack Management
Welcome to Stack Management 8.10.4
Manage your indices, data views, saved objects, Kibana settings, and more.
A complete list of apps is in the menu on the left.
https://192.168.10.2/kibana/app/home
5:41 PM
5/8/2025



I then extended the functionality by adding another Windows event log to Wazuh's configuration. I focused on the FactoryTalk Diagnostics log, commonly used in Rockwell Automation environments..



Using the Windows Event Viewer, I located the full name of the log (FTDiag), and updated the Wazuh agent's configuration file to include it. After restarting the agent, this log was also collected and sent to Security Onion



Through this lab, I learned how to enrich host-based monitoring in a Security Onion deployment by integrating Sysmon and expanding Wazuh's event collection scope. These configurations allow us to detect and analyze a broader range of activities and potential threats within industrial control systems.

I have successfully completed the lab 6.