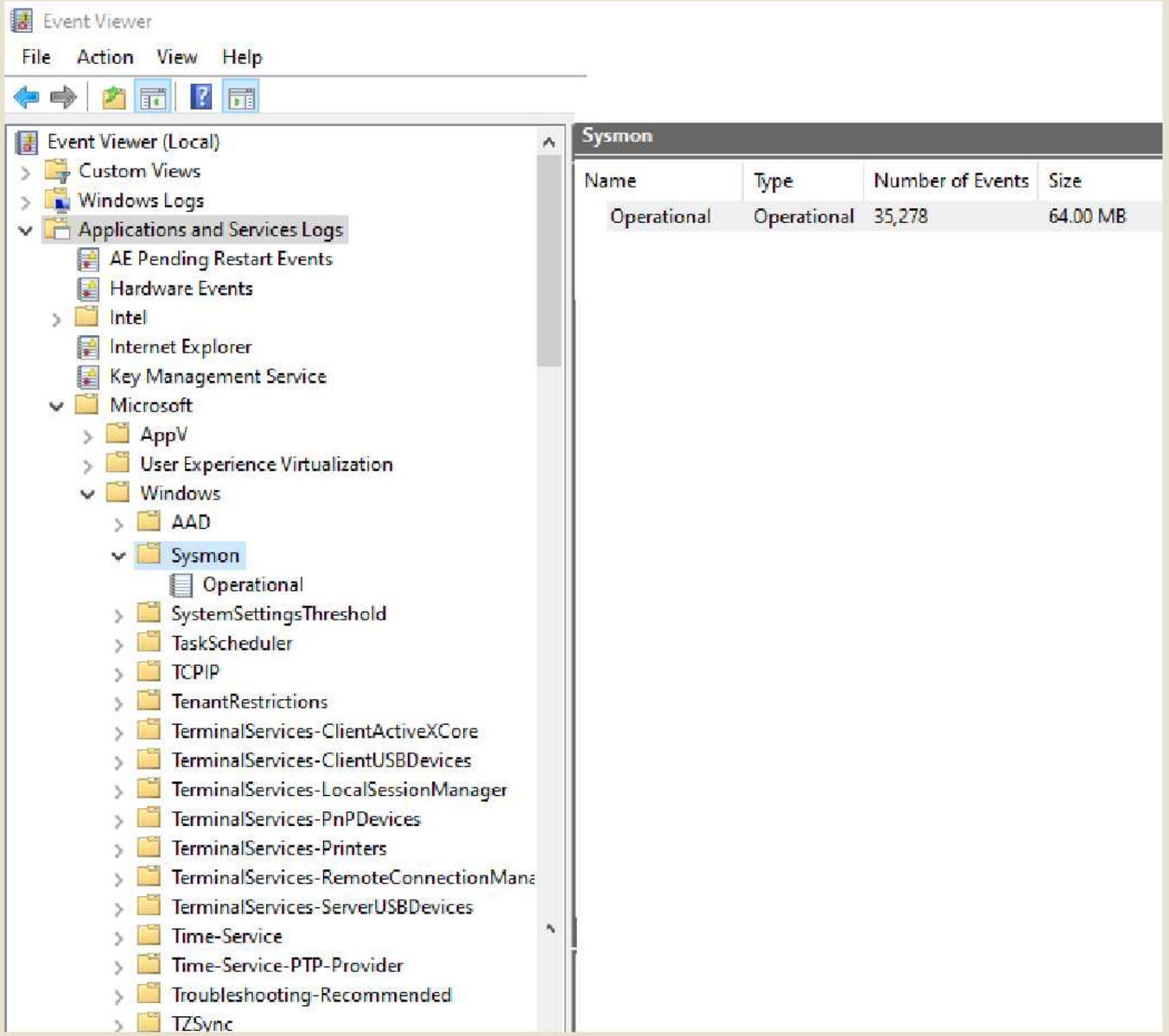
SYSMON NINJA TRAINING

It's time to prepare your company with ninja skills.

Axiom Tech



What is Sysmon?

- Part of Microsoft Sysinternals 2014 (Fee Tool)
- What is it?
  - 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
- Download Locations
  - Program It's time to prepare your company with ninja skills.
  - Configuration Files It's time to prepare your company with ninja skills.

Why Do We Use It?

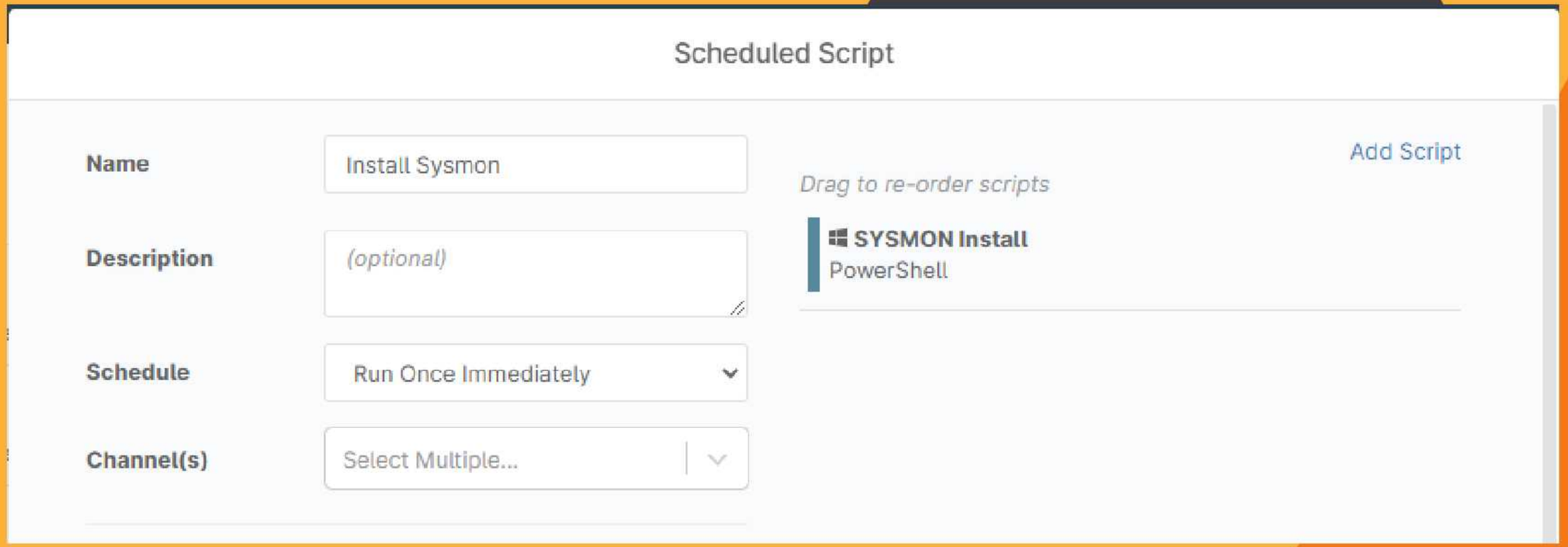
It provides insight not just for malware but much more. You will be surprised at what some of your programs are doing.

It is light weight and extremely customizable

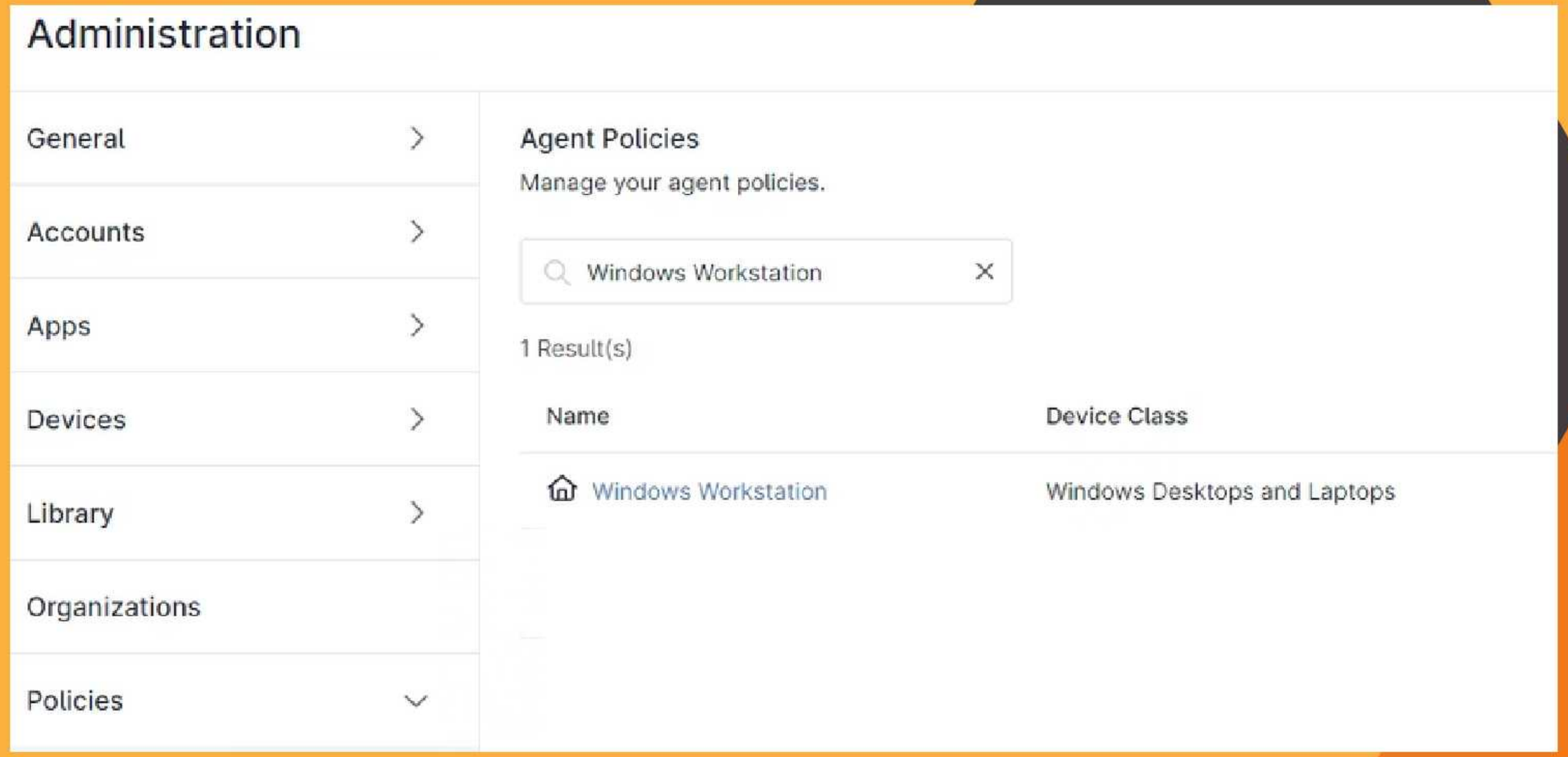
Based on DFIR reports Discovery Stage intelligence

We split our alerts into two boards Critical and Non-Critical

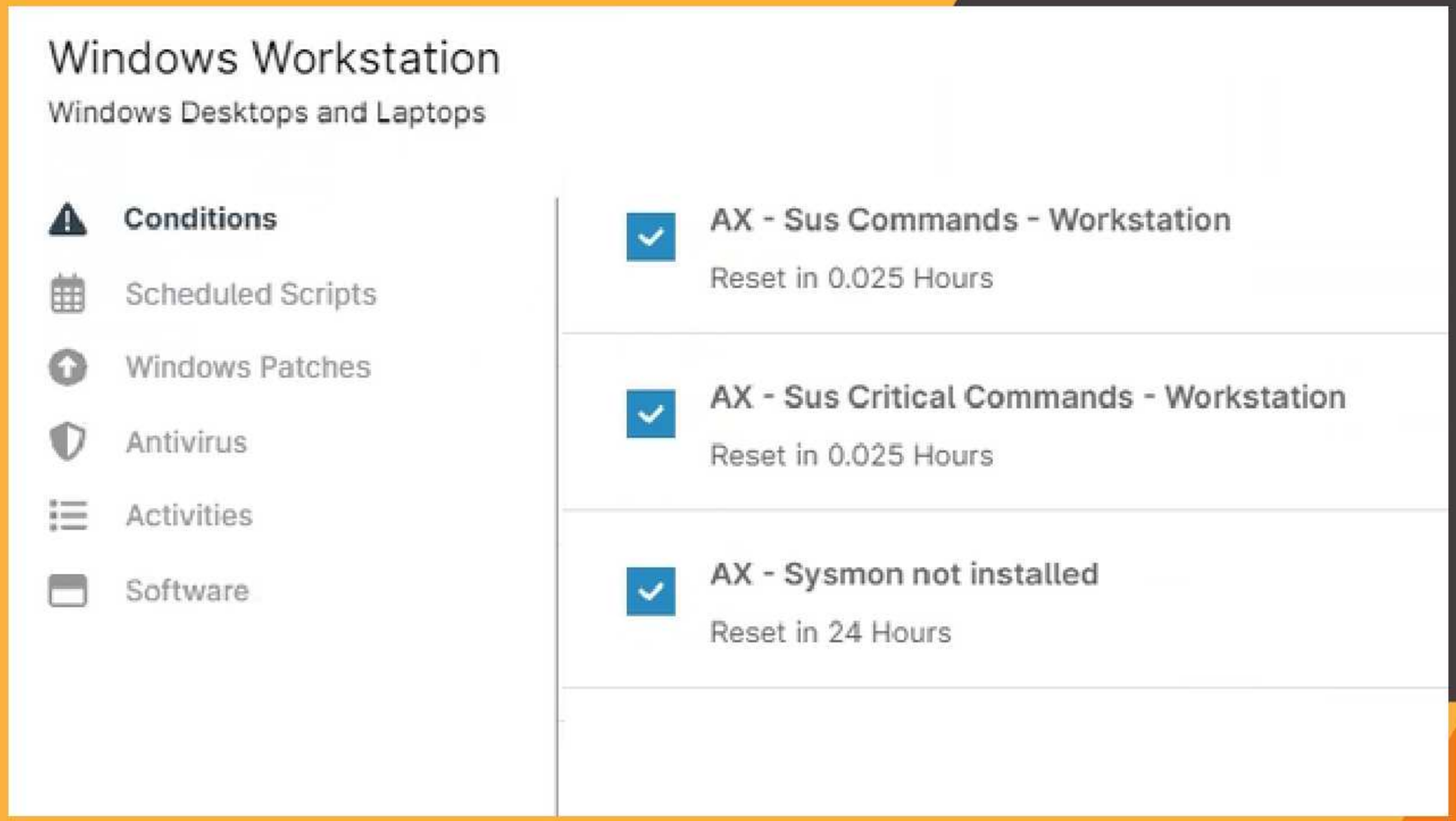
```powershell
<#
.SYNOPSIS
Install-Sysmon downloads the Sysmon executables archive and installs Sysmon64.exe
with a configuration file.
.DESCRIPTION
PowerShell script or module to install Sysmon with configuration
.PARAMETER path
The path to the working directory.  Default is user Documents.
.EXAMPLE
Install-Sysmon -path C:\Users\example\Desktop
#>

[CmdletBinding()]

#Establish parameters for path
param (
    [string]$path=[Environment]::GetFolderPath("Desktop")
)

#Test path and create it if required

If(!(test-path c:\windows\Sysmon))
{
  Write-Information -MessageData "Path does not exist.  Creating Path..." -InformationAction Continue;
  New-Item -ItemType Directory -Force -Path c:\windows\Sysmon | Out-Null;
  Write-Information -MessageData "...Complete" -InformationAction Continue
}


mkdir c:\windows\sysmon

Set-Location c:\windows\Sysmon



Write-Host "Location set c:\windows\Sysmon"

Write-Host "Retrieving Sysmon..."

Invoke-WebRequest -Uri https://download.sysinternals.com/files/Sysmon.zip -Outfile Sysmon.zip

Write-Host "Sysmon Retrived"

Write-Host "Unzip Sysmon..."

Expand-Archive Sysmon.zip

Set-Location c:\windows\Sysmon

Write-Host "Unzip Complete."

Write-Host "Retrieving Configuration File..."

Invoke-WebRequest -Uri https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml -Outfile sysmonconfig-export.xml

Write-Host "Configuration File Retrieved."

Write-Host "Installing Sysmon..."

c:\windows\Sysmon\sysmon\sysmon64.exe -accepteula -i sysmonconfig-export.xml

Write-Host "Sysmon Installed!"
```



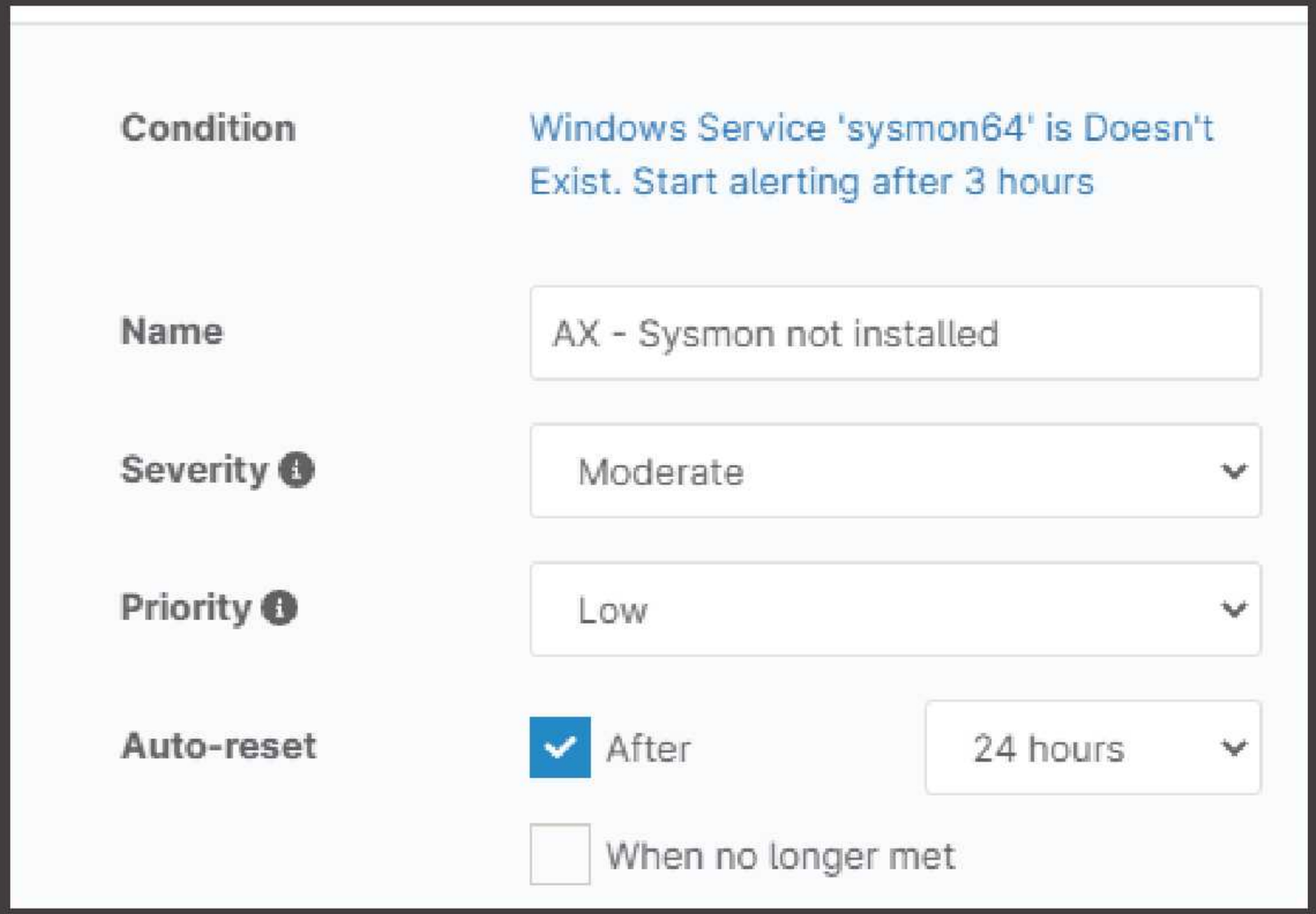
go to adminisration> Policies> Agent Policies and add scheduled script to install sysmon. We do this at our "top" or inherited policies so that it effects all systems.

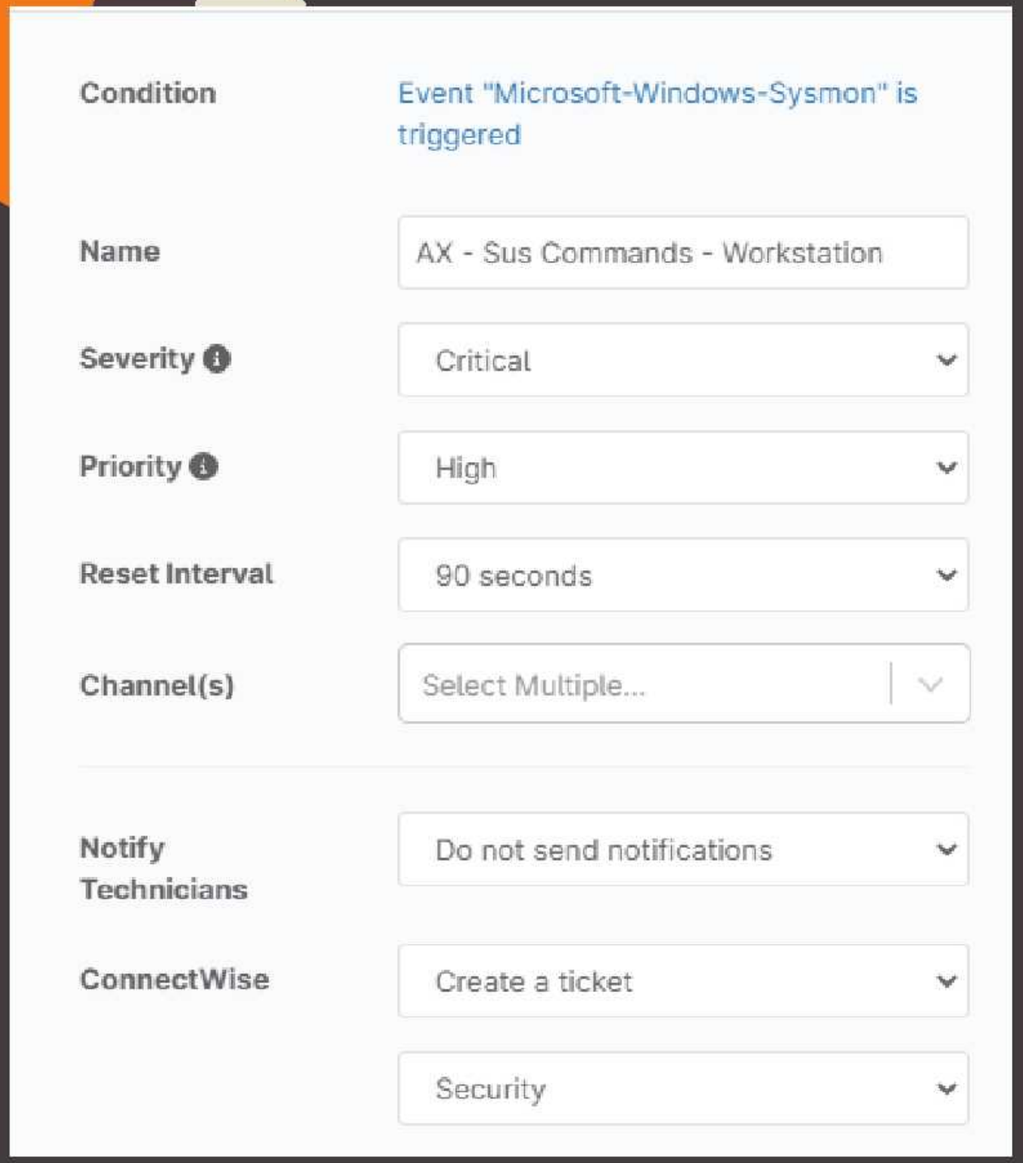


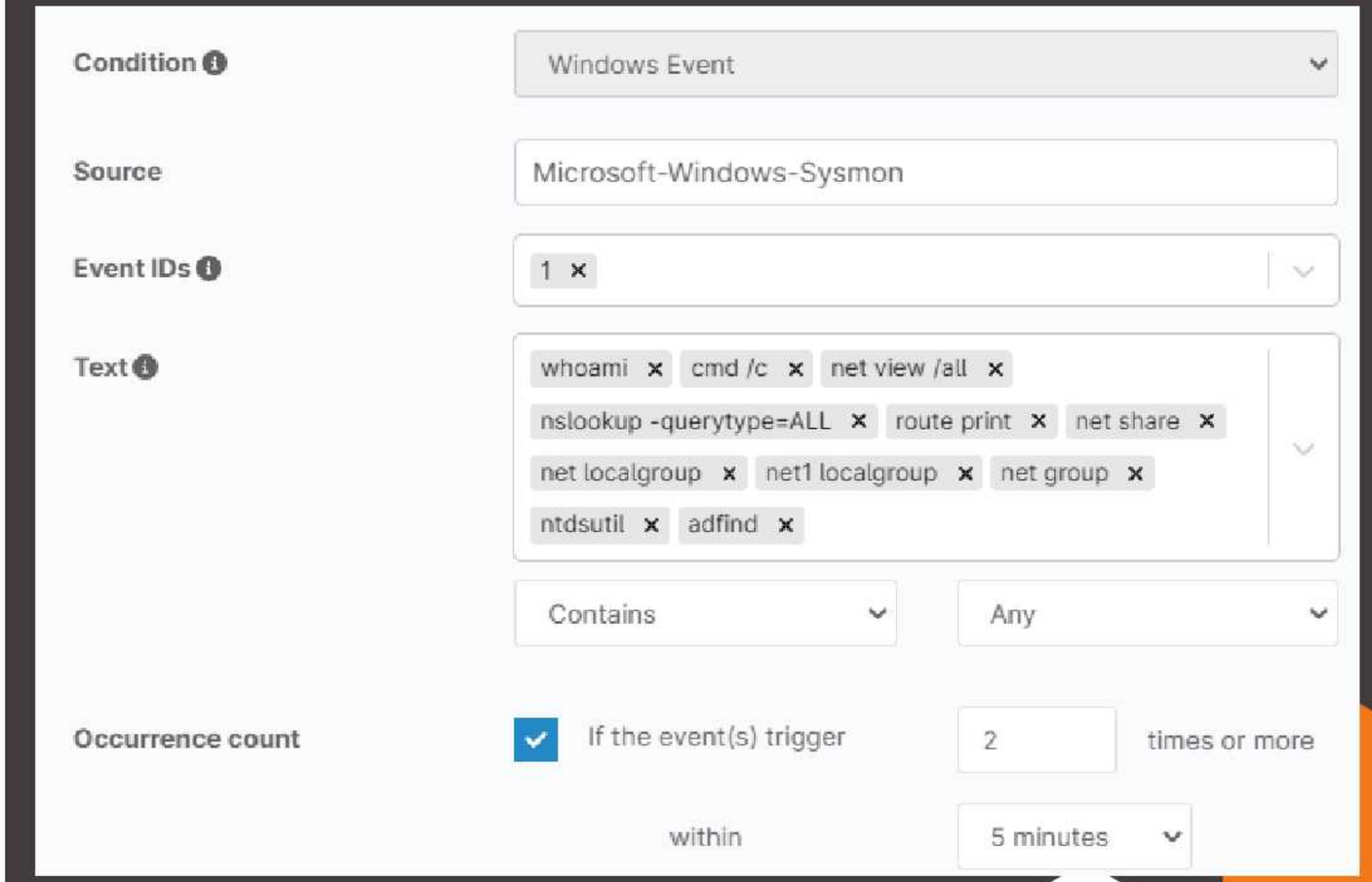
go to adminisration> Policies> Agent Policies and add the following Conditions. We do this at our "top" or inherited policies so that it effects all systems.

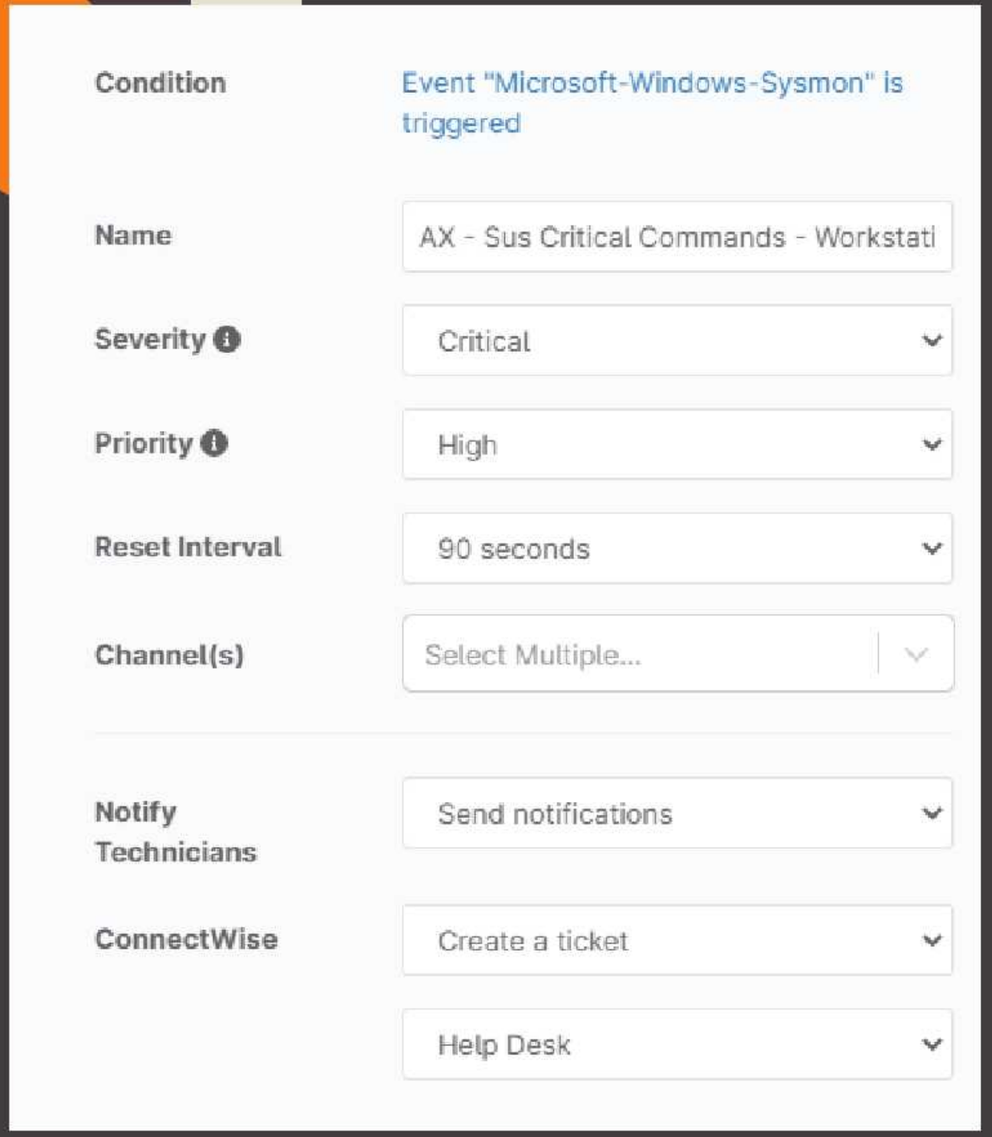


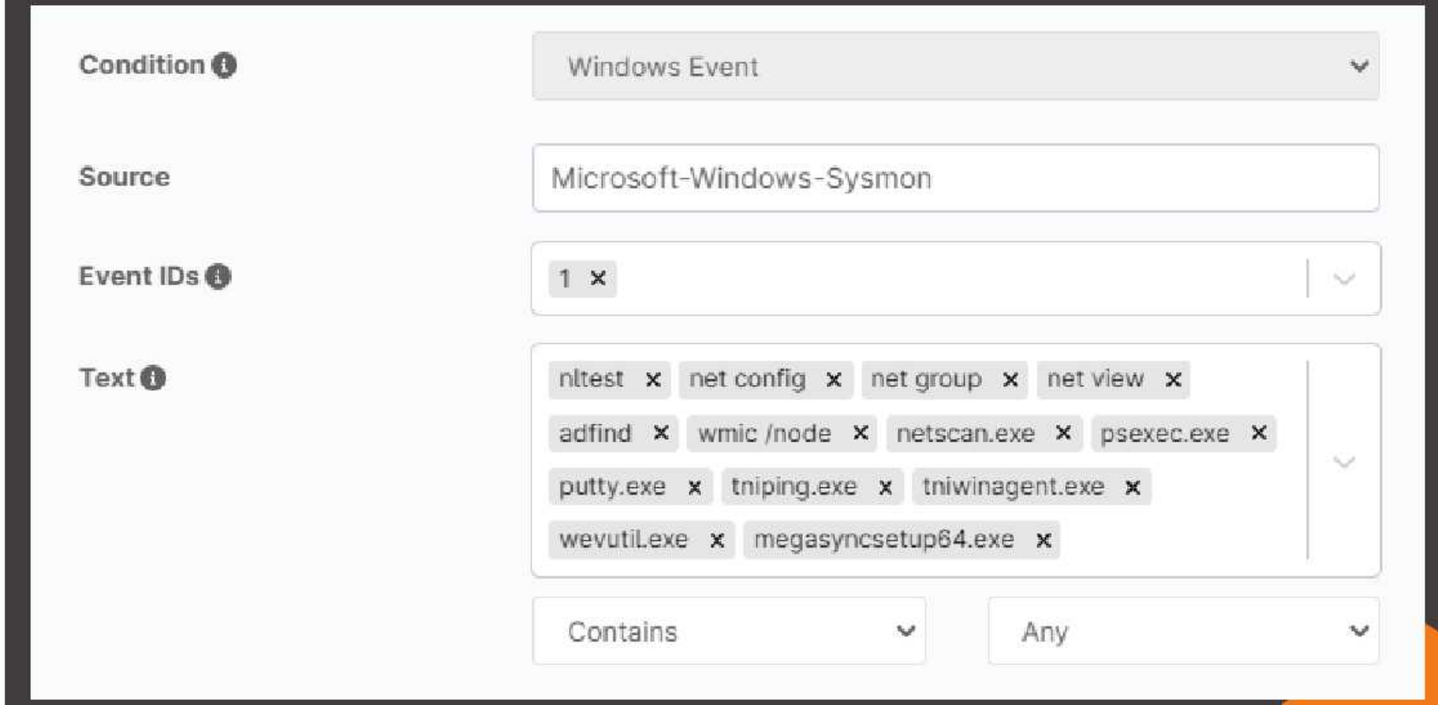
These are our conditions for Sysmon


Condition
Windows Service 'sysmon64' is Doesn't Exist. Start alerting after 3 hours
Name
AX - Sysmon not installed
Severity
Moderate
Priority
Low
Auto-reset
After
24 hours
When no longer met


Condition
Event "Microsoft-Windows-Sysmon" is triggered
Name
AX - Sus Commands - Workstation
Severity
Critical
Priority
High
Reset Interval
90 seconds
Channel(s)
Select Multiple...
Notify Technicians
Do not send notifications
ConnectWise
Create a ticket
Security

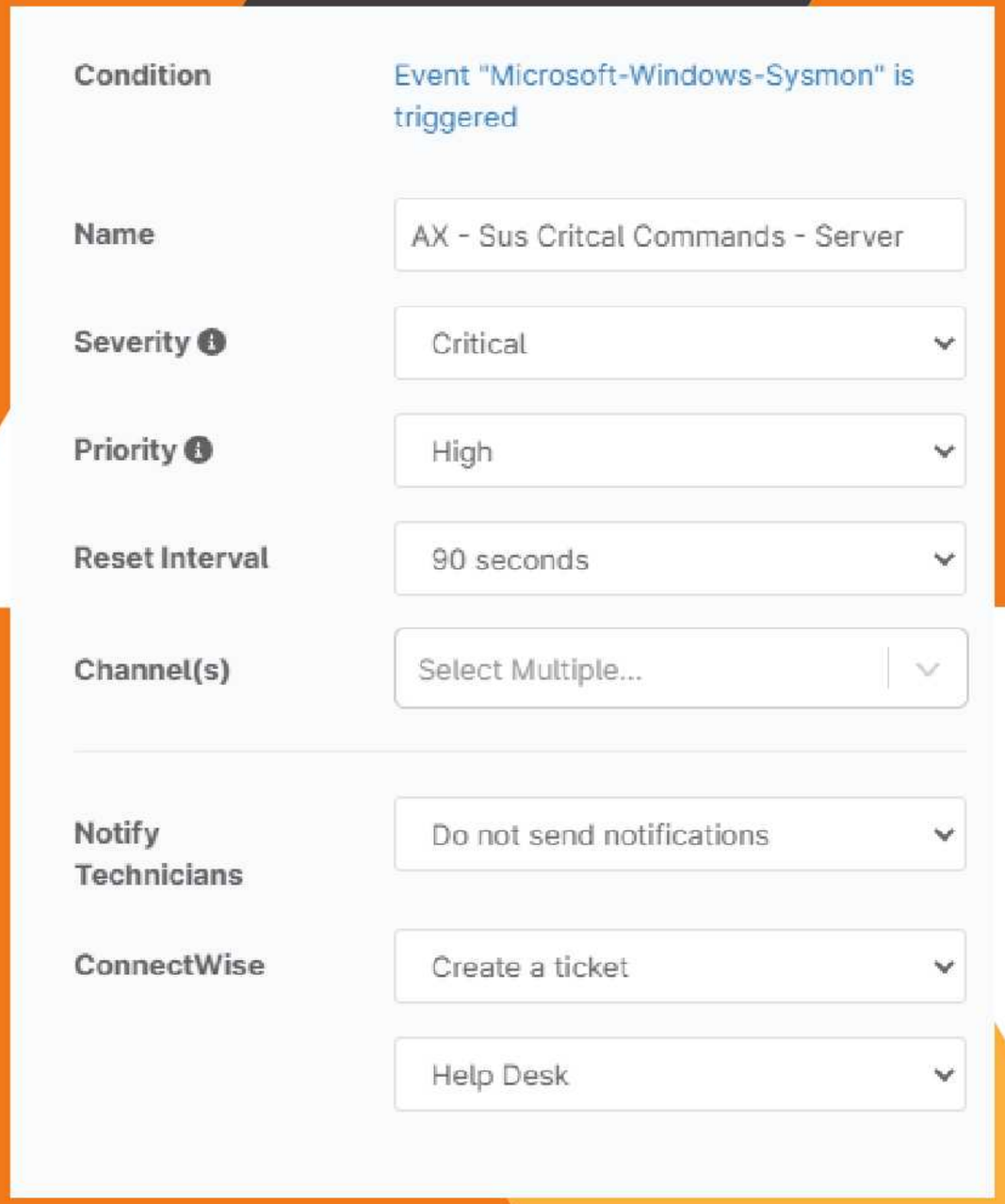

Condition
Windows Event
Source
Microsoft-Windows-Sysmon
Event IDs
1
Text
whoami
cmd /c
net view /all
nslookup -querytype=ALL
route print
net share
net localgroup
net1 localgroup
net group
ntdsutil
adfind
Contains
Any
Occurrence count
If the event(s) trigger
2
times or more
within
5 minutes

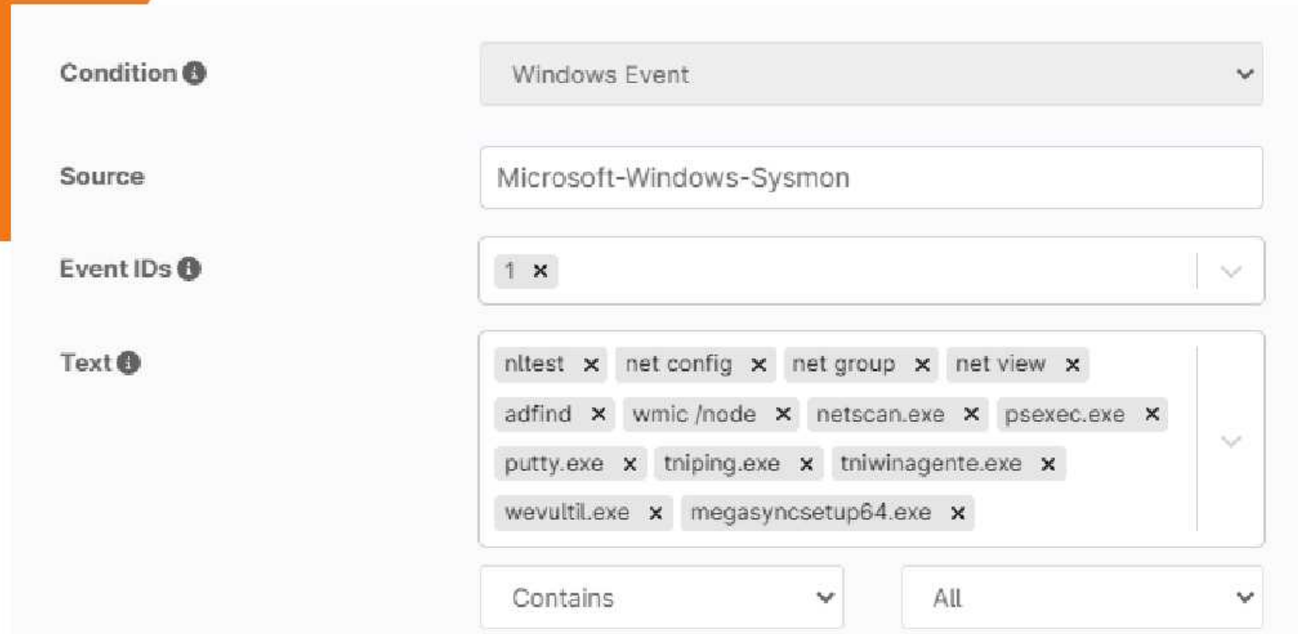

Condition
Event "Microsoft-Windows-Sysmon" is triggered
Name
AX - Sus Critical Commands - Workstati
Severity
Critical
Priority
High
Reset Interval
90 seconds
Channel(s)
Select Multiple...
Notify Technicians
Send notifications
ConnectWise
Create a ticket
Help Desk


Condition
Windows Event
Source
Microsoft-Windows-Sysmon
Event IDs
1
Text
nltest
net config
net group
net view
adfind
wmic /node
netscan.exe
psexec.exe
putty.exe
tniping.exe
tniwinagent.exe
wevutil.exe
megasyncsetup64.exe
Contains
Any

Condition	Event "Microsoft-Windows-Sysmon" is triggered
Name	AX - Sus Commands - Server
Severity	Critical
Priority	High
Reset Interval	90 seconds
Channel(s)	Select Multiple...
Notify Technicians	Do not send notifications
ConnectWise	Create a ticket
	Security

Condition	Windows Event
Source	Microsoft-Windows-Sysmon
Event IDs	1
Text	whoami, cmd /c, net view /all, nslookup- -querytype=ALL, route print, net share, net localgroup, net1 localgroup, ntdsutil, winpcap, net user
	Contains / Any


Condition
Event "Microsoft-Windows-Sysmon" is triggered
Name
AX - Sus Critcal Commands - Server
Severity
Critical
Priority
High
Reset Interval
90 seconds
Channel(s)
Select Multiple...
Notify Technicians
Do not send notifications
ConnectWise
Create a ticket
Help Desk


Condition
Windows Event
Source
Microsoft-Windows-Sysmon
Event IDs
1
Text
nltest
net config
net group
net view
adfind
wmic /node
netscan.exe
psexec.exe
putty.exe
tniping.exe
tniwinagente.exe
wevutil.exe
megasyncsetup64.exe
Contains
All

Ninja
4/21/2023 2:47 PM

EventId: 1, EventTime: 2023-04-21T18:45:09Z, Source: Microsoft-Windows-Sysmon, Message: Process Create:
RuleName: -
UtcTime: 2023-04-21 18:45:09.398
ProcessGuid: {5ef4105d-d9b5-6442-ccce-000000002b00}
ProcessId: 44600
Image: C:\Users' \Documents\Programs\putty.exe
FileVersion: Release 0.67
Description: SSH, Telnet and Rlogin client
Product: PuTTY suite
Company: Simon Tatham
OriginalFileName: PuTTY
CommandLine: "C:\Users' i\Documents\Programs\putty.exe"
CurrentDirectory: C:\User: n\Documents\Programs\
LogonGuid: {5ef4105d-bd43-643d-3492-1c0000000000}
LogonId: 0x1C9234
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes:
MD5=BA78410702F0CC8453DA1AFBB2A8B670,SHA256=9F9E74241D59ECCFE7040BFDCBBCEACB374EDA397CC53A4197B59E4F6F380
F008B4BAEB119DE
ParentProcessGuid: {5ef4105d-bd46-643d-da00-000000002b00}
ParentProcessId: 11480
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE

EventId: 4720, EventTime: 2023-04-25T20:58:52Z, Source: Microsoft-Windows-Security-Auditing, Message: A user account was created.

Account Name: Nathan
Account Domain: AXIOMDEMO

Attributes:
SAM Account Name: Nathan
Display Name: Nathan NotTheWiringGuy
User Principal Name: Nathan@AxiomDemo.Local
Home Directory: -
Home Drive: -
Script Path: -
Profile Path: -
User Workstations: -
Password Last Set: <never>
Account Expires: <never>
Primary Group ID: 513
Allowed To Delegate To: -
Old UAC Value: 0x0
New UAC Value: 0x15
User Account Control:

Account Disabled
'Password Not Required' - Enabled
'Normal Account' - Enabled
User Parameters: -
SID History: -