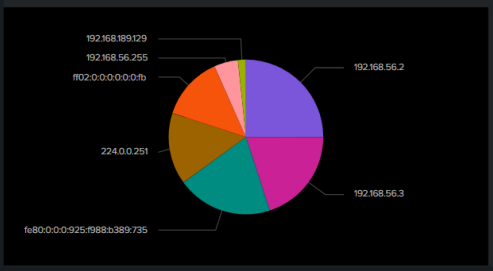
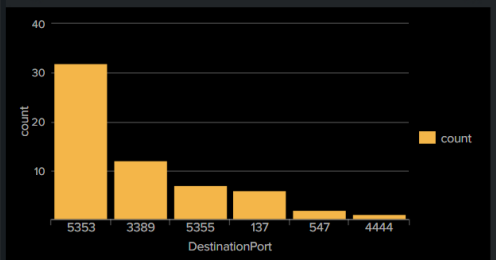
SOC LAB Monitoring Project 1

☆ Edit Export ▾ ...

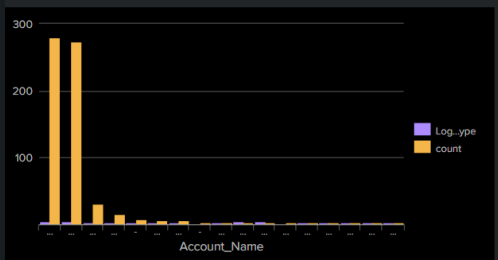
Top Source IPs Connecting to This Host



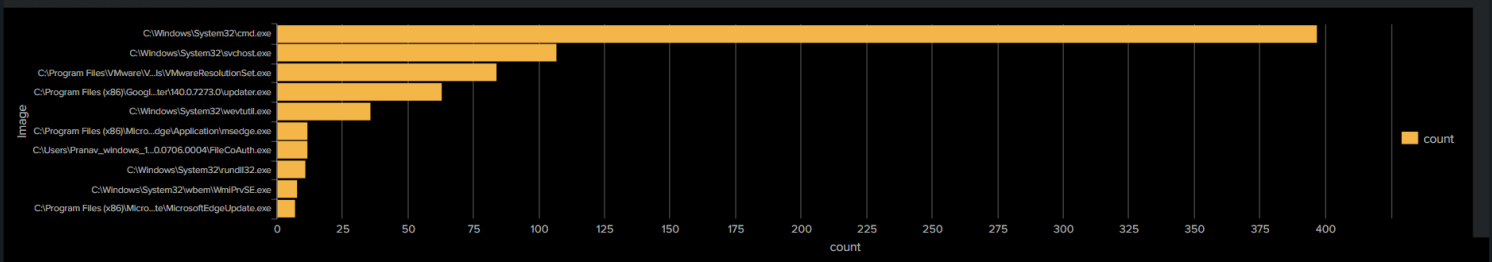
Top Destination Ports Used



User Logons



Top 10 Processes Executed



Suspicious Parent-Child Process Combinations

ParentImage	Image
C:\Windows\System32\cmd.exe	C:\Windows\System32\net.exe
C:\Windows\System32\cmd.exe	C:\Windows\System32\NETSTAT.EXE
C:\Windows\System32\cmd.exe	C:\Windows\System32\ipconfig.exe
C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\ipconfig.exe
C:\Windows\System32\CompatTelRunner.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\NETSTAT.EXE
C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\net.exe
C:\Windows\System32\cmd.exe	C:\Windows\System32\reg.exe

Reverse Shell or Netcat Indicators

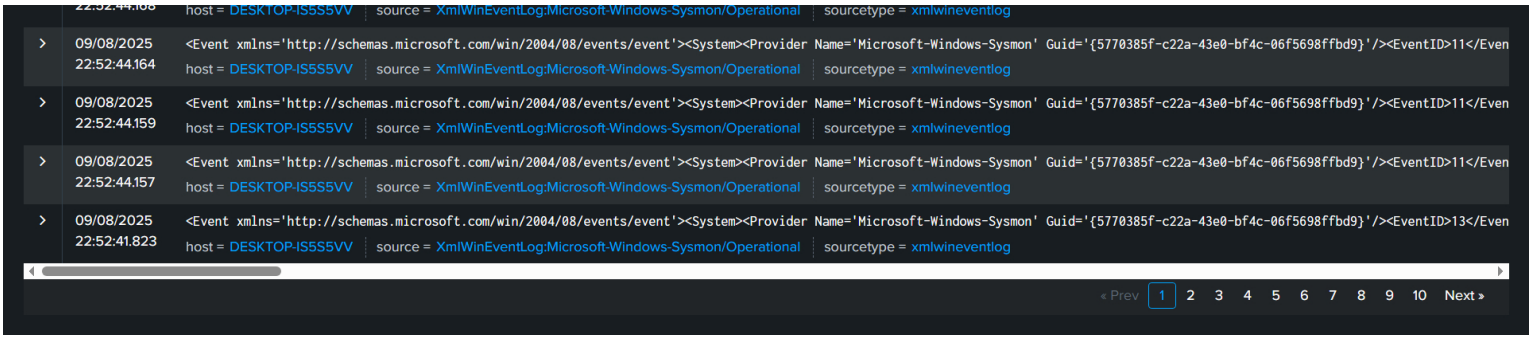
_time	ParentImage	Image
2025-08-09 03:52:47.344	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysW
2025-08-09 03:52:36.736	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysW
2025-08-09 03:52:25.175	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysW
2025-08-09 03:52:17.474	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysW
2025-08-09 03:52:11.934		C:\Windows\SysW
2025-08-09 03:52:11.918		
2025-08-09 03:52:11.922	C:\Users\Pranav_windows_10\Downloads\ProjectReport.pdf.exe	C:\Windows\SysW

New or Modified Registry Keys

TargetObject	count
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3195181318-4265862901-2077024835-1001\\Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	192
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3195181318-4265862901-2077024835-1001\\Device\HarddiskVolume3\Windows\System32\dllhost.exe	182
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3195181318-4265862901-2077024835-1001\\Device\HarddiskVolume3\Program Files\Google\Chrome\Application\chrome.exe	158
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\UpdateOrchestrator\Schedule Maintenance Work\Index	98
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\UpdateOrchestrator\Schedule Wake To Work\Index	98
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\UpdateOrchestrator\Schedule Work\Index	98
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3195181318-4265862901-2077024835-1001\MicrosoftWindows.Client.CBS_cw5n1h2txyewy	55
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3195181318-4265862901-2077024835-1001\Microsoft.Windows.Search_cw5n1h2txyewy	51
HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3195181318-4265862901-2077024835-1001\Microsoft.ScreenSketch_8wekyb3d8bbwe	46
HKLM\System\CurrentControlSet\Services\SharedAccess\Epoch\Epoch	38

Endpoint Logs

i	Time	Event
>	09/08/2025 22:52:45.549	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	09/08/2025 22:52:45.547	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	09/08/2025 22:52:45.052	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</Even host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	09/08/2025 22:52:44.178	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	09/08/2025 22:52:44.174	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
>	09/08/2025	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even


host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
09/08/2025 22:52:44.164
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even
host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
09/08/2025 22:52:44.159
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even
host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
09/08/2025 22:52:44.157
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</Even
host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
09/08/2025 22:52:41.823
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>13</Even
host = DESKTOP-IS5S5VV source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog
« Prev 1 2 3 4 5 6 7 8 9 10 Next »