New Search

```
1  index=main
2  | stats count by host
```

6 hour window

130 of 130 events matched No Event Sampling

Events (130)

Format Timeline 1 hour per column

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a attachment 3
a content 47
a datasource 2
a direction 3
a event.action 6
event.code 6
a host.name 13
a index 1
linecount 1
a process.name 14
process.pid 60
a punct 45
a recipient 39
a registry.key 11
a registry.path 11
a registry.value 3
a sender 36
a splunk_server 1
a subject 47
a timestamp 100+

9 more fields

+ Extract New Fields (/en-US/app/search/field_extractor?sid=rt_176787047l.10)

Time	Event
1/8/26 11:10:24.235 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: 01/08/2026 11:10:24.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:10:13.235 AM	{ [-] attachment: None content: Got it. Will prepare the slides. datasource: email direction: internal recipient: invoice@tryhatme.com sender: invoice@tryhatme.com subject: RE: New Hat Designs - Team Meeting Tomorrow timestamp: 01/08/2026 11:10:13.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:10:09.235 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3457 process.name: spoolsv.exe process.pid: 3823 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: 01/08/2026 11:10:09.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:10:08.235 AM	{ [-] attachment: None content: Love these! The blue one is my favorite. datasource: email direction: internal recipient: yani.zubair@tryhatme.com sender: yani.zubair@tryhatme.com subject: RE: Hat-tastic News: New Designs Unveiled! timestamp: 01/08/2026 11:10:08.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:09:48.235 AM	{ [-] attachment: None content: Thank you for the opportunity I confirm my availability and look forward to speaking with your team datasource: email direction: outbound recipient: gardner@chicchapeauqueen.com sender: invoice@tryhatme.com subject: RE: Job Interview Invitation: Exciting Career Opportunity timestamp: 01/08/2026 11:09:48.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:09:47.235 AM	{ [-] attachment: None content: Will there be a recording available for those unable to attend live datasource: email direction: outbound recipient: tobias@crowninggloryhats.org sender: armaan.terry@tryhatme.com subject: RE: RE: Seminar Registration: Hat Industry Innovation Trends timestamp: 01/08/2026 11:09:47.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:09:41.235 AM	{ [-] attachment: None content: Gorgeous hat wearing models from the Moon are searching for their Earth soulmate Could it be you Click to chat now datasource: email direction: inbound recipient: roger.fedora@tryhatme.com sender: levine@headwearmarketwatch.org subject: Lunarian Hat Models Want to Meet You Click for Love timestamp: 01/08/2026 11:09:41.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:09:33.235 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3452 process.pid: 3727 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: 01/08/2026 11:09:33.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:09:16.235 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-3456 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3674 timestamp: 01/08/2026 11:09:16.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:09:06.235 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-3461 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3948 timestamp: 01/08/2026 11:09:06.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:08:20.235 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-3451 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3771 timestamp: 01/08/2026 11:08:20.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:08:03.235 AM	{ [-] attachment: None content: Love these! The blue one is my favorite. datasource: email direction: internal recipient: kyra.flores@tryhatme.com sender: kyra.flores@tryhatme.com subject: RE: Hat-tastic News: New Designs Unveiled! timestamp: 01/08/2026 11:08:03.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:07:47.235 AM	{ [-] attachment: None content: Want a bigger more impressive hat collection Our revolutionary hat growth formula guarantees results in just days Try now before the FDA finds out datasource: email direction: inbound recipient: michael.ascot@tryhatme.com sender: keane@modernmillinerygroup.online subject: Amazing Hat Enhancement Pills Grow Your Hat Collection Instantly timestamp: 01/08/2026 11:07:47.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:07:46.235 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: 01/08/2026 11:07:46.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:07:24.235 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: 01/08/2026 11:07:24.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:07:08.235 AM	{ [-] attachment: forceupdate.ps1 content: Thanks Yani! I'll run this script right away. The update issues have been really frustrating lately. datasource: email direction: internal recipient: yani.zubair@tryhatme.com sender: michelle.smith@tryhatme.com subject: RE: Force update fix timestamp: 01/08/2026 11:07:08.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:07:00.235 AM	{ [-] datasource: sysmon event.action: CreateRemoteThread detected (rule: CreateRemoteThread) event.code: 8 host.name: win-3460 process.name: dwm.exe process.pid: 3772 timestamp: 01/08/2026 11:07:00.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:06:57.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml:OECustomProperty host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:57.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:57.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:57.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:57.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:57.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:06:57.235 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: RegistryEvent) event.code: 13 host.name: win-3449 process.name: spoolsv.exe process.pid: 3844 registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion registry.value: driverVersion timestamp: 01/08/2026 11:06:57.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:57.235 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: 01/08/2026 11:06:57.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:06:57.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml:Zone.Identifier host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:57.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:54.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml:Zone.Identifier host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:54.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:54.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml:OECustomProperty host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:54.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:06:54.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:54.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:54.235 AM	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJQB\Important: Pending Invioce!.eml host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 01/08/2026 11:06:54.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:40.235 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-3451 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3724 timestamp: 01/08/2026 11:06:40.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:06:22.235 AM	{ [-] attachment: None content: Just following up to see if the designs meet your expectations and if you need any modifications before finalizing the order datasource: email direction: inbound recipient: michelle.smith@tryhatme.com sender: edna@headwearreporter.net subject: RE: RE: Inquiry: Custom Hat Order for Corporate Gifting timestamp: 01/08/2026 11:06:22.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:08.235 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-3454 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3620 timestamp: 01/08/2026 11:06:08.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:06:06.235 AM	{ [-] attachment: None content: Hurry These suspiciously cheap hotel vouchers are selling fast Book now before they totally stop working upon arrival datasource: email direction: outbound recipient: josephine@yahoo.com sender: support@tryhatme.com subject: Scam Alert Fake Hat Hotel Vouchers Up for Grabs timestamp: 01/08/2026 11:06:06.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:06:06.235 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: Registry Event) event.code: 13 host.name: win-3455 process.name: spoolsv.exe process.pid: 3913 registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion registry.value: driverVersion timestamp: 01/08/2026 11:06:06.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:05:52.235 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-3451 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3726 timestamp: 01/08/2026 11:05:52.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:05:41.235 AM	{ [-] attachment: None content: Our exclusive system guarantees instant Bitcoin doubling Send us just 100 and watch it turn into 200 instantly datasource: email direction: inbound recipient: diego.summers@tryhatme.com sender: tim@headweartrendsetters.org subject: Instant Wealth Send Bitcoin to Double Your Money timestamp: 01/08/2026 11:05:41.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:05:39.235 AM	{ [-] attachment: None content: I have added some discussion points to the agenda We should also touch on competitive analysis datasource: email direction: inbound recipient: michael.ascot@tryhatme.com sender: silas@customcrownhats.org subject: RE: RE: Scheduling a Virtual Meeting to Discuss Market Trends timestamp: 01/08/2026 11:05:39.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:05:35.235 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3451 process.name: spoolsv.exe process.pid: 3751 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: 01/08/2026 11:05:35.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:05:33.235 AM	{ [-] attachment: None content: Just confirming my attendance Will there be a list of attendees shared beforehand datasource: email direction: inbound recipient: cain.omoore@tryhatme.com sender: juliet@panachepanamas.com subject: RE: RE: Invitation to a Business Networking Luncheon Next Week timestamp: 01/08/2026 11:05:33.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:05:31.235 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3457 process.name: spoolsv.exe process.pid: 3989 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: 01/08/2026 11:05:31.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:05:27.235 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3451 process.name: spoolsv.exe process.pid: 3955 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: 01/08/2026 11:05:27.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:05:14.235 AM	{ [-] datasource: sysmon event.action: Registry object added or deleted (rule: RegistryEvent) event.code: 12 host.name: win-3457 process.name: spoolsv.exe process.pid: 3859 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: 01/08/2026 11:05:14.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:05:02.235 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: RegistryEvent) event.code: 13 host.name: win-3450 process.name: spoolsv.exe process.pid: 3846 registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion registry.value: driverVersion timestamp: 01/08/2026 11:05:02.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:04:54.235 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: 01/08/2026 11:04:54.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:04:51.235 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: 01/08/2026 11:04:51.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:04:50.235 AM	{ [-] attachment: None content: Forwarding this information to our design team for review and feedback datasource: email direction: outbound recipient: arthur@hatfashionfair2022.com sender: support@tryhatme.com subject: FWD: Vendor Showcase: Latest Hat Materials and Designs timestamp: 01/08/2026 11:04:50.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:04:14.235 AM	{ [-] attachment: None content: Reminder: Sign-ups close tomorrow. datasource: email direction: internal recipient: roger.fedora@tryhatme.com sender: roger.fedora@tryhatme.com subject: FWD: Employee Appreciation Day - Volunteer Sign-Up timestamp: 01/08/2026 11:04:14.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:03:54.235 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: RegistryEvent) event.code: 13 host.name: win-3454 process.name: spoolsv.exe process.pid: 3953 registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5)\DsDriver\driverVersion registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5)\DsDriver\driverVersion registry.value: driverVersion timestamp: 01/08/2026 11:03:54.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:03:51.235 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: 3684 registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{9A7D6000-6360-4067-AFEC-3F8722701AC5}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{9A7D6000-6360-4067-AFEC-3F8722701AC5}#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName registry.value: FriendlyName timestamp: 01/08/2026 11:03:51.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:03:09.235 AM	{ [-] datasource: sysmon event.action: Registry value set (rule: RegistryEvent) event.code: 13 host.name: win-3449 process.name: spoolsv.exe process.pid: 3645 registry.key: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion registry.path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 4)\DsDriver\driverVersion registry.value: driverVersion timestamp: 01/08/2026 11:03:09.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json

Time	Event
1/8/26 11:02:51.235 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: 01/08/2026 11:02:51.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json
1/8/26 11:02:51.235 AM	{ [-] datasource: sysmon dns.answers.data: mail.tryhatme.finance, 34.244.197.202 dns.question.name: autodiscover.tryhatme.finance dns.resolved_ip: 34.244.197.202 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3454 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3648 timestamp: 01/08/2026 11:02:51.235 } Show as raw text host = 10.10.140.198:8989 source = eventcollector sourcetype = _json