New Search

```
1  sourcetype=_json datasource=sysmon event.code=22
2  | table timestamp host.name process.name dns.question.name dns.resolved_ip
```

Last 24 hours

✓ **21 events** (12/13/25 5:00:00.000 AM to 12/14/25 5:27:01.000 AM) No Event Sampling

Events (21)

Format Timeline 1 hour per column

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a datasource 1
a dns.answers.data 6
a dns.question.name 5
a dns.resolved_ip 5
a event.action 1
event.code 1
a host.name 12
a index 1
linecount 1
a network.protocol 1
a process.name 2
process.pid 20
a punct 1
a splunk_server 1
a timestamp 21

+ Extract New Fields (/en-US/app/search/field_extractor?sid=1765690021.258)

Time	Event
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
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

Time	Event
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 5:00:02.369 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
12/14/25 4:54:25.369 AM	{ [-] datasource: sysmon dns.answers.data: 3.22.53.161 dns.question.name: 2.tcp.ngrok.io dns.resolved_ip: 3.22.53.161 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3450 network.protocol: dns process.name: powershell.exe process.pid: 3880 timestamp: 12/14/2025 04:54:25.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:54:24.369 AM	{ [-] datasource: sysmon dns.answers.data: 185.199.111.133, 185.199.110.133, 185.199.109.133, 185.199.108.133 dns.question.name: raw.githubusercontent.com dns.resolved_ip: 185.199.111.133, 185.199.110.133, 185.199.109.133, 185.199.108.133 event.action: Dns query (rule: DnsQuery) event.code: 22 host.name: win-3450 network.protocol: dns process.name: powershell.exe process.pid: 3880 timestamp: 12/14/2025 04:54:24.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:52:08.369 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-3456 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3978 timestamp: 12/14/2025 04:52:08.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:51:15.369 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-3460 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3979 timestamp: 12/14/2025 04:51:15.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:51:14.369 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-3455 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3946 timestamp: 12/14/2025 04:51:14.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:46:37.369 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-3456 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3674 timestamp: 12/14/2025 04:46:37.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:46:27.369 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-3461 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3948 timestamp: 12/14/2025 04:46:27.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:45:41.369 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-3451 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3771 timestamp: 12/14/2025 04:45:41.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:44:01.369 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-3451 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3724 timestamp: 12/14/2025 04:44:01.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:43:29.369 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-3454 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3620 timestamp: 12/14/2025 04:43:29.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:43:13.369 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-3451 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3726 timestamp: 12/14/2025 04:43:13.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:40:12.369 AM	{ [-] datasource: sysmon dns.answers.data: mail.tryhatme.finance, 34.24g 4.197.202 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: 12/14/2025 04:40:12.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:37:55.369 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-3449 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3587 timestamp: 12/14/2025 04:37:55.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:34:15.369 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-3456 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3914 timestamp: 12/14/2025 04:34:15.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:29:36.369 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-3458 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3906 timestamp: 12/14/2025 04:29:36.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json
12/14/25 4:27:47.369 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-3455 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3600 timestamp: 12/14/2025 04:27:47.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json

Time	Event
12/14/25 4:25:20.369 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-3449 network.protocol: dns process.name: OUTLOOK.EXE process.pid: 3801 timestamp: 12/14/2025 04:25:20.369 } Show as raw text host = 10.10.106.238:8989 source = eventcollector sourcetype = _json