# New Search

```
index=_audit action="search" user="kimjoe" "botsv3"
| table _time user action search
| sort - _time
```

Time range: All time

✓ **1,848 events** (before 15/12/2025 09:58:33.000) No Event Sampling

**Statistics (1,848)**

| | _time | user | action | search |
|---|---|---|---|---|
| 60 | 2025-12-03 02:02:12.465 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail \| fieldsummary \| search field="*mfa*" OR field="*MFA*" \| table field, count' |
| 60 | 2025-12-03 02:00:24.005 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| head 10 \| table host, processor, os, category, type' |
| 60 | 2025-12-03 02:00:19.937 | kimjoe | search | 'search index=botsv3 sourcetype=hardware \| head 10 \| table host, processor, os, category, type' |
| 60 | 2025-12-03 01:57:24.000 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" \| table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |

| | _time | user | action | search |
|---|---|---|---|---|
| 60605 | 2025-12-03 01:57:20.775 | kimjoe | search | 'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" \| table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList' |
| 60606 | 2025-12-03 01:56:24.003 | kimjoe | search | 'search |
| 60607 | 2025-12-03 01:55:57.767 | kimjoe | search | 'search |
| 60608 | 2025-12-03 01:50:24.066 | kimjoe | search | 'search index=botsv3 host="SEPM" \| stats count by sourcetype' |
| 60609 | 2025-12-03 01:50:09.271 | kimjoe | search | 'search index=botsv3 host="SEPM" \| stats count by sourcetype' |
| 61060 | 2025-12-03 01:48:24.097 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^\s]+)" \| eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") \| stats count by computer, pattern \| search pattern="Different"' |
| 61061 | 2025-12-03 01:48:24.070 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^\s]+)" \| stats count by computer \| sort computer' |

| | _time | user | action | search |
|---|---|---|---|---|
| 61 | 2025-12-03 01:48:07.058 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^\s]+)" \| eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") \| stats count by computer, pattern \| search pattern="Different"' |
| 61 | 2025-12-03 01:47:55.465 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^\s]+)" \| stats count by computer \| sort computer' |
| 61 | 2025-12-03 01:45:54.086 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn' |
| 61 | 2025-12-03 01:45:41.318 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn' |
| 61 | 2025-12-03 01:44:24.000 | kimjoe | search | '\| metadata type=sourcetypes index=botsv3 \| search sourcetype="*windows*" OR sourcetype="*win*" OR sourcetype="*os*"' |
| 61 | 2025-12-03 01:44:05.875 | kimjoe | search | '\| metadata type=sourcetypes index=botsv3 \| search sourcetype="*windows*" OR sourcetype="*win*" OR sourcetype="*os*"' |
| 61 | 2025-12-03 01:42:54.080 | kimjoe | search | 'search index=botsv3 sourcetype=winhostmon \| stats count by host' |
| 61 | 2025-12-03 01:42:24.568 | kimjoe | search | 'search index=botsv3 sourcetype=winhostmon \| stats count by host' |

| | _time | user | action | search |
|---|---|---|---|---|
| 620 | 2025-12-03 01:34:24.039 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^\s]+)" \| eval pattern = if(match(computer, "-L\.froth\.ly$"), "Standard", "Different") \| stats count by computer, pattern \| search pattern="Different"' |
| 621 | 2025-12-03 01:34:24.012 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results \| search name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| stats values(os) as os_edition by host' |
| 622 | 2025-12-03 01:34:11.231 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^\s]+)" \| eval pattern = if(match(computer, "-L\.froth\.ly$"), "Standard", "Different") \| stats count by computer, pattern \| search pattern="Different"' |
| 623 | 2025-12-03 01:33:59.359 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results \| search name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| stats values(os) as os_edition by host' |
| 624 | 2025-12-03 01:33:54.010 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| search "Windows" AND ("Server" OR "Enterprise" OR "Professional") \| rex field=_raw "(?i)windows\s+(?<edition>[^\s]+)" \| stats values(edition) as editions by host' |
| 625 | 2025-12-03 01:33:47.616 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| search "Windows" AND ("Server" OR "Enterprise" OR "Professional") \| rex field=_raw "(?i)windows\s+(?<edition>[^\s]+)" \| stats values(edition) as editions by host' |
| 626 | 2025-12-03 01:30:54.008 | kimjoe | search | 'search index=botsv3 \| rex field=_raw "SEPM\.(?<domain>[^\s]+)" \| stats count by domain' |

| | _time | user | action | search |
|---|---|---|---|---|
| 627 | 2025-12-03 01:29:44.729 | kimjoe | search | 'search index=botsv3 \| rex field=_raw "SEPM\.(?<domain>[^\s]+)" \| stats count by domain' |
| 628 | 2025-12-03 01:29:24.045 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| search "Windows" AND "Version" \| rex field=_raw "Version\s+(?<version>[0-9\.]+)" \| stats values(version) as versions by host' |
| 629 | 2025-12-03 01:29:24.028 | kimjoe | search | 'search index=botsv3 \| rex field=_raw "SEPM\.(?<domain>[^\s]+)" \| stats count by domain' |
| 630 | 2025-12-03 01:28:54.713 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| search "Windows" AND "Version" \| rex field=_raw "Version\s+(?<version>[0-9\.]+)" \| stats values(version) as versions by host' |
| 631 | 2025-12-03 01:28:24.217 | kimjoe | search | 'search index=botsv3 \| search "SEPM" AND "froth.ly" \| head 5 \| table _raw' |
| 632 | 2025-12-03 01:28:24.203 | kimjoe | search | 'search index=botsv3 host="SEPM" \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn' |
| 633 | 2025-12-03 01:28:22.223 | kimjoe | search | 'search index=botsv3 \| search "SEPM" AND "froth.ly" \| head 5 \| table _raw' |
| 634 | 2025-12-03 01:27:59.207 | kimjoe | search | 'search index=botsv3 host="SEPM" \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn' |

| | _time | user | action | search |
|---|---|---|---|---|
| 63 | 2025-12-03 01:26:57.643 | kimjoe | search | 'search index=botsv3 \| rex field=_raw "SEPM\.(?<domain>[^\s]+)" \| stats count by domain' |
| 63 | 2025-12-03 01:26:54.161 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| search "Windows" AND "Version" \| rex field=_raw "Version\s+(?<version>[0-9\.]+)" \| stats values(version) as versions by host' |
| 63 | 2025-12-03 01:26:34.469 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| search "Windows" AND "Version" \| rex field=_raw "Version\s+(?<version>[0-9\.]+)" \| stats values(version) as versions by host' |
| 63 | 2025-12-03 01:26:24.181 | kimjoe | search | 'search index=botsv3 \| search "SEPM" AND "froth.ly" \| head 5 \| table _raw' |
| 63 | 2025-12-03 01:26:24.166 | kimjoe | search | 'search index=botsv3 host="SEPM" \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn' |
| 64 | 2025-12-03 01:26:20.505 | kimjoe | search | 'search index=botsv3 \| search "SEPM" AND "froth.ly" \| head 5 \| table _raw' |
| 64 | 2025-12-03 01:26:09.612 | kimjoe | search | 'search index=botsv3 host="SEPM" \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn' |
| 64 | 2025-12-03 01:23:24.068 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| sort fqdn' |

| | _time | user | action | search |
|---|---|---|---|---|
| 64 | 2025-12-03 01:22:54.054 | kimjoe | search | ' search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 64 | 2025-12-03 01:22:54.041 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| join type=inner fqdn [ search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 64 | 2025-12-03 01:22:53.080 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| sort fqdn' |
| 64 | 2025-12-03 01:22:26.401 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| join type=inner fqdn [ search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 64 | 2025-12-03 01:22:24.109 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^,\s]+)" \| stats count by computer \| sort computer' |
| 64 | 2025-12-03 01:22:08.741 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^,\s]+)" \| stats count by computer \| sort computer' |
| 64 | 2025-12-03 01:21:54.038 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| rex field=_raw "(?i)windows\s+(?<version>[0-9\.]+\|server[^\s]*)" \| where isnotnull(version) \| stats values(version) as versions by fqdn' |

| | _time | user | action | search |
|---|---|---|---|---|
| 6 | 2025-12-03 01:21:47.0 | kimj | sear | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw |
| 5 | 87 | oe | ch | "ComputerName=(?<fqdn>[^,\s]+)" \| rex field=_raw "(?i)windows |
| 0 | | | | \s+(?<version>[0-9\.]+\|server[^\s]*)" \| where isnotnull(versio |
| | | | | n) \| stats values(version) as versions by fqdn' |
| 6 | 2025-12-03 01:21:24.0 | kimj | sear | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw |
| 5 | 35 | oe | ch | "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| so |
| 1 | | | | rt fqdn' |
| 6 | 2025-12-03 01:21:17.4 | kimj | sear | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw |
| 5 | 85 | oe | ch | "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| so |
| 2 | | | | rt fqdn' |
| 6 | 2025-12-03 01:20:54.0 | kimj | sear | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw |
| 5 | 82 | oe | ch | "ComputerName=(?<fqdn>[^,\s]+)" \| stats count as event_count b |
| 3 | | | | y fqdn \| sort -event_count' |
| 6 | 2025-12-03 01:20:23.9 | kimj | sear | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw |
| 5 | 94 | oe | ch | "ComputerName=(?<fqdn>[^,\s]+)" \| stats count as event_count b |
| 4 | | | | y fqdn \| sort -event_count' |
| 6 | 2025-12-03 01:19:54.0 | kimj | sear | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw |
| 5 | 43 | oe | ch | "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| so |
| 5 | | | | rt fqdn' |
| 6 | 2025-12-03 01:19:49.6 | kimj | sear | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw |
| 5 | 33 | oe | ch | "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| so |
| 6 | | | | rt fqdn' |
| 6 | 2025-12-03 01:19:24.0 | kimj | sear | ' search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s] |
| 5 | 32 | oe | ch | *)" \| eval windows_edition = lower(' |
| 7 | | | | |

| | _time | user | action | search |
|---|---|---|---|---|
| 65228 | 2025-12-03 01:19:24.022 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| join type=inner fqdn [ search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 65219 | 2025-12-03 01:18:58.877 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| join type=inner fqdn [ search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 66070 | 2025-12-03 01:18:24.107 | kimjoe | search | ' search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 66061 | 2025-12-03 01:18:24.098 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| join type=inner fqdn [ search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 66042 | 2025-12-03 01:18:24.084 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^,\s]+)" \| stats count by computer \| sort computer' |
| 66033 | 2025-12-03 01:18:23.252 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| join type=inner fqdn [ search index=botsv3 \| rex "(?i)(windows\s+(10\|server)[^\s]*)" \| eval windows_edition = lower(' |
| 66014 | 2025-12-03 01:18:06.476 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<computer>[^,\s]+)" \| stats count by computer \| sort computer' |

| | _time | user | action | search |
|---|---|---|---|---|
| 66 | 2025-12-03 01:17:54.101 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| rex field=_raw "(?i)windows \s+(?<version>[0-9\.]+\|server[^\s]*)" \| where isnotnull(version) \| stats values(version) as versions by fqdn' |
| 66 | 2025-12-03 01:17:54.088 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| sort fqdn' |
| 67 | 2025-12-03 01:17:54.073 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| stats count as event_count by fqdn \| sort -event_count' |
| 68 | 2025-12-03 01:17:49.657 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| rex field=_raw "(?i)windows \s+(?<version>[0-9\.]+\|server[^\s]*)" \| where isnotnull(version) \| stats values(version) as versions by fqdn' |
| 69 | 2025-12-03 01:17:38.764 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| dedup fqdn \| table fqdn \| sort fqdn' |
| 70 | 2025-12-03 01:17:24.125 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\\.]+)\.(?<domain>[^\s]+)" \| eval full_fqdn = fqdn . "." . domain \| stats count as event_count by full_fqdn \| sort full_fqdn' |
| 71 | 2025-12-03 01:17:24.006 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| rex field=_raw "BuildNumber=(?<build>[^\s]+)" \| where isnotnull(build) \| stats values(build) as build_numbers by fqdn \| stats count as host_count by build_numbers \| sort host_count' |

| | _time | user | action | search |
|---|---|---|---|---|
| 6 | 2025-12-03 01:17:23.036 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^,\s]+)" \| stats count as event_count by fqdn \| sort -event_count' |
| 7 | 2025-12-03 01:17:08.902 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\\.]+)\.(?<domain>[^\s]+)" \| eval full_fqdn = fqdn . "." . domain \| stats count as event_count by full_fqdn \| sort full_fqdn' |
| 8 | 2025-12-03 01:16:54.494 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| rex field=_raw "BuildNumber=(?<build>[^\s]+)" \| where isnotnull(build) \| stats values(build) as build_numbers by fqdn \| stats count as host_count by build_numbers \| sort host_count' |
| 9 | 2025-12-03 01:16:54.087 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| search "Windows" AND "Version" \| rex field=_raw "Version\s+(?<version>[^\s]+)" \| stats values(version) as versions by fqdn' |
| 10 | 2025-12-03 01:16:54.073 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn \| sort fqdn' |
| 11 | 2025-12-03 01:16:44.046 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| search "Windows" AND "Version" \| rex field=_raw "Version\s+(?<version>[^\s]+)" \| stats values(version) as versions by fqdn' |
| 12 | 2025-12-03 01:16:29.009 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:* \| rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" \| stats count by fqdn \| sort fqdn' |

| | _time | user | action | search |
|---|---|---|---|---|
| 67 | 2025-12-03 01:13:54.212 | kimjoe | search | 'search index=botsv3 \| search "Windows" AND ("Enterprise" OR "Professional" OR "Server") \| stats count by host, _raw \| head 20' |
| 68 | 2025-12-03 01:13:28.008 | kimjoe | search | 'search index=botsv3 \| search "Windows" AND ("Enterprise" OR "Professional" OR "Server") \| stats count by host, _raw \| head 20' |
| 68 | 2025-12-03 01:13:23.997 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| stats dc(host) as host_count by os \| sort host_count' |
| 68 | 2025-12-03 01:13:19.396 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| stats dc(host) as host_count by os \| sort host_count' |
| 68 | 2025-12-03 01:12:54.091 | kimjoe | search | '\| search (index=botsv3 sourcetype=WinEventLog:Security EventCode=4624) \| rex field=_raw "TargetDomainName=(?<domain>[^\\s]+)" \| stats values(domain) as domain by host' |
| 68 | 2025-12-03 01:12:54.081 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| stats count by host \| join type=inner host [ search index=botsv3 sourcetype=WinEventLog:Security EventCode=4624 \| rex field=_raw "TargetDomainName=(?<domain>[^\s]+)" \| stats values(domain) as domain by host ] \| eval fqdn = host . "." . domain \| table fqdn' |
| 68 | 2025-12-03 01:12:54.056 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| dedup host \| table host' |

| | _time | user | action | search |
|---|---|---|---|---|
| 6 | 2025-12-03 01:12:54.039 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| where os="Microsoft" \| dedup host \| table host' |
| 6 | 2025-12-03 01:12:54.026 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| where os="Microsoft Windows 10 Pro" \| dedup host \| table host' |
| 6 | 2025-12-03 01:12:50.965 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| rex field=_raw "ComputerName=(?<host>[^\s]+)" \| stats count by host \| join type=inner host [ search index=botsv3 sourcetype=WinEventLog:Security EventCode=4624 \| rex field=_raw "TargetDomainName=(?<domain>[^\s]+)" \| stats values(domain) as domain by host ] \| eval fqdn = host . "." . domain \| table fqdn' |
| 6 | 2025-12-03 01:12:41.967 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| dedup host \| table host' |
| 6 | 2025-12-03 01:12:33.522 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| where os="Microsoft" \| dedup host \| table host' |
| 6 | 2025-12-03 01:12:27.412 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| where os="Microsoft Windows 10 Pro" \| dedup host \| table host' |
| 6 | 2025-12-03 01:12:24.003 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| where os="Microsoft Windows 10 Pro" # Replace with actual unique OS \| dedup host \| table host' |

| | _time | user | action | search |
|---|---|---|---|---|
| 693 | 2025-12-03 01:12:06.889 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| where os="Microsoft Windows 10 Pro" # Replace with actual unique OS \| dedup host \| table host' |
| 694 | 2025-12-03 01:11:54.017 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| stats dc(host) as host_count by os \| sort host_count' |
| 695 | 2025-12-03 01:11:50.382 | kimjoe | search | 'search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| stats dc(host) as host_count by os \| sort host_count' |
| 696 | 2025-12-03 01:11:24.067 | kimjoe | search | '\| search (index=botsv3 sourcetype=osquery:results name="os_version") \| spath \| eval os=((((columns . name) . " ") . columns) . version) \| dedup host \| table host, os' |
| 697 | 2025-12-03 01:11:24.049 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| dedup host \| stats count by host \| join type=left host [ search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| dedup host \| table host, os ] \| stats count as host_count by os \| sort host_count' |
| 698 | 2025-12-03 01:11:24.027 | kimjoe | search | 'search index=botsv3 sourcetype="osquery:results" \| spath \| search name="os_version" \| eval windows_edition = columns.name . " " . columns.version \| stats dc(host) as host_count by windows_edition \| sort host_count' |
| 699 | 2025-12-03 01:11:24.008 | kimjoe | search | 'search index=botsv3 sourcetype="osquery:results" \| spath \| search name="os_version" OR name="windows_info" \| table host, columns.name, columns.version, columns.platform, columns.build' |

| | _time | user | action | search |
|---|---|---|---|---|
| 70 | 2025-12-03 01:11:15.614 | kimjoe | search | 'search index=botsv3 sourcetype=WinEventLog:System \| dedup host \| stats count by host \| join type=left host [ search index=botsv3 sourcetype=osquery:results name="os_version" \| spath \| eval os = columns.name . " " . columns.version \| dedup host \| table host, os ] \| stats count as host_count by os \| sort host_count' |