

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)

		user	action	search	
		▲	▲	▲	
		↙	↙	↙	↙
7	2025-12-03 01:11:02.5	kimj	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'	
0	63	oe	h		
1					
7	2025-12-03 01:10:51.0	kimj	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'	
0	86	oe	h		
2					
7	2025-12-03 01:10:24.0	kimj	search	'search index=botsv3 sourcetype="osquery:results" search "*windows*" OR "*os*" OR "*version*" head 10 table host, name, columns'	
0	25	oe	h		
3					

		user	action	search
_time		♦	♦	♦
7	2025-12-03 01:10:24.0	kimj	search	'search index=botsv3 sourcetype=hardware rex max_match=0 field=_raw "(?<key>[A-Z_]+)\s+(?<value>.+)" eval key = trim(key), value = trim(value) search key="*OS*" OR key="*os*" OR key="*windows*" OR key="*WINDOWS*" stats values(value) as os_info by host'
0	11	oe	h	
4				
7	2025-12-03 01:10:16.6	kimj	search	'search index=botsv3 sourcetype="osquery:results" search "*windows*" OR "*os*" OR "*version*" head 10 table host, name, columns'
0	42	oe	h	
5				
7	2025-12-03 01:09:57.5	kimj	search	'search index=botsv3 sourcetype=hardware rex max_match=0 field=_raw "(?<key>[A-Z_]+)\s+(?<value>.+)" eval key = trim(key), value = trim(value) search key="*OS*" OR key="*os*" OR key="*windows*" OR key="*WINDOWS*" stats values(value) as os_info by host'
0	62	oe	h	
6				
7	2025-12-03 01:05:24.0	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
0	14	oe	h	
7				
7	2025-12-03 01:05:16.9	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
0	01	oe	h	
8				
7	2025-12-03 01:04:54.0	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype = "host" OR sourcetype = "computer" OR sourcetype = "asset" table sourcetype'
0	32	oe	h	
9				
7	2025-12-03 01:04:27.1	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype = "host" OR sourcetype = "computer" OR sourcetype = "asset" table sourcetype'
1	46	oe	h	
0				

		user	action	search
_time		↓	↓	↓
7	2025-12-03 01:03:53.9	kimj	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype ="*system*" OR sourcetype="*wmi*" head 5 table sourcetype, host, *'
1	98	oe	h	
1				
7	2025-12-03 01:03:52.8	kimj	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype ="*system*" OR sourcetype="*wmi*" head 5 table sourcetype, host, *'
1	17	oe	h	
2				
7	2025-12-03 01:03:24.1	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
1	18	oe	h	
3				
7	2025-12-03 01:02:54.0	kimj	search	'search index=botsv3 where isnotnull(os) stats dc(host) as host_count by os sort host_count'
1	06	oe	h	
4				
7	2025-12-03 01:01:51.6	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
1	60	oe	h	
5				
7	2025-12-03 01:01:18.7	kimj	search	'search index=botsv3 where isnotnull(os) stats dc(host) as host_count by os sort host_count'
1	47	oe	h	
6				
7	2025-12-03 01:00:54.0	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
1	92	oe	h	
7				
7	2025-12-03 01:00:24.0	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype ="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*" table sourcetype'
1	20	oe	h	
8				

		user	action	search
_time		↓	↓	↓
7	2025-12-03 01:00:05.0	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype ="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*" table sourcetype'
1	99	oe	h	
9				
7	2025-12-03 00:59:54.0	kimj	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype ="*system*" OR sourcetype="*wmi*" head 5 table sourcetype, host, *'
2	15	oe	h	
0				
7	2025-12-03 00:59:24.4	kimj	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype ="*system*" OR sourcetype="*wmi*" head 5 table sourcetype, host, *'
2	57	oe	h	
1				
7	2025-12-03 00:59:24.0	kimj	search	'search index=botsv3 where isnotnull(os) stats dc(host) as host_count by os sort host_count'
2	14	oe	h	
2				
7	2025-12-03 00:58:53.2	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
2	11	oe	h	
3				
7	2025-12-03 00:58:24.0	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
2	01	oe	h	
4				
7	2025-12-03 00:57:59.3	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
2	31	oe	h	
5				
7	2025-12-03 00:57:36.7	kimj	search	'search index=botsv3 where isnotnull(os) stats dc(host) as host_count by os sort host_count'
2	10	oe	h	
6				

		user	action	search
_time		↓	↓	↓
7	2025-12-03 00:57:24.0	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
2	11	oe	h	
7				
7	2025-12-03 00:57:20.9	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
2	97	oe	h	
8				
7	2025-12-03 00:56:53.9	kimj	search	'search index=botsv3 where isnotnull(os) stats count by sourcetype, os, host'
2	97	oe	h	
9				
7	2025-12-03 00:55:54.0	kimj	search	'search index=botsv3 sourcetype=hardware dedup host table host, os, version, os_version stats count by os sort count'
3	65	oe	h	
0				
7	2025-12-03 00:55:54.0	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
3	38	oe	h	
1				
7	2025-12-03 00:55:43.7	kimj	search	'search index=botsv3 sourcetype=hardware dedup host table host, os, version, os_version stats count by os sort count'
3	29	oe	h	
2				
7	2025-12-03 00:55:26.0	kimj	search	'search index=botsv3 where isnotnull(os) stats count by sourcetype, os, host'
3	44	oe	h	
3				
7	2025-12-03 00:55:23.9	kimj	search	'search index=botsv3 sourcetype="WinEventLog:*" search EventCode=6005 OR EventCode=6006 head 5 table host, Message'
3	87	oe	h	
4				

		user	action	search
_time		↓	↓	↓
7	2025-12-03 00:54:58.9	kimj	search	'search index=botsv3 sourcetype="WinEventLog:*" search EventCode=6005 OR EventCode=6006 head 5 table host, Message'
3	52	oe	h	
5				
7	2025-12-03 00:54:54.0	kimj	search	'search index=botsv3 sourcetype="WinEventLog:*" search EventCode=6005 OR EventCode=6006 # System startup/shutdown events often have OS info head 5 table host, Message'
3	14	oe	h	
6				
7	2025-12-03 00:54:53.9	kimj	search	'search index=botsv3 sourcetype=hardware stats values(os) by host'
3	96	oe	h	
7				
7	2025-12-03 00:54:50.9	kimj	search	'search index=botsv3 sourcetype="WinEventLog:*" search EventCode=6005 OR EventCode=6006 # System startup/shutdown events often have OS info head 5 table host, Message'
3	62	oe	h	
8				
7	2025-12-03 00:54:41.8	kimj	search	'search index=botsv3 sourcetype=hardware stats values(os) by host'
3	00	oe	h	
9				
7	2025-12-03 00:54:18.9	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
4	06	oe	h	
0				
7	2025-12-02 15:31:28.5	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
4	71	oe	h	
1				
7	2025-12-02 15:30:58.5	kimj	search	'search index=botsv3 where isnotnull(os) stats dc(host) as host_count by os sort host_count'
4	91	oe	h	
2				

		user	action	search
_time		user	action	search
7	2025-12-02 15:29:32.3	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
4	82	oe	h	
3				
7	2025-12-02 15:28:38.7	kimj	search	'search index=botsv3 where isnotnull(os) stats dc(host) as host_count by os sort host_count'
4	52	oe	h	
4				
7	2025-12-02 15:28:28.5	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
4	56	oe	h	
5				
7	2025-12-02 15:28:28.5	kimj	search	'search index=botsv3 sourcetype=hardware os="Windows 10 Professional" dedup host table host'
4	35	oe	h	
6				
7	2025-12-02 15:28:26.3	kimj	search	'search index=botsv3 sourcetype=hardware stats dc(host) as host_count by os sort host_count'
4	02	oe	h	
7				
7	2025-12-02 15:28:17.6	kimj	search	'search index=botsv3 sourcetype=hardware os="Windows 10 Professional" dedup host table host'
4	53	oe	h	
8				
7	2025-12-02 15:27:58.5	kimj	search	'search index=botsv3 sourcetype=hardware dedup host table host, os, version, os_version stats count by os sort count'
4	22	oe	h	
9				
7	2025-12-02 15:27:58.5	kimj	search	'search # Query 3: Check for common Windows inventory tools index=botsv3 sourcetype="*wmi*" OR sourcetype="*sccm*" OR sourcetype="*lan*" head 10 table sourcetype, host, *'
5	06	oe	h	
0				

		user	action	search
_time		user	action	search
7	2025-12-02 15:27:58.4	kimj	search	'search # Query 2: Look for Windows versions index=botsv3 search "Windows *" AND "Enterprise" OR "Professional" OR "Server" stats count by sourcetype, host, _raw'
5	87	oe	h	
1				
7	2025-12-02 15:27:48.8	kimj	search	'search index=botsv3 sourcetype=hardware dedup host table host, os, version, os_version stats count by os sort count'
5	91	oe	h	
2				
7	2025-12-02 15:27:37.7	kimj	search	'search # Query 3: Check for common Windows inventory tools index=botsv3 sourcetype="*wmi*" OR sourcetype="*sccm*" OR sourcetype="*lan*" head 10 table sourcetype, host, *'
5	73	oe	h	
3				
7	2025-12-02 15:27:29.6	kimj	search	'search # Query 2: Look for Windows versions index=botsv3 search "Windows *" AND "Enterprise" OR "Professional" OR "Server" stats count by sourcetype, host, _raw'
5	49	oe	h	
4				
7	2025-12-02 15:27:28.5	kimj	search	'search # Query 1: Check all sourcetypes for OS field index=botsv3 where isnotnull(os) stats count by sourcetype, os, host'
5	37	oe	h	
5				
7	2025-12-02 15:27:28.5	kimj	search	'search index=botsv3 sourcetype="WinEventLog:*" search EventCode=6005 OR EventCode=6006 head 5 table host, Message'
5	23	oe	h	
6				
7	2025-12-02 15:27:28.5	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
5	07	oe	h	
7				
7	2025-12-02 15:27:18.8	kimj	search	'search # Query 1: Check all sourcetypes for OS field index=botsv3 where isnotnull(os) stats count by sourcetype, os, host'
5	41	oe	h	
8				

		user	action	search
_time		↓	↓	↓
7	2025-12-02 15:27:04.9	kimj	search	'search index=botsv3 sourcetype="WinEventLog:*" search EventCode=6005 OR EventCode=6006 head 5 table host, Message'
5	87	oe	h	
9				
7	2025-12-02 15:26:58.4	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype ="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*" table sourcetype'
6	83	oe	h	
0				
7	2025-12-02 15:26:58.4	kimj	search	'search index=botsv3 sourcetype=hardware stats values(os) by host'
6	71	oe	h	
1				
7	2025-12-02 15:26:44.1	kimj	search	'search index=botsv3 sourcetype=hardware stats values(os) by host'
6	76	oe	h	
2				
7	2025-12-02 15:26:30.8	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype ="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*" table sourcetype'
6	60	oe	h	
3				
7	2025-12-02 15:26:28.4	kimj	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype ="*system*" OR sourcetype="*wmi*" head 5 table sourcetype, host, *'
6	83	oe	h	
4				
7	2025-12-02 15:26:17.1	kimj	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype ="*system*" OR sourcetype="*wmi*" head 5 table sourcetype, host, *'
6	78	oe	h	
5				
7	2025-12-02 15:26:05.7	kimj	search	'search index=botsv3 search "*windows*" OR "*os*" OR "*operating*" stats count by sourcetype sort -count'
6	78	oe	h	
6				

		user	action	search
_time		↓	↓	↓
7	2025-12-02 15:25:58.4	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype =*windows* OR sourcetype=*win* OR sourcetype=*host* OR sourcetype=*os* table sourcetype'
6	84	oe	h	
7	2025-12-02 15:25:32.8	kimj	search	' metadata type=sourcetypes index=botsv3 search sourcetype =*windows* OR sourcetype=*win* OR sourcetype=*host* OR sourcetype=*os* table sourcetype'
6	14	oe	h	
8				
7	2025-12-02 15:24:28.4	kimj	search	'search index=botsv3 sourcetype=winhostmon head 20 table
6	96	oe	h	*
9				
7	2025-12-02 15:24:28.4	kimj	search	'search index=botsv3 sourcetype=winhostmon head 20 table
7	81	oe	h	*
0				
7	2025-12-02 15:24:17.6	kimj	search	'search index=botsv3 sourcetype=winhostmon head 20 table
7	71	oe	h	*
1				
7	2025-12-02 15:23:59.4	kimj	search	'search index=botsv3 sourcetype=winhostmon head 20 table
7	08	oe	h	*
2				
7	2025-12-02 15:23:28.5	kimj	search	'search index=botsv3 sourcetype=winhostmon head 1 fieldsu
7	67	oe	h	mmmary table field, count search field=*os* OR field=*v
3				ersion* OR field=*windows* OR field=*host*'
7	2025-12-02 15:23:24.6	kimj	search	'search index=botsv3 sourcetype=winhostmon head 1 fieldsu
7	36	oe	h	mmmary table field, count search field=*os* OR field=*v
4				ersion* OR field=*windows* OR field=*host*'

		user	action	search
7	2025-12-02 15:22:58.6	kimj	search	'search index=botsv3 sourcetype=winhostmon stats count'
7	82	oe	h	
5				
7	2025-12-02 15:22:22.7	kimj	search	'search index=botsv3 sourcetype=winhostmon stats count'
7	63	oe	h	
6				
7	2025-12-02 15:21:58.5	kimj	search	'typeahead prefix="index=botsv3 sourcetype=winhostmon" max_time="1" count="50" use_cache=1'
7	04	oe	h	
7				
7	2025-12-02 15:21:58.4	kimj	search	'search index=botsv3 sourcetype=winhostmon foreach os OperatingSystem os_version version OS operating_system windows_edition [eval field_value = <<FIELD>> where isnotnull(field_value) stats dc(host) as host_count by field_value rename field_value as os_type] sort host_count'
7	93	oe	h	
8				
7	2025-12-02 15:21:53.6	kimj	search	'search index=botsv3 sourcetype=winhostmon foreach os OperatingSystem os_version version OS operating_system windows_edition [eval field_value = <<FIELD>> where isnotnull(field_value) stats dc(host) as host_count by field_value rename field_value as os_type] sort host_count'
7	08	oe	h	
9				
7	2025-12-02 15:21:28.5	kimj	search	'search index=botsv3 sourcetype=winhostmon head 20 table *'
8	88	oe	h	
0				
7	2025-12-02 15:21:08.7	kimj	search	'search index=botsv3 sourcetype=winhostmon head 20 table *'
8	88	oe	h	
1				

		user	action	search
_time		user	action	search
7	2025-12-02 15:20:58.5	kimj	search	'search index=botsv3 sourcetype=winhostmon fieldsummary table field, count search field="*os*" OR field="*version*" OR field="*windows*" OR field="*host*'"
8	42	oe	search	
2				
7	2025-12-02 15:20:58.4	kimj	search	'search index=botsv3 sourcetype=winhostmon head 1 fields summary table field, count search field="*os*" OR field="*version*" OR field="*windows*" OR field="*host*'"
8	71	oe	search	
3				
7	2025-12-02 15:20:49.7	kimj	search	'search index=botsv3 sourcetype=winhostmon fieldsummary table field, count search field="*os*" OR field="*version*" OR field="*windows*" OR field="*host*'"
8	06	oe	search	
4				
7	2025-12-02 15:20:48.9	kimj	search	'typeahead prefix="index=botsv3 sourcetype=winhostmon" max_time="1" count="50" use_cache=1'
8	54	oe	search	
5				
7	2025-12-02 15:20:35.5	kimj	search	'search index=botsv3 sourcetype=winhostmon head 1 fields summary table field, count search field="*os*" OR field="*version*" OR field="*windows*" OR field="*host*'"
8	22	oe	search	
6				
7	2025-12-02 15:20:28.6	kimj	search	'search index=botsv3 sourcetype=winhostmon stats count'
8	20	oe	search	
7				
7	2025-12-02 15:20:21.0	kimj	search	'search index=botsv3 sourcetype=winhostmon stats count'
8	24	oe	search	
8				
7	2025-12-02 15:18:28.5	kimj	search	' search (index=botsv3 sourcetype=winhostmon) table host, os'
8	25	oe	search	
9				

		user	action	search
_time	↓	↓	↓	↓
7 07	2025-12-02 15:18:28.5	kimjoe	search	'search index=botsv3 sourcetype=winhostmon Manufacturer=Intel stats dc(host) as host_count by os where host_count=1 join type=inner os [search index=botsv3 sourcetype=winhostmon table host, os] table host, os'
9 02	2025-12-02 15:18:07.1	kimjoe	search	'search index=botsv3 sourcetype=winhostmon Manufacturer=Intel stats dc(host) as host_count by os where host_count=1 join type=inner os [search index=botsv3 sourcetype=winhostmon table host, os] table host, os'
9 70	2025-12-02 15:16:28.5	kimjoe	search	' search (index=botsv3 sourcetype=winhostmon) table host, os'
9 48	2025-12-02 15:16:28.5	kimjoe	search	'search index=botsv3 sourcetype=winhostmon stats dc(host) as host_count by os where host_count=1 join type=inner os [search index=botsv3 sourcetype=winhostmon table host, os] table host, os'
9 16	2025-12-02 15:16:02.5	kimjoe	search	'search index=botsv3 sourcetype=winhostmon stats dc(host) as host_count by os join type=inner os [search index=botsv3 sourcetype=winhostmon table host, os] table host, os'
9 80	2025-12-02 15:15:58.4	kimjoe	search	'search index=botsv3 sourcetype=winhostmon dedup host, os stats count as host_count by os sort host_count'
9 41	2025-12-02 15:15:29.5	kimjoe	search	'search index=botsv3 sourcetype=winhostmon dedup host, os stats count as host_count by os sort host_count'

		user	action	search	
7	2025-12-02 15:15:28.5	kimj	search	'typeahead prefix="index=botsv3 sourcetype=winhostmon os" max	
9	16	oe	h	_time="1" count="50" use_cache=1'	
7					
7	2025-12-02 15:15:28.5	kimj	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pr	
9	06	oe	h	o" dedup host table host'	
8					
7	2025-12-02 15:15:28.4	kimj	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pr	
9	93	oe	h	o" # Replace with actual OS dedup host table host'	
9					
8	2025-12-02 15:15:28.4	kimj	search	'search index=botsv3 sourcetype=winhostmon dedup host tab	
0	79	oe	h	le host'	
0					