

# 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)









	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
7 0 1	2025-12-03 01:11:02.563	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'
7 0 2	2025-12-03 01:10:51.086	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'
7 0 3	2025-12-03 01:10:24.025	kimjoe	search	'search index=botsv3 sourcetype="osquery:results"   search "*windows*" OR "*os*" OR "*version*"   head 10   table host, name, columns'









	_time ↕	user ↕ 	action ↕ 	search ↕ 
704	2025-12-03 01:10:24.011	kimjoe	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'
705	2025-12-03 01:10:16.642	kimjoe	search	'search index=botsv3 sourcetype="osquery:results"   search "*windows*" OR "*os*" OR "*version*"   head 10   table host, name, columns'
706	2025-12-03 01:09:57.562	kimjoe	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'
707	2025-12-03 01:05:24.014	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats dc(host) as host_count by os   sort host_count'
708	2025-12-03 01:05:16.901	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats dc(host) as host_count by os   sort host_count'
709	2025-12-03 01:04:54.032	kimjoe	search	'  metadata type=sourcetypes index=botsv3   search sourcetype="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*"   table sourcetype'
710	2025-12-03 01:04:27.146	kimjoe	search	'  metadata type=sourcetypes index=botsv3   search sourcetype="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*"   table sourcetype'









	<div><div><div></div><div>_time</div><div></div></div></div>	<div><div><div></div><div>user</div><div></div></div></div>	<div><div><div></div><div>action</div><div></div></div></div>	<div><div><div></div><div>search</div><div></div></div></div>
711	2025-12-03 01:03:53.998	kimjoe	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype="*system*" OR sourcetype="*wmi*"   head 5   table sourcetype, host, *'
712	2025-12-03 01:03:52.817	kimjoe	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype="*system*" OR sourcetype="*wmi*"   head 5   table sourcetype, host, *'
713	2025-12-03 01:03:24.118	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
714	2025-12-03 01:02:54.006	kimjoe	search	'search index=botsv3   where isnotnull(os)   stats dc(host) as host_count by os   sort host_count'
715	2025-12-03 01:01:51.660	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
716	2025-12-03 01:01:18.747	kimjoe	search	'search index=botsv3   where isnotnull(os)   stats dc(host) as host_count by os   sort host_count'
717	2025-12-03 01:00:54.092	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
718	2025-12-03 01:00:24.020	kimjoe	search	'  metadata type=sourcetypes index=botsv3   search sourcetype="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*"   table sourcetype'

	<div><div></div><div>_time ↕</div></div>	<div><div></div><div>user ↕</div></div>	<div><div></div><div>action ↕</div></div>	<div><div></div><div>search ↕</div></div>
719	2025-12-03 01:00:05.099	kimjoe	search	'  metadata type=sourcetypes index=botsv3   search sourcetype="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*"   table sourcetype'
720	2025-12-03 00:59:54.015	kimjoe	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype="*system*" OR sourcetype="*wmi*"   head 5   table sourcetype, host, *'
721	2025-12-03 00:59:24.457	kimjoe	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype="*system*" OR sourcetype="*wmi*"   head 5   table sourcetype, host, *'
722	2025-12-03 00:59:24.014	kimjoe	search	'search index=botsv3   where isnotnull(os)   stats dc(host) as host_count by os   sort host_count'
723	2025-12-03 00:58:53.211	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
724	2025-12-03 00:58:24.001	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats dc(host) as host_count by os   sort host_count'
725	2025-12-03 00:57:59.331	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats dc(host) as host_count by os   sort host_count'
726	2025-12-03 00:57:36.710	kimjoe	search	'search index=botsv3   where isnotnull(os)   stats dc(host) as host_count by os   sort host_count'






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









	 _time 	user  	action  	search  
735	2025-12-03 00:54:58.952	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*"   search EventCode=6005 OR EventCode=6006   head 5   table host, Message'
736	2025-12-03 00:54:54.014	kimjoe	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'
737	2025-12-03 00:54:53.996	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats values(os) by host'
738	2025-12-03 00:54:50.962	kimjoe	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'
739	2025-12-03 00:54:41.800	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats values(os) by host'
740	2025-12-03 00:54:18.906	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
741	2025-12-02 15:31:28.571	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
742	2025-12-02 15:30:58.591	kimjoe	search	'search index=botsv3   where isnotnull(os)   stats dc(host) as host_count by os   sort host_count'







	 _time 	 user 	 action 	 search 
743	2025-12-02 15:29:32.382	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
744	2025-12-02 15:28:38.752	kimjoe	search	'search index=botsv3   where isnotnull(os)   stats dc(host) as host_count by os   sort host_count'
745	2025-12-02 15:28:28.556	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats dc(host) as host_count by os   sort host_count'
746	2025-12-02 15:28:28.535	kimjoe	search	'search index=botsv3 sourcetype=hardware os="Windows 10 Professional"   dedup host   table host'
747	2025-12-02 15:28:26.302	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats dc(host) as host_count by os   sort host_count'
748	2025-12-02 15:28:17.653	kimjoe	search	'search index=botsv3 sourcetype=hardware os="Windows 10 Professional"   dedup host   table host'
749	2025-12-02 15:27:58.522	kimjoe	search	'search index=botsv3 sourcetype=hardware   dedup host   table host, os, version, os_version   stats count by os   sort count'
750	2025-12-02 15:27:58.506	kimjoe	search	'search # Query 3: Check for common Windows inventory tools index=botsv3 sourcetype="*wmi*" OR sourcetype="*scm*" OR sourcetype="*lan*"   head 10   table sourcetype, host, *'

	 _time 	 user 	 action 	 search 
751	2025-12-02 15:27:58.487	kimjoe	search	'search # Query 2: Look for Windows versions index=botsv3   search "Windows *" AND "Enterprise" OR "Professional" OR "Server"   stats count by sourcetype, host, _raw'
752	2025-12-02 15:27:48.891	kimjoe	search	'search index=botsv3 sourcetype=hardware   dedup host   table host, os, version, os_version   stats count by os   sort count'
753	2025-12-02 15:27:37.773	kimjoe	search	'search # Query 3: Check for common Windows inventory tools index=botsv3 sourcetype="*wmi*" OR sourcetype="*scm*" OR sourcetype="*lan*"   head 10   table sourcetype, host, *'
754	2025-12-02 15:27:29.649	kimjoe	search	'search # Query 2: Look for Windows versions index=botsv3   search "Windows *" AND "Enterprise" OR "Professional" OR "Server"   stats count by sourcetype, host, _raw'
755	2025-12-02 15:27:28.537	kimjoe	search	'search # Query 1: Check all sourcetypes for OS field index=botsv3   where isnotnull(os)   stats count by sourcetype, os, host'
756	2025-12-02 15:27:28.523	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*"   search EventCode=6005 OR EventCode=6006   head 5   table host, Message'
757	2025-12-02 15:27:28.507	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'
758	2025-12-02 15:27:18.841	kimjoe	search	'search # Query 1: Check all sourcetypes for OS field index=botsv3   where isnotnull(os)   stats count by sourcetype, os, host'

	_time ↕	user ↕ 	action ↕ 	search ↕ 
759	2025-12-02 15:27:04.987	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*"   search EventCode=6005 OR EventCode=6006   head 5   table host, Message'
760	2025-12-02 15:26:58.483	kimjoe	search	'  metadata type=sourcetypes index=botsv3   search sourcetype="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*"   table sourcetype'
761	2025-12-02 15:26:58.471	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats values(os) by host'
762	2025-12-02 15:26:44.176	kimjoe	search	'search index=botsv3 sourcetype=hardware   stats values(os) by host'
763	2025-12-02 15:26:30.860	kimjoe	search	'  metadata type=sourcetypes index=botsv3   search sourcetype="*host*" OR sourcetype="*computer*" OR sourcetype="*asset*"   table sourcetype'
764	2025-12-02 15:26:28.483	kimjoe	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype="*system*" OR sourcetype="*wmi*"   head 5   table source_type, host, *'
765	2025-12-02 15:26:17.178	kimjoe	search	'search index=botsv3 sourcetype="*inventory*" OR sourcetype="*system*" OR sourcetype="*wmi*"   head 5   table source_type, host, *'
766	2025-12-02 15:26:05.778	kimjoe	search	'search index=botsv3   search "*windows*" OR "*os*" OR "*operating*"   stats count by sourcetype   sort -count'

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

	 _time 	 user 	 action 	 search 
7 7 5	2025-12-02 15:22:58.6 82	kimj oe	searc h	'search index=botsv3 sourcetype=winhostmon   stats count'
7 7 6	2025-12-02 15:22:22.7 63	kimj oe	searc h	'search index=botsv3 sourcetype=winhostmon   stats count'
7 7 7	2025-12-02 15:21:58.5 04	kimj oe	searc h	'typeahead prefix="index=botsv3 sourcetype=winhostmon" max_time="1" count="50" use_cache=1'
7 7 8	2025-12-02 15:21:58.4 93	kimj oe	searc h	'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 7 9	2025-12-02 15:21:53.6 08	kimj oe	searc h	'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 8 0	2025-12-02 15:21:28.5 88	kimj oe	searc h	'search index=botsv3 sourcetype=winhostmon   head 20   table *'
7 8 1	2025-12-02 15:21:08.7 88	kimj oe	searc h	'search index=botsv3 sourcetype=winhostmon   head 20   table *'

						
	_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	h			
2						
7	2025-12-02 15:20:58.4	kimj	search	'search index=botsv3 sourcetype=winhostmon   head 1   fieldsummary   table field, count   search field="*os*" OR field="*version*" OR field="*windows*" OR field="*host*"'		
8	71	oe	h			
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	h			
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	h			
5						
7	2025-12-02 15:20:35.5	kimj	search	'search index=botsv3 sourcetype=winhostmon   head 1   fieldsummary   table field, count   search field="*os*" OR field="*version*" OR field="*windows*" OR field="*host*"'		
8	22	oe	h			
6						
7	2025-12-02 15:20:28.6	kimj	search	'search index=botsv3 sourcetype=winhostmon   stats count'		
8	20	oe	h			
7						
7	2025-12-02 15:20:21.0	kimj	search	'search index=botsv3 sourcetype=winhostmon   stats count'		
8	24	oe	h			
8						
7	2025-12-02 15:18:28.5	kimj	search	'  search (index=botsv3 sourcetype=winhostmon)   table host, os'		
8	25	oe	h			
9						

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
7 9 0	2025-12-02 15:18:28.507	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'
7 9 1	2025-12-02 15:18:07.102	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'
7 9 2	2025-12-02 15:16:28.570	kimjoe	search	'  search (index=botsv3 sourcetype=winhostmon)   table host, os'
7 9 3	2025-12-02 15:16:28.548	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'
7 9 4	2025-12-02 15:16:02.516	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'
7 9 5	2025-12-02 15:15:58.480	kimjoe	search	'search index=botsv3 sourcetype=winhostmon   dedup host, os   stats count as host_count by os   sort host_count'
7 9 6	2025-12-02 15:15:29.541	kimjoe	search	'search index=botsv3 sourcetype=winhostmon   dedup host, os   stats count as host_count by os   sort host_count'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
797	2025-12-02 15:15:28.516	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=winhostmon os" max _time="1" count="50" use_cache=1'
798	2025-12-02 15:15:28.506	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pro"   dedup host   table host'
799	2025-12-02 15:15:28.493	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pro" # Replace with actual OS   dedup host   table host'
800	2025-12-02 15:15:28.479	kimjoe	search	'search index=botsv3 sourcetype=winhostmon   dedup host   table host'