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
801	2025-12-02 15:15:22.449	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pro" | dedup host | table host'
802	2025-12-02 15:15:12.781	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pro" # Replace with actual OS | dedup host | table host'
803	2025-12-02 15:15:03.010	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host | table host'
804	2025-12-02 15:14:28.590	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host | table host'

	_time	user	action	search
805	2025-12-02 15:14:03.026	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host | table host'
806	2025-12-02 15:14:01.737	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=winhostmon os" max_time="1" count="50" use_cache=1'
807	2025-12-02 15:13:58.687	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="1" | dedup host | table host'
808	2025-12-02 15:13:58.672	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="[THE_UNIQUE_OS]" | dedup host | table host'
809	2025-12-02 15:13:58.645	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count'
810	2025-12-02 15:13:55.249	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="1" | dedup host | table host'
811	2025-12-02 15:13:44.457	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="[THE_UNIQUE_OS]" | dedup host | table host'
812	2025-12-02 15:13:31.300	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count'

	_time	user	action	search
813	2025-12-02 15:13:28.537	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field | head 10'
814	2025-12-02 15:13:04.105	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field | head 10'
815	2025-12-02 15:12:58.597	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'
816	2025-12-02 15:12:58.536	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
817	2025-12-02 15:12:51.398	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'
818	2025-12-02 15:12:33.235	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
819	2025-12-02 15:12:28.636	kimjoe	search	'| search (index=botsv3 sourcetype=winhostmon) | table host, os'
820	2025-12-02 15:12:28.616	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'

	_time	user	action	search
821	2025-12-02 15:12:28.553	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'
822	2025-12-02 15:12:28.488	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | eventstats count as os_count by os | where os_count=1 | table host, os'
823	2025-12-02 15:12:17.863	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'
824	2025-12-02 15:12:05.312	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'
825	2025-12-02 15:11:54.552	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | eventstats count as os_count by os | where os_count=1 | table host, os'
826	2025-12-02 15:11:28.525	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | stats count as host_count by os | sort host_count'
827	2025-12-02 15:11:28.499	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pro" # Replace with actual OS | dedup host | table host'
828	2025-12-02 15:11:14.488	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | stats count as host_count by os | sort host_count'

	_time	user	action	search
829	2025-12-02 15:11:04.824	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="Windows 10 Pro" # Replace with actual OS | dedup host | table host'
830	2025-12-02 15:10:58.560	kimjoe	search	'| search (index=botsv3 sourcetype=winhostmon) | table host, os'
831	2025-12-02 15:10:58.543	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, host_count'
832	2025-12-02 15:10:38.550	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, host_count'
833	2025-12-02 15:10:28.545	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host | table host | head 10'
834	2025-12-02 15:10:28.528	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | eval windows_edition = coalesce(os, os_version, version) | stats dc(host) as host_count by windows_edition | sort host_count'
835	2025-12-02 15:10:17.910	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host | table host | head 10'
836	2025-12-02 15:10:04.774	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | eval windows_edition = coalesce(os, os_version, version) | stats dc(host) as host_count by windows_edition | sort host_count'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>837</td><td>2025-12-02 15:09:58.517</td><td>kimjoe</td><td>search</td><td>'typeahead prefix="index=botsv3 sourcetype=winhostmon" max_time="1" count="50" use_cache=1'</td></tr>
<tr><td>838</td><td>2025-12-02 15:09:58.508</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=winhostmon | dedup host, os | stats values(os) as operating_systems by host | where mvcount(operating_systems) > 1'</td></tr>
<tr><td>839</td><td>2025-12-02 15:09:58.496</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=winhostmon os="windows" | stats dc(host) as unique_hosts'</td></tr>
<tr><td>840</td><td>2025-12-02 15:09:58.481</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=winhostmon os="7" | stats dc(host) as unique_hosts'</td></tr>
<tr><td>841</td><td>2025-12-02 15:09:47.392</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=winhostmon | dedup host, os | stats values(os) as operating_systems by host | where mvcount(operating_systems) > 1'</td></tr>
<tr><td>842</td><td>2025-12-02 15:09:35.179</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=winhostmon os="windows" | stats dc(host) as unique_hosts'</td></tr>
<tr><td>843</td><td>2025-12-02 15:09:28.488</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=winhostmon os="8" | stats dc(host) as unique_hosts'</td></tr>
<tr><td>844</td><td>2025-12-02 15:09:28.487</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=winhostmon os="7" | stats dc(host) as unique_hosts'</td></tr>
</table>

	_time	user	action	search
845	2025-12-02 15:09:28.471	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="5" | stats dc(host) as unique_hosts'
846	2025-12-02 15:09:22.471	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="8" | stats dc(host) as unique_hosts'
847	2025-12-02 15:09:17.600	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="5" | stats dc(host) as unique_hosts'
848	2025-12-02 15:08:58.515	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as unique_hosts'
849	2025-12-02 15:08:58.458	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="[SUSPECTED_UNIQUE_OS]" | stats dc(host) as unique_hosts'
850	2025-12-02 15:08:50.564	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as unique_hosts'
851	2025-12-02 15:08:48.835	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=winhostmon" max_time="1" count="50" use_cache=1'
852	2025-12-02 15:08:30.334	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="[SUSPECTED_UNIQUE_OS]" | stats dc(host) as unique_hosts'

	_time	user	action	search
853	2025-12-02 15:08:28.491	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | stats count as host_count by os | sort host_count'
854	2025-12-02 15:08:28.476	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | eventstats count as os_count by os | where os_count=1 | table host, os'
855	2025-12-02 15:08:15.299	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | stats count as host_count by os | sort host_count'
856	2025-12-02 15:08:04.822	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | dedup host, os | eventstats count as os_count by os | where os_count=1 | table host, os'
857	2025-12-02 15:07:58.589	kimjoe	search	'| search (index=botsv3 sourcetype=winhostmon) | table host, os'
858	2025-12-02 15:07:58.573	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'
859	2025-12-02 15:07:58.513	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="[THE_UNIQUE_OS_HERE]" | table host, os | dedup host'
860	2025-12-02 15:07:58.500	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count | head 5'

	_time	user	action	search
861	2025-12-02 15:07:51.010	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'
862	2025-12-02 15:07:41.812	kimjoe	search	'search index=botsv3 sourcetype=winhostmon os="[THE_UNIQUE_OS_HERE]" | table host, os | dedup host'
863	2025-12-02 15:07:23.504	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count | head 5'
864	2025-12-02 15:06:58.524	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
865	2025-12-02 15:06:40.293	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
866	2025-12-02 15:05:28.524	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
867	2025-12-02 15:05:01.941	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
868	2025-12-02 15:04:58.580	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort -count'

	_time	user	action	search
869	2025-12-02 15:04:58.518	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
870	2025-12-02 15:04:52.142	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort -count'
871	2025-12-02 15:04:41.415	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
872	2025-12-02 15:04:28.584	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'
873	2025-12-02 15:04:28.517	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
874	2025-12-02 15:04:20.060	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'
875	2025-12-02 15:04:05.563	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by os | sort count'
876	2025-12-02 15:03:28.521	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'

	_time	user	action	search
877	2025-12-02 15:03:06.034	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | fieldsummary | search field="*os*" OR field="*version*" OR field="*windows*" | table field'
878	2025-12-02 15:00:58.482	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | head 10 | table host, os, os_version, version'
879	2025-12-02 15:00:42.093	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | head 10 | table host, os, os_version, version'
880	2025-12-02 14:46:58.469	kimjoe	search	'search
881	2025-12-02 14:46:36.242	kimjoe	search	'search
882	2025-12-02 14:45:58.473	kimjoe	search	'search
883	2025-12-02 14:45:48.583	kimjoe	search	'search
884	2025-12-02 14:44:28.482	kimjoe	search	'search

	_time	user	action	search
885	2025-12-02 14:44:24.367	kimjoe	search	'search
886	2025-12-02 14:42:28.470	kimjoe	search	'search
887	2025-12-02 14:42:22.628	kimjoe	search	'search
888	2025-12-02 14:41:28.532	kimjoe	search	'search
889	2025-12-02 14:41:10.146	kimjoe	search	'search
890	2025-12-02 14:37:58.482	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
891	2025-12-02 14:37:45.046	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'
892	2025-12-02 14:35:58.480	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, key, http_method, http_status'

<table>
<tr><th></th><th>_time ⬍</th><th>user ⬍</th><th>action ⬍</th><th>search ⬍</th></tr>
<tr><td>893</td><td>2025-12-02 14:35:28.810</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | head 5 | table _time, bucket, key, http_method, http_status'</td></tr>
<tr><td>894</td><td>2025-12-02 14:35:28.482</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | table _time, bucket, key, http_method, http_status'</td></tr>
<tr><td>895</td><td>2025-12-02 14:35:23.574</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | table _time, bucket, key, http_method, http_status'</td></tr>
<tr><td>896</td><td>2025-12-02 14:34:28.481</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'</td></tr>
<tr><td>897</td><td>2025-12-02 14:34:28.466</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | rex field=key "(?<filename>[^/]+\.\w+)$" | where isnotnull(filename) | stats count by bucket, filename'</td></tr>
<tr><td>898</td><td>2025-12-02 14:34:22.366</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | head 1 | fieldsummary | table field'</td></tr>
<tr><td>899</td><td>2025-12-02 14:34:03.914</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | rex field=key "(?<filename>[^/]+\.\w+)$" | where isnotnull(filename) | stats count by bucket, filename'</td></tr>
<tr><td>900</td><td>2025-12-02 14:33:58.491</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:s3:accesslogs | search "*.txt" | table _time, bucket, key, object, http_method, http_status'</td></tr>
</table>