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
1801	2025-12-01 02:08:19.332	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | stats values(sourcetype)'
1802	2025-12-01 02:08:14.290	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | stats values(sourcetype)'
1803	2025-12-01 02:05:40.532	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail\"" max_time="1" count="50" use_cache=1'
1804	2025-12-01 02:05:10.509	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'
1805	2025-12-01 02:04:43.713	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'
1806	2025-12-01 02:04:40.529	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'

	_time	user	action	search
1807	2025-12-01 02:04:40.518	kimjoe	search	'search index="botsv3" indesourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'
1808	2025-12-01 02:04:34.767	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'
1809	2025-12-01 02:04:33.455	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail\"" max_time="1" count="50" use_cache=1'
1810	2025-12-01 02:04:29.198	kimjoe	search	'search index="botsv3" indesourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'
1811	2025-12-01 02:04:10.517	kimjoe	search	'search index=botsv3 indesourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'
1812	2025-12-01 02:03:43.331	kimjoe	search	'search index=botsv3 indesourcetype="aws:cloudtrail" | stats count by userIdentity.userName | sort userIdentity.userName'
1813	2025-12-01 02:02:40.520	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1814	2025-12-01 02:02:13.228	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1815	2025-12-01 02:01:10.567	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'

	_time ⬍	user ⬍	action ⬍	search ⬍
1816	2025-12-01 02:00:45.869	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1817	2025-12-01 02:00:40.614	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1818	2025-12-01 02:00:40.555	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1819	2025-12-01 02:00:38.987	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1820	2025-12-01 02:00:32.824	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1821	2025-12-01 01:59:40.562	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1822	2025-12-01 01:59:26.491	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1823	2025-11-30 23:00:24.552	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'

	_time	user	action	search
1824	2025-11-30 23:00:08.562	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1825	2025-11-30 22:55:24.371	kimjoe	search	'typeahead prefix="metasearch index=botsv3 sourcetype=aws:cloudtrail user_type\"IAMUser\"" max_time="1" count="50" use_cache=1'
1826	2025-11-30 22:54:54.577	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1827	2025-11-30 22:54:54.324	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:cloudtrail user_type"IAMUser"'
1828	2025-11-30 22:54:47.033	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1829	2025-11-30 22:54:29.965	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:cloudtrail user_type"IAMUser"'
1830	2025-11-30 22:54:22.127	kimjoe	search	'typeahead prefix="metasearch index=botsv3 sourcetype=aws:cloudtrail user_type\"IAMUser\"" max_time="1" count="50" use_cache=1'
1831	2025-11-30 22:51:54.534	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1832	2025-11-30 22:51:29.411	kimjoe	search	'| metasearch index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'

	_time	user	action	search
1833	2025-11-30 22:49:24.494	kimjoe	search	'typeahead prefix="metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000" max_time="1" count="50" use_cache=1'
1834	2025-11-30 22:49:24.321	kimjoe	search	'search index="botsv3"'
1835	2025-11-30 22:48:24.317	kimjoe	search	'|metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000'
1836	2025-11-30 22:48:11.670	kimjoe	search	'|metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000'
1837	2025-11-30 22:48:04.840	kimjoe	search	'typeahead prefix="metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000" max_time="1" count="50" use_cache=1'
1838	2025-11-30 22:46:12.424	kimjoe	search	'search index="botsv3"'
1839	2025-11-30 22:35:24.366	kimjoe	search	'search index="botsv3"'
1840	2025-11-30 22:35:24.324	kimjoe	search	'search index="botsv3"'
1841	2025-11-30 22:35:07.981	kimjoe	search	'search index="botsv3"'
1842	2025-11-30 22:34:58.456	kimjoe	search	'search index="botsv3"'
1843	2025-11-30 22:34:54.422	kimjoe	search	'search index=botsv3'

	_time	user	action	search
1844	2025-11-30 22:34:54.367	kimjoe	search	'search index=botsv3'
1845	2025-11-30 22:34:54.318	kimjoe	search	'search index=botsv3'
1846	2025-11-30 22:34:38.319	kimjoe	search	'search index=botsv3'
1847	2025-11-30 22:34:36.057	kimjoe	search	'search index=botsv3'
1848	2025-11-30 22:34:30.646	kimjoe	search	'search index=botsv3'