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
1	2025-12-09 04:36:19.410	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table requestParameters.bucketName'
2	2025-12-09 04:33:11.437	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'
3	2025-12-09 04:32:48.382	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'
4	2025-12-09 04:27:11.426	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'

	_time	user	action	search
40	2025-12-09 04:26:51.159	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
40	2025-12-09 04:25:41.439	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
40	2025-12-09 04:25:17.725	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
40	2025-12-09 04:24:11.431	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, userIdentity.userName, requestParameters.bucketName'
40	2025-12-09 04:23:50.987	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, userIdentity.userName, requestParameters.bucketName'
41	2025-12-09 04:20:41.426	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
41	2025-12-09 04:20:27.139	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
41	2025-12-09 04:20:11.464	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<full_cpu>.+)" | stats count by full_cpu'

	_time	user	action	search
41	2025-12-09 04:20:11.449	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<full_cpu>.+)" | rex field=full_cpu | stats count by full_cpu'
41	2025-12-09 04:20:11.436	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<full_cpu>.+)" | rex field=full_cpu "E5-\d+" | stats count by full_cpu'
41	2025-12-09 04:20:06.077	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<full_cpu>.+)" | stats count by full_cpu'
41	2025-12-09 04:19:59.891	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<full_cpu>.+)" | rex field=full_cpu | stats count by full_cpu'
41	2025-12-09 04:19:43.956	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<full_cpu>.+)" | rex field=full_cpu "E5-\d+" | stats count by full_cpu'
41	2025-12-09 04:19:41.435	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex "CPU_TYPE\s+(?<processor>.+)" | dedup processor | table processor'
41	2025-12-09 04:19:19.622	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex "CPU_TYPE\s+(?<processor>.+)" | dedup processor | table processor'
42	2025-12-09 04:19:11.442	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'

	_time	user	action	search
42 1	2025-12-09 04:19:11.427	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host, CPU_TYPE, os, category, type'
42 2	2025-12-09 04:19:08.357	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
42 3	2025-12-09 04:18:56.806	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host, CPU_TYPE, os, category, type'
42 4	2025-12-09 04:15:11.414	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
42 5	2025-12-09 04:14:57.678	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
42 6	2025-12-09 04:14:11.433	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host processor'
42 7	2025-12-09 04:14:06.474	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host processor'
42 8	2025-12-09 04:03:41.419	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=hardware" max_time="1" count="50" use_cache=1'

	_time	user	action	search
4	2025-12-09 04:02:41.436	kimjoe	search	'search index=botsv3 sourcetype=hardware'
4	2025-12-09 04:02:21.431	kimjoe	search	'search index=botsv3 sourcetype=hardware'
4	2025-12-09 04:02:20.379	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=hardware" max_time="1" count="50" use_cache=1'
4	2025-12-09 04:02:11.428	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host processor'
4	2025-12-09 04:02:03.607	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host processor'
4	2025-12-09 03:51:11.493	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | fieldsummary'
4	2025-12-09 03:50:58.692	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | fieldsummary'
4	2025-12-09 03:49:41.486	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | fieldsummary | search field="*MFA*" | table field, count'

	_time	user	action	search
4	2025-12-09 03:49:13.822	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | fieldsummary | search field="*MFA*" | table field, count'
4	2025-12-09 03:49:11.445	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 2 | fieldsummary | search field="*MFA*" | table field, count'
4	2025-12-09 03:49:11.431	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
4	2025-12-09 03:49:03.404	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 2 | fieldsummary | search field="*MFA*" | table field, count'
4	2025-12-09 03:48:55.218	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
4	2025-12-09 03:47:41.482	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
4	2025-12-09 03:47:31.581	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
4	2025-12-09 03:47:11.425	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'

	_time	user	action	search
44	2025-12-09 03:46:53.889	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
46	2025-12-09 03:28:41.476	kimjoe	search	'| search (index=botsv3 sourcetype=aws:cloudtrail "userIdentity.type"="IAMUser") | stats values(userIdentity.userName) as usernames | eval usernames=mvdedup(usernames) | eval usernames=mvsort(usernames) | eval answer=mvjoin(usernames,",")'
47	2025-12-09 03:28:41.459	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames,",")] | table unique_users, answer'
48	2025-12-09 03:28:28.452	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames,",")] | table unique_users, answer'
49	2025-12-09 03:28:11.478	kimjoe	search	'| search (index=botsv3 sourcetype=aws:cloudtrail "userIdentity.type"="IAMUser") | stats values(userIdentity.userName) as usernames | eval usernames=mvdedup(usernames) | eval usernames=mvsort(usernames) | eval answer=mvjoin(usernames,",")'

	_time	user	action	search
45	2025-12-09 03:28:11.461	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames, ",")] | table unique_users, answer'
45	2025-12-09 03:27:55.271	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvsort(usernames) | eval answer = mvjoin(usernames, ",")] | table unique_users, answer'
45	2025-12-09 03:27:41.483	kimjoe	search	' search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",") '
45	2025-12-09 03:27:41.475	kimjoe	search	' search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",") '

	_time	user	action	search
45	2025-12-09 03:27:41.460	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",")] | table unique_users, answer'
45	2025-12-09 03:27:41.447	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",")]'
46	2025-12-09 03:27:36.517	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",")] | table unique_users, answer'
47	2025-12-09 03:27:20.737	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",")]'

	_time	user	action	search
45908	2025-12-09 03:27:11.490	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvsort(mvdedup(usernames)) | table usernames'
45909	2025-12-09 03:27:00.139	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvsort(mvdedup(usernames)) | table usernames'
46060	2025-12-09 03:16:11.480	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
46061	2025-12-09 03:15:46.803	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
46062	2025-12-09 03:11:41.440	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
46063	2025-12-09 03:11:35.957	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
46064	2025-12-09 03:10:11.461	kimjoe	search	'search index=botsv3 | stats count by sourcetype'
46065	2025-12-09 03:08:55.641	kimjoe	search	'search index=botsv3 | stats count by sourcetype'

	_time	user	action	search
46	2025-12-09 02:24:41.582	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
46	2025-12-09 02:24:36.252	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
46	2025-12-09 02:23:11.664	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*MFA*"'
46	2025-12-09 02:23:11.597	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\\\|]+)" | stats count by computer'
47	2025-12-09 02:23:11.537	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by host'
47	2025-12-09 02:22:41.750	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
47	2025-12-09 02:22:41.733	kimjoe	search	'search Let'
47	2025-12-09 02:22:41.715	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=AssumeRole | table eventName, userIdentity.sessionContext.attributes.mfaAuthenticated, additionalEventData.MFAUsed'

	_time	user	action	search
47	2025-12-09 02:22:41.684	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=AssumeRole | table eventName, userIdentity.sessionContext.attributes.mfaAuthenticated, additionalEventData.MFAUsed'
47	2025-12-09 02:22:41.651	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as mfaAuth, values(additionalEventData.MFAUsed) as MFAUsed'
47	2025-12-09 02:22:41.573	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | fieldsummary | search field="*MFA*"'
47	2025-12-09 02:22:40.718	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
47	2025-12-09 02:22:31.745	kimjoe	search	'search Let'
47	2025-12-09 02:22:17.668	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=AssumeRole | table eventName, userIdentity.sessionContext.attributes.mfaAuthenticated, additionalEventData.MFAUsed'
48	2025-12-09 02:22:17.513	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=AssumeRole | table eventName, userIdentity.sessionContext.attributes.mfaAuthenticated, additionalEventData.MFAUsed'
48	2025-12-09 02:22:17.261	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as mfaAuth, values(additionalEventData.MFAUsed) as MFAUsed'

	_time	user	action	search
48232	2025-12-09 02:22:12.320	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | fieldsummary | search field="*MFA*"'
48231	2025-12-09 02:22:11.681	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA*'
48234	2025-12-09 02:22:11.595	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) | stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'
48235	2025-12-09 02:22:11.579	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionalEventData.MFAUsed) | stats count by additionalEventData.MFAUsed'
48236	2025-12-09 02:22:11.565	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail'
48237	2025-12-09 02:22:02.924	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA*'
48238	2025-12-09 02:21:59.056	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*MFA*"'
48239	2025-12-09 02:21:57.457	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) | stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'

	_time	user	action	search
49	2025-12-09 02:21:53.059	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionalEventData.MFAUsed) | stats count by additionalEventData.MFAUsed'
49	2025-12-09 02:21:46.269	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail'
49	2025-12-09 02:21:43.335	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\\\|]+)" | stats count by computer'
49	2025-12-09 02:21:41.608	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern'
49	2025-12-09 02:21:40.120	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by host'
49	2025-12-09 02:21:34.726	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern'
49	2025-12-09 02:19:41.553	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* Account_Domain=AzureAD | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="BSTOLL-L.froth.ly"'
49	2025-12-09 02:19:22.723	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* Account_Domain=AzureAD | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="BSTOLL-L.froth.ly"'

	_time	user	action	search
49668	2025-12-09 02:18:11.566	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="BSTOLL-L.froth.ly"'
49699	2025-12-09 02:18:04.392	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="BSTOLL-L.froth.ly"'
50000	2025-12-09 00:34:11.879	kimjoe	search	'search index=botsv3 (sourcetype=WinEventLog:* OR sourcetype=winhostmon) | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval type = case(match(computer, "-L\.froth\.ly$"), "Client", match(computer, "SEPM"), "Server", true(), "Other") | stats count by computer, type'