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
50	2025-12-09 00:33:41.725	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="BSTOLL-L.froth.ly"'
50	2025-12-09 00:33:36.479	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'
50	2025-12-09 00:33:19.627	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="BSTOLL-L.froth.ly"'
50	2025-12-09 00:33:11.665	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="SEPM"'

	_time	user	action	search
50	2025-12-09 00:32:47.347	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer | search computer="SEPM"'
50	2025-12-09 00:27:41.677	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern | search pattern="Different"\='
50	2025-12-09 00:27:11.820	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern'
50	2025-12-09 00:27:03.213	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern'
50	2025-12-09 00:26:41.892	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern | search pattern="Different"'
51	2025-12-09 00:26:24.428	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 | search pattern="Different"'

	_time	user	action	search
51	2025-12-09 00:26:22.158	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 | search pattern="Different"\='
52	2025-12-09 00:26:11.911	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
53	2025-12-09 00:26:03.121	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
54	2025-12-09 00:25:41.818	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*windows*" OR sourcetype="*win*" OR sourcetype="*os*"'
55	2025-12-09 00:25:41.804	kimjoe	search	'search From Windows Event Logs: index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
56	2025-12-09 00:25:33.129	kimjoe	search	'search From Windows Event Logs: index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
57	2025-12-09 00:25:16.741	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*windows*" OR sourcetype="*win*" OR sourcetype="*os*"'
58	2025-12-09 00:25:11.717	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by host'

	_time	user	action	search
519	2025-12-09 00:24:44.873	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by host'
520	2025-12-09 00:24:41.670	kimjoe	search	'search From Windows Event Logs: index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
521	2025-12-09 00:24:29.892	kimjoe	search	'search From Windows Event Logs: index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
522	2025-12-09 00:22:41.785	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<computer>\\S+)" | stats dc(sourcetype) as sourcetype_count, count by computer | sort computer'
523	2025-12-09 00:22:41.680	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:*'
524	2025-12-09 00:22:26.216	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<computer>\\S+)" | stats dc(sourcetype) as sourcetype_count, count by computer | sort computer'
525	2025-12-09 00:21:41.743	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<fqdn>[^\\s\\|]+)" | stats count by fqdn | sort fqdn'
526	2025-12-09 00:21:14.026	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<fqdn>[^\\s\\|]+)" | stats count by fqdn | sort fqdn'

	_time	user	action	search
527	2025-12-09 00:21:11.671	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<fqdn>[^\\s\\\|]+)" | dedup fqdn | eval pattern=if(match(fqdn, "-L\\.froth\\.ly$"), "Standard", "Unique") | table fqdn, pattern'
528	2025-12-09 00:20:53.247	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<fqdn>[^\\s\\\|]+)" | dedup fqdn | eval pattern=if(match(fqdn, "-L\\.froth\\.ly$"), "Standard", "Unique") | table fqdn, pattern'
529	2025-12-09 00:20:41.687	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<fqdn>[^\\s\\\|]+)" | dedup fqdn | table fqdn'
530	2025-12-09 00:20:32.836	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex "ComputerName=(?<fqdn>[^\\s\\\|]+)" | dedup fqdn | table fqdn'
531	2025-12-09 00:20:11.842	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\\\|]+)" | stats count by computer'
532	2025-12-09 00:20:11.755	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:*'
533	2025-12-09 00:20:01.991	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\\\|]+)" | stats count by computer'
534	2025-12-09 00:19:46.872	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:*'

	_time	user	action	search
53	2025-12-09 00:19:36.649	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:*'
53	2025-12-09 00:18:41.660	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=PutBucketAct userIdentity.userName=bstoll | search *public* OR *Public*'
53	2025-12-09 00:18:16.801	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=PutBucketAct userIdentity.userName=bstoll | search *public* OR *Public*'
53	2025-12-09 00:18:11.669	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=PutBucketAct userIdentity.userName=bstoll'
53	2025-12-09 00:17:58.239	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=PutBucketAct userIdentity.userName=bstoll'
54	2025-12-09 00:17:11.857	kimjoe	search	'typeahead prefix="index=botsv3 s" max_time="1" count="50" use_cache=1'
54	2025-12-09 00:17:11.842	kimjoe	search	'typeahead prefix="index=botsv3 so" max_time="1" count="50" use_cache=1'
54	2025-12-09 00:17:11.826	kimjoe	search	'typeahead prefix="index=botsv3 sour" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1	2025-12-09 00:17:11.811	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:clo" max_time="1" count="50" use_cache=1'
2	2025-12-09 00:17:11.797	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
3	2025-12-09 00:17:11.772	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=AssumeRole | table eventName, userIdentity.sessionContext.attributes.mfaAuthenticated, additionalEventData.MFAUsed'
4	2025-12-09 00:17:11.743	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as mfaAuth, values(additionalEventData.MFAUsed) as MFAUsed'
5	2025-12-09 00:17:02.237	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName=AssumeRole | table eventName, userIdentity.sessionContext.attributes.mfaAuthenticated, additionalEventData.MFAUsed'
6	2025-12-09 00:16:45.753	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as mfaAuth, values(additionalEventData.MFAUsed) as MFAUsed'
7	2025-12-09 00:16:41.735	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | fieldsummary | search field="*MFA*"'
8	2025-12-09 00:16:31.416	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA* | fieldsummary | search field="*MFA*"'

	_time	user	action	search
5	2025-12-09 00:16:11.817	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA*'
5	2025-12-09 00:16:11.714	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail'
5	2025-12-09 00:16:05.454	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail *MFA*'
5	2025-12-09 00:15:53.439	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail'
5	2025-12-09 00:15:50.716	kimjoe	search	'typeahead prefix="index=botsv3 s" max_time="1" count="50" use_cache=1'
5	2025-12-09 00:15:50.256	kimjoe	search	'typeahead prefix="index=botsv3 so" max_time="1" count="50" use_cache=1'
5	2025-12-09 00:15:49.757	kimjoe	search	'typeahead prefix="index=botsv3 sour" max_time="1" count="50" use_cache=1'
5	2025-12-09 00:15:49.248	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:clo" max_time="1" count="50" use_cache=1'

	_time	user	action	search
55	2025-12-09 00:15:48.529	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
56	2025-12-08 23:59:41.713	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*MFA*"'
57	2025-12-08 23:59:34.215	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*MFA*"'
58	2025-12-08 23:56:41.672	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) | stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'
59	2025-12-08 23:56:21.334	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated) | stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'
60	2025-12-08 23:55:41.683	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionalEventData.MFAUsed) | stats count by additionalEventData.MFAUsed'
61	2025-12-08 23:55:41.670	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 5 | table _time, eventName, additionalEventData.*'
62	2025-12-08 23:55:39.279	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionalEventData.MFAUsed) | stats count by additionalEventData.MFAUsed'

	_time	user	action	search
5 6 7	2025-12-08 23:55:19.865	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 5 | table _time, eventName, additionalEventData.*'
5 6 8	2025-12-08 23:54:11.718	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
5 6 9	2025-12-08 23:53:41.455	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
5 7 0	2025-12-08 23:48:11.673	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
5 7 1	2025-12-08 23:48:03.403	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
5 7 2	2025-12-04 18:31:35.582	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
5 7 3	2025-12-04 18:31:21.813	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
5 7 4	2025-12-04 03:37:06.714	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'

	_time	user	action	search
57	2025-12-04 03:36:37.453	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
56	2025-12-04 03:36:36.772	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
57	2025-12-04 03:36:36.757	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
57	2025-12-04 03:36:26.749	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
58	2025-12-04 03:36:19.154	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
59	2025-12-04 03:36:06.710	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
60	2025-12-04 03:35:48.315	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
61	2025-12-04 03:29:06.729	kimjoe	search	botsv3
62				

	_time	user	action	search
1	2025-12-04 03:28:52.885	kimjoe	search	botsv3
2	2025-12-04 03:23:06.737	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3"'
3	2025-12-04 03:22:44.979	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3"'
4	2025-12-04 03:21:36.735	kimjoe	search	botsv3
5	2025-12-04 03:21:36.718	kimjoe	search	botsv3
6	2025-12-04 03:21:23.672	kimjoe	search	botsv3
7	2025-12-04 03:21:06.822	kimjoe	search	botsv3
8				

	_time	user	action	search
59	2025-12-04 03:21:06.751	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
59	2025-12-04 03:21:03.330	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
59	2025-12-03 23:05:16.040	kimjoe	search	'search index="botsv3"'
59	2025-12-03 23:03:51.575	kimjoe	search	'search index="botsv3"'
59	2025-12-03 02:05:24.041	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
59	2025-12-03 02:05:24.015	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'

	_time	user	action	search
59	2025-12-03 02:05:13.891	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = mvsort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
59	2025-12-03 02:05:00.214	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
59	2025-12-03 02:04:54.024	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'
59	2025-12-03 02:04:35.954	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'
60	2025-12-03 02:02:24.046	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'