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	2025-12-01 02:51:46.808	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri, http_method, http_status'
2	2025-12-01 02:51:40.549	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | table _time, bucket, object, uri, http_method, http_status'
3	2025-12-01 02:51:40.535	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri, http_method, http_status'

	_time	user	action	search
17704	2025-12-01 02:51:22.315	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | table _time, bucket, object, uri, http_method, http_status'
17705	2025-12-01 02:51:21.512	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs" max_time="1" count="50" use_cache=1'
17706	2025-12-01 02:51:13.024	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri, http_method, http_status'
17707	2025-12-01 02:51:10.599	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail:" max_time="1" count="50" use_cache=1'
17708	2025-12-01 02:51:10.589	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail" max_time="1" count="50" use_cache=1'
17709	2025-12-01 02:51:10.579	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"a" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1	2025-12-01 02:51:10.568	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"" max_time="1" count="50" use_cache=1'
2	2025-12-01 02:51:10.558	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=aws" max_time="1" count="50" use_cache=1'
3	2025-12-01 02:51:10.544	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcet" max_time="1" count="50" use_cache=1'
4	2025-12-01 02:50:40.514	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
5	2025-12-01 02:50:12.210	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
6	2025-12-01 02:50:10.562	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName,'

	_time	user	action	search
1	2025-12-01 02:50:10.550	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
2	2025-12-01 02:50:10.536	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
3	2025-12-01 02:50:08.242	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName,'
4	2025-12-01 02:49:58.517	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
5	2025-12-01 02:49:55.039	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail:" max_time="1" count="50" use_cache=1'
6	2025-12-01 02:49:54.305	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1	2025-12-01 02:49:53.168	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"a" max_time="1" count="50" use_cache=1'
2	2025-12-01 02:49:52.639	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"" max_time="1" count="50" use_cache=1'
3	2025-12-01 02:49:50.469	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=aws" max_time="1" count="50" use_cache=1'
4	2025-12-01 02:49:50.041	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcet" max_time="1" count="50" use_cache=1'
5	2025-12-01 02:49:40.176	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
6	2025-12-01 02:48:40.531	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(eventName) by sourcetype'
7				

	_time	user	action	search
17728	2025-12-01 02:48:40.518	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
17729	2025-12-01 02:48:32.162	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(eventName) by sourcetype'
17730	2025-12-01 02:48:18.188	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
17731	2025-12-01 02:48:10.521	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
17732	2025-12-01 02:47:57.779	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
17733	2025-12-01 02:43:10.615	kimjoe	search	'search index="botsv3" sourcetype="winhostmon" | stats dc(host) AS host_count BY os'

	_time	user	action	search
1	2025-12-01 02:42:42.442	kimjoe	search	'search index="botsv3" sourcetype="winhostmon" | stats dc(host) AS host_count BY os'
2	2025-12-01 02:42:40.526	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
3	2025-12-01 02:42:10.569	kimjoe	search	'search index="botsv3" sourcetype="winhostmon" | stats dc(host) AS host_count BY os'
4	2025-12-01 02:42:10.552	kimjoe	search	'search indext="botsv3" sourcetype="winhostmon" | stats dc(host) AS host_count BY os'
5	2025-12-01 02:42:10.296	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
6	2025-12-01 02:41:51.500	kimjoe	search	'search index="botsv3" sourcetype="winhostmon" | stats dc(host) AS host_count BY os'

	_time	user	action	search
1	2025-12-01 02:41:45.607	kimjoe	search	'search indext="botsv3" sourcetype="winhostmon" | stats dc(host) AS host_count BY os'
2	2025-12-01 02:40:10.527	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
3	2025-12-01 02:40:08.178	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
4	2025-12-01 02:37:10.544	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
5	2025-12-01 02:36:55.629	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
6	2025-12-01 02:36:40.540	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail\" \"MFAUsed\"" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1	2025-12-01 02:36:40.529	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail\"" max_time="1" count="50" use_cache=1'
2	2025-12-01 02:36:10.522	kimjoe	search	'search index="botsv3" sourcetype="hardware" | stats values(processor) BY host'
3	2025-12-01 02:36:02.344	kimjoe	search	'search index="botsv3" sourcetype="hardware" | stats values(processor) BY host'
4	2025-12-01 02:35:40.517	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" "MFAUsed" | table _time, eventName, userIdentity.userName, additionalEventData.MFAUsed'
5	2025-12-01 02:35:29.024	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" "MFAUsed" | table _time, eventName, userIdentity.userName, additionalEventData.MFAUsed'
6	2025-12-01 02:35:27.924	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail\" \"MFAUsed\"" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1	2025-12-01 02:35:24.832	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail\"" max_time="1" count="50" use_cache=1'
2	2025-12-01 02:35:10.520	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
3	2025-12-01 02:34:45.320	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
4	2025-12-01 02:33:10.640	kimjoe	search	'search index=botsv3 | stats earliest(_time) as start, latest(_time) as end'
5	2025-12-01 02:33:10.575	kimjoe	search	'search index=botsv3 | stats count by sourcetype'
6	2025-12-01 02:32:52.370	kimjoe	search	'search index=botsv3 | stats earliest(_time) as start, latest(_time) as end'
7				

	_time	user	action	search
1	2025-12-01 02:32:40.673	kimjoe	search	'search index=botsv3 | stats count by sourcetype'
2	2025-12-01 02:32:40.527	kimjoe	search	'search # Check total events by sourcetype index=botsv3 | stats count by sourcetype # Check time range of your data index=botsv3 | stats earliest(_time) as start, latest(_time) as end'
3	2025-12-01 02:32:22.452	kimjoe	search	'search # Check total events by sourcetype index=botsv3 | stats count by sourcetype # Check time range of your data index=botsv3 | stats earliest(_time) as start, latest(_time) as end'
4	2025-12-01 02:31:40.546	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count'
5	2025-12-01 02:31:40.522	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
6	2025-12-01 02:31:37.111	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count'

	_time	user	action	search
1	2025-12-01 02:31:20.044	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
2	2025-12-01 02:31:10.613	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
3	2025-12-01 02:31:10.599	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
4	2025-12-01 02:31:03.927	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
5	2025-12-01 02:30:58.517	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
6	2025-12-01 02:27:40.544	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'

	_time	user	action	search
1	2025-12-01 02:27:13.663	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
2	2025-12-01 02:27:10.545	kimjoe	search	'search index=botsv3 sourcetype=hardware | search "web" OR "www" OR "http" | stats values(processor) by host'
3	2025-12-01 02:26:47.133	kimjoe	search	'search index=botsv3 sourcetype=hardware | search "web" OR "www" OR "http" | stats values(processor) by host'
4	2025-12-01 02:24:10.547	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search "MFAUsed" | head 5 | table _time, eventName, additionalEventData.MFAUsed'
5	2025-12-01 02:24:10.534	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'
6	2025-12-01 02:24:01.454	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search "MFAUsed" | head 5 | table _time, eventName, additionalEventData.MFAUsed'

	_time	user	action	search
1	2025-12-01 02:23:49.847	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'
2	2025-12-01 02:23:40.535	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri, http_method, http_status'
3	2025-12-01 02:23:15.692	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri, http_method, http_status'
4	2025-12-01 02:22:10.526	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
5	2025-12-01 02:21:55.815	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
6	2025-12-01 02:21:40.551	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(eventName) by sourcetype'

	_time	user	action	search
1	2025-12-01 02:21:14.807	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(eventName) by sourcetype'
2	2025-12-01 02:20:40.580	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'
3	2025-12-01 02:20:33.154	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'
4	2025-12-01 02:19:10.624	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host, processor, os | stats values(processor) by host'
5	2025-12-01 02:18:53.531	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host, processor, os | stats values(processor) by host'
6	2025-12-01 02:18:10.560	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'
7				
8				

	_time	user	action	search
1	2025-12-01 02:18:07.561	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'
2	2025-12-01 02:17:10.558	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
3	2025-12-01 02:16:51.503	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
4	2025-12-01 02:13:40.531	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'
5	2025-12-01 02:13:29.193	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'
6	2025-12-01 02:11:40.531	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS usernames | eval usernames = mvdedup(usernames) | eval usernames = replace(usernames, "\s+", ",")'

	_time	user	action	search
1	2025-12-01 02:11:24.899	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS usernames | eval usernames = mvdedup(usernames) | eval usernames = replace(usernames, "\s+", ",")'
2	2025-12-01 02:09:40.540	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000'
3	2025-12-01 02:09:10.607	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:*'
4	2025-12-01 02:09:10.398	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000'
5	2025-12-01 02:08:49.783	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:*'
6	2025-12-01 02:08:40.532	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | stats values(sourcetype)'

	_time	user	action	search
1	2025-12-01 02:08:40.524	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | stats values(sourcetype)'
8				
0				
0				