

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 02:51:46.8	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search o	
7	08	e	h	bject="*.txt" OR uri="*.txt" table _time, bucket, object,	
0				uri, http_method, http_status'	
1					
1	2025-12-01 02:51:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs table _t	
7	49	e	h	ime, bucket, object, uri, http_method, http_status'	
0					
2					
1	2025-12-01 02:51:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search o	
7	35	e	h	bject="*.txt" OR uri="*.txt" table _time, bucket, object,	
0				uri, http_method, http_status'	
3					

		user	action	search
1	2025-12-01 02:51:22.3	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs table _t
7	15	e	h	ime, bucket, object, uri, http_method, http_status'
0				
4				
1	2025-12-01 02:51:21.5	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslog
7	12	e	h	s" max_time="1" count="50" use_cache=1'
0				
5				
1	2025-12-01 02:51:13.0	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search o
7	24	e	h	bject="*.txt" OR uri="*.txt" table _time, bucket, object,
0				uri, http_method, http_status'
6				
1	2025-12-01 02:51:10.5	kimjo	searc	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtr
7	99	e	h	ail:\" max_time="1" count="50" use_cache=1'
0				
7				
1	2025-12-01 02:51:10.5	kimjo	searc	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtr
7	89	e	h	ail\" max_time="1" count="50" use_cache=1'
0				
8				
1	2025-12-01 02:51:10.5	kimjo	searc	'typeahead prefix="index=\"botsv3\" sourcetype=\"a" max_time
7	79	e	h	= "1" count="50" use_cache=1'
0				
9				

		user	action	
	_time	▼	↙	search
1	2025-12-01 02:51:10.5	kimjo	searc	'typeahead prefix=\"index=\\"botsv3\\" sourcetype=\"\" max_time
7	68	e	h	=\"1\" count=\"50\" use_cache=1'
1				
0				
1	2025-12-01 02:51:10.5	kimjo	searc	'typeahead prefix=\"index=\\"botsv3\\" sourcetype=aws\" max_time
7	58	e	h	=\"1\" count=\"50\" use_cache=1'
1				
1	2025-12-01 02:51:10.5	kimjo	searc	'typeahead prefix=\"index=\\"botsv3\\" sourcet\" max_time=\"1\" co
7	44	e	h	unt=\"50\" use_cache=1'
1				
2				
1	2025-12-01 02:50:40.5	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" eventName
7	14	e	h	=\"PutBucketAcl\" table _time, eventName, eventID, userIdent
1				ity.userName, requestParameters.bucketName, requestParameter
3				s.acl'
1	2025-12-01 02:50:12.2	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" eventName
7	10	e	h	=\"PutBucketAcl\" table _time, eventName, eventID, userIdent
1				ity.userName, requestParameters.bucketName, requestParameter
4				s.acl'
1	2025-12-01 02:50:10.5	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" eventName
7	62	e	h	=\"PutBucketAcl\" table _time, eventName, eventID, userIdent
1				ity.userName, requestParameters.bucketName, '
5				

		user	action	search
1	2025-12-01 02:50:10.5	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName = "PutBucketAcl" table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
7	50	e	h	
1	2025-12-01 02:50:10.5	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
7	36	e	h	
1	2025-12-01 02:50:08.2	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName = "PutBucketAcl" table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, '
7	42	e	h	
1	2025-12-01 02:49:58.5	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" eventName = "PutBucketAcl" table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
7	17	e	h	
1	2025-12-01 02:49:55.0	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail:" max_time="1" count="50" use_cache=1'
7	39	e	h	
2	0			
1	2025-12-01 02:49:54.3	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrail" max_time="1" count="50" use_cache=1'
7	05	e	h	
2	1			

		user	action	search
1	2025-12-01 02:49:53.1	kimjo	searc	'typeahead prefix=\"index=\\"botsv3\\" sourcetype=\\"a\" max_time=\\\"1\\\" count=\\\"50\\\" use_cache=1'
7	68	e	h	
2				
1	2025-12-01 02:49:52.6	kimjo	searc	'typeahead prefix=\"index=\\"botsv3\\" sourcetype=\\"\" max_time=\\\"1\\\" count=\\\"50\\\" use_cache=1'
7	39	e	h	
2				
3				
1	2025-12-01 02:49:50.4	kimjo	searc	'typeahead prefix=\"index=\\"botsv3\\" sourcetype=aws\" max_time=\\\"1\\\" count=\\\"50\\\" use_cache=1'
7	69	e	h	
2				
4				
1	2025-12-01 02:49:50.0	kimjo	searc	'typeahead prefix=\"index=\\"botsv3\\" sourcet\" max_time=\\\"1\\\" count=\\\"50\\\" use_cache=1'
7	41	e	h	
2				
5				
1	2025-12-01 02:49:40.1	kimjo	searc	'search index= botsv3 sourcetype=aws:cloudtrail eventName=\\\"PutBucketAcl\\\" table _time, eventName, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
7	76	e	h	
2				
6				
1	2025-12-01 02:48:40.5	kimjo	searc	'search index= botsv3 sourcetype=aws:cloudtrail stats values(eventName) by sourcetype'
7	31	e	h	
2				
7				

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-01 02:48:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	18	e	h	tBucketAcl" table _time, eventID, userIdentity.userName, r
2				equestParameters.bucketName'
8				
1	2025-12-01 02:48:32.1	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail stats value
7	62	e	h	s(eventName) by sourcetype'
2				
9				
1	2025-12-01 02:48:18.1	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	88	e	h	tBucketAcl" table _time, eventID, userIdentity.userName, r
3				equestParameters.bucketName'
0				
1	2025-12-01 02:48:10.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	21	e	h	tBucketAcl" table _time, eventName, eventID, userIdentity.
3				userName, requestParameters.bucketName, requestParameters.ac
1				l'
1	2025-12-01 02:47:57.7	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	79	e	h	tBucketAcl" table _time, eventName, eventID, userIdentity.
3				userName, requestParameters.bucketName, requestParameters.ac
2				l'
1	2025-12-01 02:43:10.6	kimjo	searc	'search index="botsv3" sourcetype="winhostmon" stats dc(ho
7	15	e	h	st) AS host_count BY os'
3				
3				

		user	action	search	
1	2025-12-01 02:42:42.4	kimjo	searc	'search index="botsv3" sourcetype="winhostmon" stats dc(ho	
7	42	e	h	st) AS host_count BY os'	
3					
4					
1	2025-12-01 02:42:40.5	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" eventName	
7	26	e	h	="PutBucketAcl" table _time, eventID, userIdentity.userName	
3				, requestParameters.bucketName'	
5					
1	2025-12-01 02:42:10.5	kimjo	searc	'search index="botsv3" sourcetype="winhostmon" stats dc(ho	
7	69	e	h	st) AS host_count BY os'	
3					
6					
1	2025-12-01 02:42:10.5	kimjo	searc	'search index="botsv3" sourcetype="winhostmon" stats dc(ho	
7	52	e	h	st) AS host_count BY os'	
3					
7					
1	2025-12-01 02:42:10.2	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" eventName	
7	96	e	h	="PutBucketAcl" table _time, eventID, userIdentity.userName	
3				, requestParameters.bucketName'	
8					
1	2025-12-01 02:41:51.5	kimjo	searc	'search index="botsv3" sourcetype="winhostmon" stats dc(ho	
7	00	e	h	st) AS host_count BY os'	
3					
9					

		user	action	search
1	2025-12-01 02:41:45.6	kimjo	searc	'search index="botsv3" sourcetype="winhostmon" stats dc(h
7	07	e	h	ost) AS host_count BY os'
4				
0				
1	2025-12-01 02:40:10.5	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" eventName
7	27	e	h	="PutBucketAcl" table _time, eventID, userIdentity.userName,
4				requestParameters.bucketName'
1				
1	2025-12-01 02:40:08.1	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" eventName
7	78	e	h	="PutBucketAcl" table _time, eventID, userIdentity.userName,
4				requestParameters.bucketName'
2				
1	2025-12-01 02:37:10.5	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" stats c
7	44	e	h	ount by userIdentity.userName rename userIdentity.userName
4				AS "IAM_User"'
3				
1	2025-12-01 02:36:55.6	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" stats c
7	29	e	h	ount by userIdentity.userName rename userIdentity.userName
4				AS "IAM_User"'
4				
1	2025-12-01 02:36:40.5	kimjo	searc	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtr
7	40	e	h	ail\" \"MFAUsed\" max_time=\"1\" count=\"50\" use_cache=1'
4				
5				

		user	action	search
1	2025-12-01 02:36:40.5	kimjo	searc	'typeahead prefix="index=\\"botsv3\\" sourcetype=\\"aws:cloudtrai
7	29	e	h	nl\\\" max_time="1" count="50" use_cache=1'
4				
6				
1	2025-12-01 02:36:10.5	kimjo	searc	'search index="botsv3" sourcetype="hardware" stats values
7	22	e	h	(processor) BY host'
4				
7				
1	2025-12-01 02:36:02.3	kimjo	searc	'search index="botsv3" sourcetype="hardware" stats values
7	44	e	h	(processor) BY host'
4				
8				
1	2025-12-01 02:35:40.5	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" "MFAUsed"
7	17	e	h	table _time, eventName, userIdentity.userName, additionalEventData.MFAUsed'
4				
9				
1	2025-12-01 02:35:29.0	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" "MFAUsed"
7	24	e	h	table _time, eventName, userIdentity.userName, additionalEventData.MFAUsed'
5				
0				
1	2025-12-01 02:35:27.9	kimjo	searc	'typeahead prefix="index=\\"botsv3\\" sourcetype=\\"aws:cloudtrai
7	24	e	h	nl\\\" MFAUsed\\\" max_time="1" count="50" use_cache=1'
5				
1				

		user	action	search
1	2025-12-01 02:35:24.8	kimjo	searc	'typeahead prefix="index=\\"botsv3\\" sourcetype=\\"aws:cloudtrai
7	32	e	h	nl\\\" max_time="1" count="50" use_cache=1'
5				
2				
1	2025-12-01 02:35:10.5	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" stats c
7	20	e	h	ount by userIdentity.userName rename userIdentity.userName
5				AS "IAM_User"
3				
1	2025-12-01 02:34:45.3	kimjo	searc	'search index="botsv3" sourcetype="aws:cloudtrail" stats c
7	20	e	h	ount by userIdentity.userName rename userIdentity.userName
5				AS "IAM_User"
4				
1	2025-12-01 02:33:10.6	kimjo	searc	'search index=botsv3 stats earliest(_time) as start, lates
7	40	e	h	t(_time) as end'
5				
5				
1	2025-12-01 02:33:10.5	kimjo	searc	'search index=botsv3 stats count by sourcetype'
7	75	e	h	
5				
6				
1	2025-12-01 02:32:52.3	kimjo	searc	'search index=botsv3 stats earliest(_time) as start, lates
7	70	e	h	t(_time) as end'
5				
7				

		user	action	search	
1	2025-12-01 02:32:40.6	kimjo	searc	'search index=botsv3 stats count by sourcetype'	
7	73	e	h		
5					
8					
1	2025-12-01 02:32:40.5	kimjo	searc	'search # Check total events by sourcetype index=botsv3 st	
7	27	e	h	ats count by sourcetype # Check time range of your data inde	
5				x=botsv3 stats earliest(_time) as start, latest(_time) as	
9				end'	
1	2025-12-01 02:32:22.4	kimjo	searc	'search # Check total events by sourcetype index=botsv3 st	
7	52	e	h	ats count by sourcetype # Check time range of your data inde	
6				x=botsv3 stats earliest(_time) as start, latest(_time) as	
0				end'	
1	2025-12-01 02:31:40.5	kimjo	searc	'search index=botsv3 sourcetype=winhostmon stats dc(host)	
7	46	e	h	as host_count by os sort host_count'	
6					
1					
1	2025-12-01 02:31:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search h	
7	22	e	h	ttp_method="PUT" http_status=200 search object="*.txt" OR	
6				uri="*.txt" table _time, bucket, object, uri'	
2					
1	2025-12-01 02:31:37.1	kimjo	searc	'search index=botsv3 sourcetype=winhostmon stats dc(host)	
7	11	e	h	as host_count by os sort host_count'	
6					
3					

		user	action	search
_time	◆	◆	◆	◆
1	2025-12-01 02:31:20.0	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search h
7	44	e	h	ttp_method="PUT" http_status=200 search object="*.txt" OR
6				uri="*.txt" table _time, bucket, object, uri'
4				
1	2025-12-01 02:31:10.6	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search h
7	13	e	h	ttp_method="PUT" http_status=200 search object="*.txt" OR
6				uri="*.txt" table _time, bucket, object, uri'
5				
1	2025-12-01 02:31:10.5	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search h
7	99	e	h	ttp_method="PUT" http_status=200 search object="*.txt" OR
6				uri="*.txt" table _time, bucket, object, uri'
6				
1	2025-12-01 02:31:03.9	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search h
7	27	e	h	ttp_method="PUT" http_status=200 search object="*.txt" OR
6				uri="*.txt" table _time, bucket, object, uri'
7				
1	2025-12-01 02:30:58.5	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search h
7	17	e	h	ttp_method="PUT" http_status=200 search object="*.txt" OR
6				uri="*.txt" table _time, bucket, object, uri'
8				
1	2025-12-01 02:27:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	44	e	h	tBucketAcl" table _time, eventID, userIdentity.userName, r
6				equestParameters.bucketName'
9				

		user	action	search
1	2025-12-01 02:27:13.6	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	63	e	h	tBucketAcl" table _time, eventID, userIdentity.userName, r
7				equestParameters.bucketName'
0				
1	2025-12-01 02:27:10.5	kimjo	searc	'search index=botsv3 sourcetype=hardware search "web" OR
7	45	e	h	"www" OR "http" stats values(processor) by host'
7				
1				
1	2025-12-01 02:26:47.1	kimjo	searc	'search index=botsv3 sourcetype=hardware search "web" OR
7	33	e	h	"www" OR "http" stats values(processor) by host'
7				
2				
1	2025-12-01 02:24:10.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail search "MFA
7	47	e	h	Used" head 5 table _time, eventName, additionalEventDat
7				a.MFAUsed'
3				
1	2025-12-01 02:24:10.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.
7	34	e	h	type="IAMUser" stats values(userIdentity.userName) AS IAM_
7				Users eval IAM_Users = mvdedup(IAM_Users)'
4				
1	2025-12-01 02:24:01.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail search "MFA
7	54	e	h	Used" head 5 table _time, eventName, additionalEventDat
7				a.MFAUsed'
5				

		user	action	search
1	2025-12-01 02:23:49.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.
7	47	e	h	type="IAMUser" stats values(userIdentity.userName) AS IAM_
7				Users eval IAM_Users = mvdedup(IAM_Users)'
6				
1	2025-12-01 02:23:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search o
7	35	e	h	bject="*.txt" OR uri="*.txt" table _time, bucket, object,
7				uri, http_method, http_status'
7				
1	2025-12-01 02:23:15.6	kimjo	searc	'search index=botsv3 sourcetype=aws:s3:accesslogs search o
7	92	e	h	bject="*.txt" OR uri="*.txt" table _time, bucket, object,
7				uri, http_method, http_status'
8				
1	2025-12-01 02:22:10.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	26	e	h	tBucketAcl" table _time, eventName, eventID, userIdentity.
7				userName, requestParameters.bucketName, requestParameters.ac
9				l'
1	2025-12-01 02:21:55.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Pu
7	15	e	h	tBucketAcl" table _time, eventName, eventID, userIdentity.
8				userName, requestParameters.bucketName, requestParameters.ac
0				l'
1	2025-12-01 02:21:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail stats value
7	51	e	h	s(eventName) by sourcetype'
8				
1				

		user	action	search
1	2025-12-01 02:21:14.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail stats value
7	07	e	h	s(eventName) by sourcetype'
8				
1	2025-12-01 02:20:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail stats value
7	80	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentiti
8				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent
3				icated'
1	2025-12-01 02:20:33.1	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail stats value
7	54	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentiti
8				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent
4				icated'
1	2025-12-01 02:19:10.6	kimjo	searc	'search index=botsv3 sourcetype=hardware table host, proce
7	24	e	h	ssor, os stats values(processor) by host'
8				
5				
1	2025-12-01 02:18:53.5	kimjo	searc	'search index=botsv3 sourcetype=hardware table host, proce
7	31	e	h	ssor, os stats values(processor) by host'
8				
6				
1	2025-12-01 02:18:10.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail stats value
7	60	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentiti
8				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent
7				icated'

		user	action	search
1	2025-12-01 02:18:07.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail stats value
7	61	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdenti
8				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent
8				icated'
1	2025-12-01 02:17:10.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail fieldsummar
7	58	e	h	y search field="*mfa*" OR field="*MFA*" table field, cou
8				nt'
9				
1	2025-12-01 02:16:51.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail fieldsummar
7	03	e	h	y search field="*mfa*" OR field="*MFA*" table field, cou
9				nt'
0				
1	2025-12-01 02:13:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.
7	31	e	h	type="IAMUser" stats values(userIdentity.userName) AS IAM_
9				Users eval IAM_Users = mvdedup(IAM_Users)'
1				
1	2025-12-01 02:13:29.1	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.
7	93	e	h	type="IAMUser" stats values(userIdentity.userName) AS IAM_
9				Users eval IAM_Users = mvdedup(IAM_Users)'
2				
1	2025-12-01 02:11:40.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.
7	31	e	h	type="IAMUser" stats values(userIdentity.userName) AS user
9				names eval usernames = mvdedup(usernames) eval usernames
3				= replace(usernames, "\s+", ",")'

		user	action	search
1	2025-12-01 02:11:24.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity. type="IAMUser" stats values(userIdentity.userName) AS user names eval usernames = mvdedup(usernames) eval usernames = replace(usernames, "\s+", ",")'
7	99	e	h	
9				
4				
1	2025-12-01 02:09:40.5	kimjo	searc	' metasearch index=botsv3 sourcetype=aws:cloudtrail field u ser* head 10000'
7	40	e	h	
9				
5				
1	2025-12-01 02:09:10.6	kimjo	searc	' metasearch index=botsv3 sourcetype=aws:*
7	07	e	h	
9				
6				
1	2025-12-01 02:09:10.3	kimjo	searc	' metasearch index=botsv3 sourcetype=aws:cloudtrail field u ser* head 10000'
7	98	e	h	
9				
7				
1	2025-12-01 02:08:49.7	kimjo	searc	' metasearch index=botsv3 sourcetype=aws:*
7	83	e	h	
9				
8				
1	2025-12-01 02:08:40.5	kimjo	searc	' metadata type=sourcetypes index=botsv3 stats values(sou rcetype)'
7	32	e	h	
9				
9				

		user	action	
_time	sort	sort	sort	sort
1	2025-12-01 02:08:40.5	kimjo	searc	' metadata type=sourcetypes index=botsv3 stats values(sou
8	24	e	h	rcetype)'
0				
0				