

# 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	actio	search	
1	2025-12-02 03:23:09.3	kimj	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N"	
3	84	oe	h	max_time="1" count="50" use_cache=1'	
0					
1					
1	2025-12-02 03:23:09.3	kimj	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName	
3	71	oe	h	= "ConsoleLogin"   search additionalEventData.MFAUsed="No"   t	
0				able _time, eventName, additionalEventData.MFAUsed   head 5'	
2					
1	2025-12-02 03:22:56.5	kimj	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName	
3	33	oe	h	= "ConsoleLogin"   search additionalEventData.MFAUsed="No"   t	
0				able _time, eventName, additionalEventData.MFAUsed   head 5'	
3					

		user	action	search
_time	time	user	action	search
1	2025-12-02 03:22:39.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   eval mfa_field = case( isnotnull(additionaleventData.MFAUsed), "API_MFA_Field", isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated), "Console_MFA_Field", true(), "No_MFA_Info" )   stats count by mfa_field'
3	23	oe	h	
0				
4				
1	2025-12-02 03:22:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search additionaleventData.MFAUsed="No"   table _time, eventName, additionaleventData.MFAUsed   head 5'
3	57	oe	h	
0				
5				
1	2025-12-02 03:22:31.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   eval mfa_field = case( isnotnull(additionaleventData.MFAUsed), "API_MFA_Field", isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated), "Console_MFA_Field", true(), "No_MFA_Info" )   stats count by mfa_field'
3	55	oe	h	
0				
6				
1	2025-12-02 03:22:22.2	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search additionaleventData.MFAUsed="No"   table _time, eventName, additionaleventData.MFAUsed   head 5'
3	10	oe	h	
0				
7				
1	2025-12-02 03:22:09.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search additionaleventData.MFAUsed=*   head 5'
3	05	oe	h	
0				
8				
1	2025-12-02 03:22:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail Not eventName ="ConsoleLogin"   search additionaleventData.MFAUsed=*   head 5'
3	93	oe	h	
0				
9				

		user	action	search
1	2025-12-02 03:22:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed=*   head 5'
3	79			
1				
0				
1	2025-12-02 03:21:54.8	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search additionalEventData.MFAUsed=*   head 5'
3	74			
1				
1	2025-12-02 03:21:53.9	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT" max_time="1" count="50" use_cache=1'
3	37			
1				
2				
1	2025-12-02 03:21:53.1	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT" max_time="1" count="50" use_cache=1'
3	41			
1				
3				
1	2025-12-02 03:21:49.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail Not eventName = "ConsoleLogin"   search additionalEventData.MFAUsed=*   head 5'
3	13			
1				
4				
1	2025-12-02 03:21:49.0	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail Not" max_time="1" count="50" use_cache=1'
3	68			
1				
5				

		user	action	search
1	2025-12-02 03:21:48.5	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail No'
3	79	oe	h	t" max_time="1" count="50" use_cache=1'
1				
6				
1	2025-12-02 03:21:48.1	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail No"
3	61	oe	h	max_time="1" count="50" use_cache=1'
1				
7				
1	2025-12-02 03:21:47.6	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N"
3	07	oe	h	max_time="1" count="50" use_cache=1'
1				
8				
1	2025-12-02 03:21:43.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con'
3	04	oe	h	soleLogin"   search additionalEventData.MFAUsed=*   head 5'
1				
9				
1	2025-12-02 03:21:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con"
3	74	oe	h	soleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
0				
1	2025-12-02 03:21:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con"
3	59	oe	h	soleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
1				

		user	action	search
1	2025-12-02 03:21:39.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
1	2025-12-02 03:21:39.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
3				
1	2025-12-02 03:21:33.8	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
3				
4				
1	2025-12-02 03:21:30.7	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
3				
4				
5				
1	2025-12-02 03:21:26.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
3				
4				
5				
1	2025-12-02 03:21:20.9	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
2				
3				
4				
5				
6				
7				

		user	action	search
1	2025-12-02 03:21:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   where isnotnull(additionaleventData.MFAUsed)   stats count by additionaleventData.MFAUsed'
3	81	oe	h	
2				
8				
1	2025-12-02 03:21:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionaleventData.MFAUsed)   stats count by additionaleventData.MFAUsed'
3	70	oe	h	
2				
9				
1	2025-12-02 03:21:06.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   where isnotnull(additionaleventData.MFAUsed)   stats count by additionaleventData.MFAUsed'
3	91	oe	h	
3				
0				
1	2025-12-02 03:21:01.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionaleventData.MFAUsed)   stats count by additionaleventData.MFAUsed'
3	48	oe	h	
3				
1				
1	2025-12-02 03:20:39.4	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
3	22	oe	h	
3				
2				
1	2025-12-02 03:20:39.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [eval <>_exists = if(isnotnull('
3	04	oe	h	
3				
3				

		user	action	search
1	2025-12-02 03:20:22.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [e
3	15	oe	h	val <>FIELD>>_exists = if(isnotnull('
3				
4				
1	2025-12-02 03:20:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con
3	75	oe	h	soleLogin"   stats values(additionalEventData.MFAUsed) as MFA
3				_Values, count by eventName   where MFA_Values="No"   head 1
5				0'
1	2025-12-02 03:20:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con
3	61	oe	h	soleLogin"   stats values(additionalEventData.MFAUsed) as MFA
3				_Values, count by eventName   where MFA_Values="No"   head 1
6				0'
1	2025-12-02 03:19:44.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con
3	44	oe	h	soleLogin"   stats values(additionalEventData.MFAUsed) as MFA
3				_Values, count by eventName   where MFA_Values="No"   head 1
7				0'
1	2025-12-02 03:19:41.1	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con
3	17	oe	h	soleLogin"   stats values(additionalEventData.MFAUsed) as MFA
3				_Values, count by eventName   where MFA_Values="No"   head 1
8				0'
1	2025-12-02 03:19:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
3	85	oe	h	="ConsoleLogin"   stats values(additionalEventData.MFAUsed) a
3				s MFA_Values, count by eventName   where MFA_Values="No"   he
9				ad 10'

		user	action	search
1	2025-12-02 03:19:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
3	28	oe	h	
4				
0				
1	2025-12-02 03:19:36.2	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
3	24	oe	h	
4				
1	2025-12-02 03:19:16.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
3	51	oe	h	
4				
2				
1	2025-12-02 03:19:15.4	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
3	81	oe	h	
4				
3				
1	2025-12-02 03:19:09.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
3	77	oe	h	
4				
4				
1	2025-12-02 03:19:08.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
3	81	oe	h	
4				
5				

		user	action	search
_time	time	user	action	search
1	2025-12-02 03:18:39.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
3	94	oe	h	
4				
6				
1	2025-12-02 03:18:34.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
3	81	oe	h	
4				
7				
1	2025-12-02 03:17:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   eval mfa_field = case( isnotnull(additionaleventData.MFAUsed), "API_MFA_Field", isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated), "Console_MFA_Field", true(), "No_MFA_Info" )   stats count by mfa_field'
3	76	oe	h	
4				
8				
1	2025-12-02 03:17:13.0	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   eval mfa_field = case( isnotnull(additionaleventData.MFAUsed), "API_MFA_Field", isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated), "Console_MFA_Field", true(), "No_MFA_Info" )   stats count by mfa_field'
3	41	oe	h	
4				
9				
1	2025-12-02 03:17:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search additionaleventData.MFAUsed="No"   table _time, eventName, additionaleventData.MFAUsed   head 5'
3	84	oe	h	
5				
0				
1	2025-12-02 03:17:02.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search additionaleventData.MFAUsed="No"   table _time, eventName, additionaleventData.MFAUsed   head 5'
3	38	oe	h	
5				
1				

		user	action	search
	_time	user	action	search
1	2025-12-02 03:16:39.4	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
3				
5				
2				
1	2025-12-02 03:16:39.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3				
5				
3				
1	2025-12-02 03:16:28.5	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
3				
5				
4				
1	2025-12-02 03:16:17.8	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3				
5				
5				
1	2025-12-02 03:09:39.4	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
3				
5				
6				
1	2025-12-02 03:09:39.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
3				
5				
7				

		user	action	search
1	2025-12-02 03:09:22.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
3	22	oe	h	
5				
8				
1	2025-12-02 03:09:13.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
3	21	oe	h	
5				
9				
1	2025-12-02 03:09:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [e
3	80	oe	h	val <>_exists = if(isnotnull('
6				
0				
1	2025-12-02 03:09:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	25	oe	h	
6				
1				
1	2025-12-02 03:09:00.9	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [e
3	51	oe	h	val <>_exists = if(isnotnull('
6				
2				
1	2025-12-02 03:08:47.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	61	oe	h	
6				
3				

		user	action	search
1	2025-12-02 03:06:39.4	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA*   fieldsummary   search field="*MFA*'"
3	33			
6				
4				
1	2025-12-02 03:06:34.6	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA*   fieldsummary   search field="*MFA*'"
3	70			
6				
5				
1	2025-12-02 03:06:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
3	70			
6				
6				
1	2025-12-02 03:05:49.5	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
3	97			
6				
7				
1	2025-12-02 03:05:39.3	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" a" max_time="1" count="50" use_cache=1'
3	52			
6				
8				
1	2025-12-02 03:05:39.3	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" addi" max_time="1" count="50" use_cache=1'
3	42			
6				
9				

		user	action	search
_time	time	user	action	search
1	2025-12-02 03:05:39.3	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" additionalEventData" max_time="1" count="50" use_cache=1'
3	31			
7				
0				
1	2025-12-02 03:05:39.3	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" additionalEventData.MFAUsed" max_time="1" count="50" use_cache=1'
3	21			
7				
1				
1	2025-12-02 03:05:39.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\\"ConsoleLogin\\"   search *MFA*   head 1   fieldsummary   search field=\"*MFA*\"   table field, count'
3	13			
7				
2				
1	2025-12-02 03:05:23.6	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\\"ConsoleLogin\\"   search *MFA*   head 1   fieldsummary   search field=\"*MFA*\"   table field, count'
3	06			
7				
3				
1	2025-12-02 03:05:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [e
3	97			val <>_exists = if(isnotnull('
7				
4				
1	2025-12-02 03:04:47.4	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [e
3	38			val <>_exists = if(isnotnull('
7				
5				

		user	action	search
1	2025-12-02 03:04:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"
3	80	oe	h	
7				
6				
1	2025-12-02 03:04:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin" additionalEventData.MFAUsed=*'
3	21	oe	h	
7				
7				
1	2025-12-02 03:04:15.7	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"
3	05	oe	h	
7				
8				
1	2025-12-02 03:04:15.0	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" a" max_time="1" count="50" use_cache=1'
3	51	oe	h	
7				
9				
1	2025-12-02 03:04:14.6	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" addi" max_time="1" count="50" use_cache=1'
3	16	oe	h	
8				
0				
1	2025-12-02 03:04:14.1	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" additionalEventData" max_time="1" count="50" use_cache=1'
3	85	oe	h	
8				
1				

		user	action	search
1	2025-12-02 03:04:13.7	kimj	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\\"ConsoleLogin\\" additionalEventData.MFAUsed" max_time="1" count="50" use_cache=1'
3	34	oe	h	
8				
2				
1	2025-12-02 03:04:11.8	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\\"ConsoleLogin" additionalEventData.MFAUsed=*'
3	17	oe	h	
8				
3				
1	2025-12-02 03:04:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\\"ConsoleLogin" additionalEventData.MFAUsed=*"   stats count by additionalEventData.MFAUsed'
3	07	oe	h	
8				
4				
1	2025-12-02 03:03:44.7	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\\"ConsoleLogin" additionalEventData.MFAUsed=*"   stats count by additionalEventData.MFAUsed'
3	59	oe	h	
8				
5				
1	2025-12-02 03:03:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\\"ConsoleLogin" additionalEventData.MFAUsed=*''
3	64	oe	h	
8				
6				
1	2025-12-02 03:03:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName =\\"ConsoleLogin" additionalEventData.MFAUsed=*"   stats count by additionalEventData.MFAUsed'
3	51	oe	h	
8				
7				

		user	action	search
	_time	user	action	search
1	2025-12-02 03:03:22.7	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin" additionalEventData.MFAUsed=*'
3	76			
8				
1	2025-12-02 03:03:16.2	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'
3	94			
8				
9				
1	2025-12-02 03:03:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	14			
9				
0				
1	2025-12-02 03:02:44.5	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	75			
9				
1				
1	2025-12-02 03:02:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	16			
9				
2				
1	2025-12-02 03:01:54.8	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	72			
9				
3				

		user	action	search
1	2025-12-02 03:01:39.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA*   fieldsummary   search field="*MFA*'"
3	63	oe	h	
9				
4				
1	2025-12-02 03:01:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 5   table _time, eventName, additionalEventData.*'
3	88	oe	h	
9				
5				
1	2025-12-02 03:01:28.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA*   fieldsummary   search field="*MFA*'"
3	24	oe	h	
9				
6				
1	2025-12-02 03:01:24.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   search *MFA*   head 5   table _time, eventName, additionalEventData.*'
3	11	oe	h	
9				
7				
1	2025-12-02 03:01:09.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	39	oe	h	
9				
8				
1	2025-12-02 03:00:44.6	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName = "ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
3	48	oe	h	
9				
9				

		user	action	search	
1	2025-12-02 03:00:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin"   search *MFA*   head 5   table _time, eventN ame, additionalEventData.*'	
4	73	oe	h		
0					
0					