

# 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)









	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1	2025-12-02 03:23:09.3	kimj	search	'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	search	'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	search	'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				









	 _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					

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1310	2025-12-02 03:22:09.379	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed=*   head 5'
1311	2025-12-02 03:21:54.874	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search additionalEventData.MFAUsed=*   head 5'
1312	2025-12-02 03:21:53.937	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT" max_time="1" count="50" use_cache=1'
1313	2025-12-02 03:21:53.141	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT" max_time="1" count="50" use_cache=1'
1314	2025-12-02 03:21:49.313	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail Not eventName="ConsoleLogin"   search additionalEventData.MFAUsed=*   head 5'
1315	2025-12-02 03:21:49.068	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail Not" max_time="1" count="50" use_cache=1'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1316	2025-12-02 03:21:48.579	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail No t" max_time="1" count="50" use_cache=1'
1317	2025-12-02 03:21:48.161	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail No" max_time="1" count="50" use_cache=1'
1318	2025-12-02 03:21:47.607	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N" max_time="1" count="50" use_cache=1'
1319	2025-12-02 03:21:43.404	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con soleLogin"   search additionalEventData.MFAUsed=*   head 5'
1320	2025-12-02 03:21:39.374	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con soleLogin"   search additionalEventData.MFAUsed="No"   head 5'
1321	2025-12-02 03:21:39.359	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Con soleLogin"   search additionalEventData.MFAUsed="No"   head 5'









	_time ↕	user ↕ 	action ↕ 	search ↕ 
1 3 2 2	2025-12-02 03:21:39.344	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
1 3 2 3	2025-12-02 03:21:39.331	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
1 3 2 4	2025-12-02 03:21:33.849	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
1 3 2 5	2025-12-02 03:21:30.760	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
1 3 2 6	2025-12-02 03:21:26.362	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
1 3 2 7	2025-12-02 03:21:20.956	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'

	 _time 	 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 <<FIELD>>_exists = if(isnotnull('
3	04	oe	h	
3				
3				

	 _time 	 user 	 action 	 search 
1 3 3 4	2025-12-02 03:20:22.6 15	kimj oe	search h	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [eval <<FIELD>>_exists = if(isnotnull('
1 3 3 5	2025-12-02 03:20:09.3 75	kimj oe	search h	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1 3 3 6	2025-12-02 03:20:09.3 61	kimj oe	search h	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1 3 3 7	2025-12-02 03:19:44.6 44	kimj oe	search h	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1 3 3 8	2025-12-02 03:19:41.1 17	kimj oe	search h	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1 3 3 9	2025-12-02 03:19:39.3 85	kimj oe	search h	'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'

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
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				
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				











	 _time 	 user 	 action 	 search 
1 3 4 6	2025-12-02 03:18:39.4 94	kimj oe	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'
1 3 4 7	2025-12-02 03:18:34.3 81	kimj oe	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'
1 3 4 8	2025-12-02 03:17:39.3 76	kimj oe	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'
1 3 4 9	2025-12-02 03:17:13.0 41	kimj oe	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'
1 3 5 0	2025-12-02 03:17:09.3 84	kimj oe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   table _time, eventName, additionalEventData.MFAUsed   head 5'
1 3 5 1	2025-12-02 03:17:02.9 38	kimj oe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search additionalEventData.MFAUsed="No"   table _time, eventName, additionalEventData.MFAUsed   head 5'

	<div><div>_time</div></div>	<div><div>user</div></div>	<div><div>action</div></div>	<div><div>search</div></div>
1	2025-12-02 03:16:39.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
3	44	oe	h	="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
5				
2				
1	2025-12-02 03:16:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
3	93	oe	h	="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
5				
3				
1	2025-12-02 03:16:28.5	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
3	71	oe	h	="ConsoleLogin"   search additionalEventData.MFAUsed="No"   head 5'
5				
4				
1	2025-12-02 03:16:17.8	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
3	32	oe	h	="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
5				
5				
1	2025-12-02 03:09:39.4	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
3	44	oe	h	="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
5				
6				
1	2025-12-02 03:09:39.3	kimj	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
3	80	oe	h	="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
5				
7				

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1 3 5 8	2025-12-02 03:09:22.622	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'
1 3 5 9	2025-12-02 03:09:13.421	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
1 3 6 0	2025-12-02 03:09:09.380	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [eval <<FIELD>>_exists = if(isnotnull('
1 3 6 1	2025-12-02 03:09:09.325	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
1 3 6 2	2025-12-02 03:09:00.951	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   foreach * [eval <<FIELD>>_exists = if(isnotnull('
1 3 6 3	2025-12-02 03:08:47.461	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1 3 6 4	2025-12-02 03:06:39.433	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA*   fieldsummary   search field="*MFA*"'
1 3 6 5	2025-12-02 03:06:34.670	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA*   fieldsummary   search field="*MFA*"'
1 3 6 6	2025-12-02 03:06:09.370	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'
1 3 6 7	2025-12-02 03:05:49.597	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'
1 3 6 8	2025-12-02 03:05:39.352	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" a" max_time="1" count="50" use_cache=1'
1 3 6 9	2025-12-02 03:05:39.342	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" addi" max_time="1" count="50" use_cache=1'









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

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

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

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
138	2025-12-02 03:03:22.776	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*
139	2025-12-02 03:03:16.294	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'
140	2025-12-02 03:03:09.314	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
141	2025-12-02 03:02:44.575	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
142	2025-12-02 03:02:09.316	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
143	2025-12-02 03:01:54.872	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'



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

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