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	2025-12-02 03:23:09.384	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N" max_time="1" count="50" use_cache=1'
2	2025-12-02 03:23:09.371	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'
3	2025-12-02 03:22:56.533	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'

	_time	user	action	search
1	2025-12-02 03:22:39.423	kimjoe	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'
2	2025-12-02 03:22:39.357	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'
3	2025-12-02 03:22:31.955	kimjoe	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'
4	2025-12-02 03:22:22.210	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'
5	2025-12-02 03:22:09.405	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'
6	2025-12-02 03:22:09.393	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail Not eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'

	_time	user	action	search
1	2025-12-02 03:22:09.379	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'
2	2025-12-02 03:21:54.874	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'
3	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'
4	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'
5	2025-12-02 03:21:49.313	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail Not eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'
6	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'

	_time	user	action	search
1	2025-12-02 03:21:48.579	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail Not" max_time="1" count="50" use_cache=1'
2	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'
3	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'
4	2025-12-02 03:21:43.404	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'
5	2025-12-02 03:21:39.374	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'
6	2025-12-02 03:21:39.359	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'

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

	_time	user	action	search
1	2025-12-02 03:21:09.381	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'
2	2025-12-02 03:21:09.370	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'
3	2025-12-02 03:21:06.591	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'
4	2025-12-02 03:21:01.048	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'
5	2025-12-02 03:20:39.422	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
6	2025-12-02 03:20:39.404	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('

	_time	user	action	search
1	2025-12-02 03:20:22.615	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('
2	2025-12-02 03:20:09.375	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName | where MFA_Values="No" | head 10'
3	2025-12-02 03:20:09.361	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName | where MFA_Values="No" | head 10'
4	2025-12-02 03:19:44.644	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName | where MFA_Values="No" | head 10'
5	2025-12-02 03:19:41.117	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName | where MFA_Values="No" | head 10'
6	2025-12-02 03:19:39.385	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'

	_time	user	action	search
1	2025-12-02 03:19:39.328	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
2	2025-12-02 03:19:36.224	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	2025-12-02 03:19:16.951	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
4	2025-12-02 03:19:15.481	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
5	2025-12-02 03:19:09.477	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
6	2025-12-02 03:19:08.081	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'

	_time	user	action	search
1	2025-12-02 03:18:39.494	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'
2	2025-12-02 03:18:34.381	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	2025-12-02 03:17:39.376	kimjoe	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'
4	2025-12-02 03:17:13.041	kimjoe	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'
5	2025-12-02 03:17:09.384	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'
6	2025-12-02 03:17:02.938	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'

	_time	user	action	search
1	2025-12-02 03:16:39.444	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'
2				
1	2025-12-02 03:16:39.393	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'
3				
1	2025-12-02 03:16:28.571	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'
4				
1	2025-12-02 03:16:17.832	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'
5				
1	2025-12-02 03:09:39.444	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'
6				
1	2025-12-02 03:09:39.380	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
7				

	_time	user	action	search
1	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'
2	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'
3	2025-12-02 03:09:09.380	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('
4	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'
5	2025-12-02 03:09:00.951	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('
6	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'

	_time	user	action	search
1	2025-12-02 03:06:39.433	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
1	2025-12-02 03:06:34.670	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
1	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	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	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	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	2025-12-02 03:05:39.331	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" additionalEventData" max_time="1" count="50" use_cache=1'
2	2025-12-02 03:05:39.321	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" additionalEventData.MFAUsed" max_time="1" count="50" use_cache=1'
3	2025-12-02 03:05:39.313	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
4	2025-12-02 03:05:23.606	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
5	2025-12-02 03:05:09.397	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('
6	2025-12-02 03:04:47.438	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('

	_time	user	action	search
1	2025-12-02 03:04:39.380	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
2	2025-12-02 03:04:39.321	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*'
3	2025-12-02 03:04:15.705	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
4	2025-12-02 03:04:15.051	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" a" max_time="1" count="50" use_cache=1'
5	2025-12-02 03:04:14.616	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" addi" max_time="1" count="50" use_cache=1'
6	2025-12-02 03:04:14.185	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" additionalEventData" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1	2025-12-02 03:04:13.734	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" additionalEventData.MFAUsed" max_time="1" count="50" use_cache=1'
1	2025-12-02 03:04:11.817	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*'
1	2025-12-02 03:04:09.307	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=* | stats count by additionalEventData.MFAUsed'
1	2025-12-02 03:03:44.759	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=* | stats count by additionalEventData.MFAUsed'
1	2025-12-02 03:03:39.364	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*'
1	2025-12-02 03:03:39.351	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=* | stats count by additionalEventData.MFAUsed'

	_time	user	action	search
1	2025-12-02 03:03:22.776	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*'
2	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'
3	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'
4	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'
5	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'
6	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	2025-12-02 03:01:39.463	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
2	2025-12-02 03:01:39.388	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 5 | table _time, eventName, additionalEventData.*'
3	2025-12-02 03:01:28.424	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
4	2025-12-02 03:01:24.511	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 5 | table _time, eventName, additionalEventData.*'
5	2025-12-02 03:01:09.339	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnotnull(additionalEventData.MFAUsed) | stats count by additionalEventData.MFAUsed'
6	2025-12-02 03:00:44.648	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	2025-12-02 03:00:39.373	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search *MFA* | head 5 | table _time, eventName, additionalEventData.*'
4				
0				
0				