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
1201	2025-12-02 11:21:28.524	kimjoe	search	'search index=botsv3 sourcetype=hardware | search host=*web* OR category=*web* OR type=*web* OR os=*web* | table host, processor, os, category, type'
1202	2025-12-02 11:21:08.716	kimjoe	search	'search index=botsv3 sourcetype=hardware | search host=*web* OR category=*web* OR type=*web* OR os=*web* | table host, processor, os, category, type'
1203	2025-12-02 11:18:28.618	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | search host="gacrux.i-09cbc261e84259b54"'

	_time	user	action	search
1204	2025-12-02 11:18:28.540	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
1205	2025-12-02 11:18:07.565	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | search host="gacrux.i-09cbc261e84259b54"'
1206	2025-12-02 11:17:59.829	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
1207	2025-12-02 11:17:58.539	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, CPU_TYPE, os, category, type'
1208	2025-12-02 11:17:48.736	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, CPU_TYPE, os, category, type'
1209	2025-12-02 11:16:58.533	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'

	_time	user	action	search
1210	2025-12-02 11:16:46.554	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
1211	2025-12-02 11:13:58.744	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
1212	2025-12-02 11:13:42.446	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
1213	2025-12-02 11:13:28.814	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName ="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'
1214	2025-12-02 11:13:28.749	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'
1215	2025-12-02 11:13:16.928	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
1216	2025-12-02 11:12:59.401	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'
1217	2025-12-02 11:12:28.551	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count by host | where (count > 0)'
1218	2025-12-02 11:12:28.508	kimjoe	search	'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host | where count > 0] | stats values(processor) as processors by host | table host, processors'
1219	2025-12-02 11:12:01.302	kimjoe	search	'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host | where count > 0] | stats values(processor) as processors by host | table host, processors'
1220	2025-12-02 03:54:39.357	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count by host | where (count > 0)'
1221	2025-12-02 03:54:39.350	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count as http_events by host'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>1222</td><td>2025-12-02 03:54:39.340</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host | where count > 0] | stats values(processor) as processors by host | table host, processors'</td></tr>
<tr><td>1223</td><td>2025-12-02 03:54:39.328</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=hardware | search processor=* | join type=left host [search index=botsv3 sourcetype=stream:http | stats count as http_events by host] | eval is_web_server = if(isnotnull(http_events), "Yes", "No") | table host, processor, os, http_events, is_web_server | sort -http_events'</td></tr>
<tr><td>1224</td><td>2025-12-02 03:54:27.333</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host | where count > 0] | stats values(processor) as processors by host | table host, processors'</td></tr>
<tr><td>1225</td><td>2025-12-02 03:54:12.850</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=hardware | search processor=* | join type=left host [search index=botsv3 sourcetype=stream:http | stats count as http_events by host] | eval is_web_server = if(isnotnull(http_events), "Yes", "No") | table host, processor, os, http_events, is_web_server | sort -http_events'</td></tr>
<tr><td>1226</td><td>2025-12-02 03:54:09.457</td><td>kimjoe</td><td>search</td><td>'| search (index=botsv3 sourcetype=hardware) | dedup host | table host, processor'</td></tr>
</table>

	_time	user	action	search
1227	2025-12-02 03:54:09.446	kimjoe	search	'search index=botsv3 sourcetype=hardware | search os=*Server* AND (processor=*) | table host, processor, os'
1228	2025-12-02 03:54:09.431	kimjoe	search	'search index=botsv3 sourcetype=stream:http OR sourcetype=stream:tcp | stats count by host | join type=inner host [search index=botsv3 sourcetype=hardware | dedup host | table host, processor] | table host, processor, count'
1229	2025-12-02 03:54:00.395	kimjoe	search	'search index=botsv3 sourcetype=hardware | search os=*Server* AND (processor=*) | table host, processor, os'
1230	2025-12-02 03:53:45.462	kimjoe	search	'search index=botsv3 sourcetype=stream:http OR sourcetype=stream:tcp | stats count by host | join type=inner host [search index=botsv3 sourcetype=hardware | dedup host | table host, processor] | table host, processor, count'
1231	2025-12-02 03:53:39.333	kimjoe	search	'search index=botsv3 sourcetype=hardware | search host=*web* OR category=*web* OR type=*web* OR os=*web* | table host, processor, os, category, type'
1232	2025-12-02 03:53:39.318	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'

	_time	user	action	search
1233	2025-12-02 03:53:31.454	kimjoe	search	'search index=botsv3 sourcetype=hardware | search host=*web* OR category=*web* OR type=*web* OR os=*web* | table host, processor, os, category, type'
1234	2025-12-02 03:53:11.693	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
1235	2025-12-02 03:53:09.378	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count by host'
1236	2025-12-02 03:53:09.363	kimjoe	search	'search index=botsv3 sourcetype=hardware | search host=*www* OR host=*web* | table host, processor'
1237	2025-12-02 03:53:09.351	kimjoe	search	'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host] | stats count as server_count by processor | sort -server_count | head 1'
1238	2025-12-02 03:52:56.787	kimjoe	search	'search index=botsv3 sourcetype=hardware | search host=*www* OR host=*web* | table host, processor'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>1239</td><td>2025-12-02 03:52:41.971</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host] | stats count as server_count by processor | sort -server_count | head 1'</td></tr>
<tr><td>1240</td><td>2025-12-02 03:52:39.371</td><td>kimjoe</td><td>search</td><td>'| search (index=botsv3 sourcetype=hardware) | dedup host | table host, processor, os'</td></tr>
<tr><td>1241</td><td>2025-12-02 03:52:39.363</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=stream:http | stats count by host | join type=inner host [search index=botsv3 sourcetype=hardware | dedup host | table host, processor, os] | table host, processor, os, count | sort -count'</td></tr>
<tr><td>1242</td><td>2025-12-02 03:52:09.642</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=stream:http | stats count by host | join type=inner host [search index=botsv3 sourcetype=hardware | dedup host | table host, processor, os] | table host, processor, os, count | sort -count'</td></tr>
<tr><td>1243</td><td>2025-12-02 03:52:09.425</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=stream:http | stats dc(host) as unique_web_hosts'</td></tr>
<tr><td>1244</td><td>2025-12-02 03:51:59.710</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=stream:http | stats dc(host) as unique_web_hosts'</td></tr>
</table>

	_time	user	action	search
1245	2025-12-02 03:51:39.345	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count by host'
1246	2025-12-02 03:51:39.320	kimjoe	search	'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host] | table host, processor'
1247	2025-12-02 03:51:36.711	kimjoe	search	'search index=botsv3 sourcetype=hardware | join type=inner host [search index=botsv3 sourcetype=stream:http | stats count by host] | table host, processor'
1248	2025-12-02 03:31:39.433	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('
1249	2025-12-02 03:31:09.513	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N" max_time="1" count="50" use_cache=1'
1250	2025-12-02 03:31:09.267	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('

	_time	user	action	search
1251	2025-12-02 03:30:39.357	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO" max_time="1" count="50" use_cache=1'
1252	2025-12-02 03:30:39.342	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT" max_time="1" count="50" use_cache=1'
1253	2025-12-02 03:30:09.376	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
1254	2025-12-02 03:29:39.993	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search *MFA* | head 1 | fieldsummary | search field="*MFA*" | table field, count'
1255	2025-12-02 03:29:39.037	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N" max_time="1" count="50" use_cache=1'
1256	2025-12-02 03:29:38.589	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1257	2025-12-02 03:29:38.112	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT" max_time="1" count="50" use_cache=1'
1258	2025-12-02 03:28:39.507	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'
1259	2025-12-02 03:28:39.494	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'
1260	2025-12-02 03:28:35.400	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | table _time, eventName, additionaleventData.MFAUsed | head 5'
1261	2025-12-02 03:28:09.402	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N" max_time="1" count="50" use_cache=1'
1262	2025-12-02 03:28:09.392	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1263	2025-12-02 03:28:09.377	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | eval mfa_field = case(isnotnull(additionaleventData.MFAUsed), isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated), "Console_MFA_Field", true(), "No_MFA_Info") | stats count by mfa_field'
1264	2025-12-02 03:28:09.153	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'
1265	2025-12-02 03:27:55.178	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | eval mfa_field = case(isnotnull(additionaleventData.MFAUsed), isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated), "Console_MFA_Field", true(), "No_MFA_Info") | stats count by mfa_field'
1266	2025-12-02 03:27:39.455	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail '
1267	2025-12-02 03:27:39.443	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1268	2025-12-02 03:27:39.431	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'
1269	2025-12-02 03:27:39.371	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"'
1270	2025-12-02 03:27:39.352	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"'
1271	2025-12-02 03:27:31.939	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'
1272	2025-12-02 03:27:15.027	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"'
1273	2025-12-02 03:27:11.519	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>1274</td><td>2025-12-02 03:27:09.399</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'</td></tr>
<tr><td>1275</td><td>2025-12-02 03:27:01.081</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | where isnotnull(additionaleventData.MFAUsed) | stats count by additionaleventData.MFAUsed'</td></tr>
<tr><td>1276</td><td>2025-12-02 03:26:55.672</td><td>kimjoe</td><td>search</td><td>'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail N" max_time="1" count="50" use_cache=1'</td></tr>
<tr><td>1277</td><td>2025-12-02 03:26:55.187</td><td>kimjoe</td><td>search</td><td>'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO" max_time="1" count="50" use_cache=1'</td></tr>
<tr><td>1278</td><td>2025-12-02 03:26:39.550</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | search additionaleventData.MFAUsed="No" | head 5'</td></tr>
<tr><td>1279</td><td>2025-12-02 03:26:39.527</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'</td></tr>
</table>

	_time	user	action	search
1280	2025-12-02 03:26:38.082	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search additionaleventData.MFAUsed="No" | head 5'
1281	2025-12-02 03:26:31.490	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'
1282	2025-12-02 03:26:29.685	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail '
1283	2025-12-02 03:26:27.603	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
1284	2025-12-02 03:26:09.422	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'
1285	2025-12-02 03:26:09.397	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'

	_time	user	action	search
1286	2025-12-02 03:26:06.996	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed=* | head 5'
1287	2025-12-02 03:25:58.560	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | search additionaleventData.MFAUsed="No" | head 5'
1288	2025-12-02 03:25:39.361	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search "MFAUsed" | head 5 | table _time, eventName, additionalEventData.MFAUsed'
1289	2025-12-02 03:25:11.634	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search "MFAUsed" | head 5 | table _time, eventName, additionalEventData.MFAUsed'
1290	2025-12-02 03:24:09.441	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail '
1291	2025-12-02 03:23:44.887	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail '

	_time	user	action	search
1292	2025-12-02 03:23:39.452	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'
1293	2025-12-02 03:23:39.388	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
1294	2025-12-02 03:23:35.634	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'
1295	2025-12-02 03:23:17.295	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
1296	2025-12-02 03:23:09.437	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT" max_time="1" count="50" use_cache=1'
1297	2025-12-02 03:23:09.427	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1298	2025-12-02 03:23:09.414	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail Not" max_time="1" count="50" use_cache=1'
1299	2025-12-02 03:23:09.405	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail Not" max_time="1" count="50" use_cache=1'
1300	2025-12-02 03:23:09.395	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail No" max_time="1" count="50" use_cache=1'