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
1101	2025-12-02 12:40:20.055	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'
1102	2025-12-02 12:39:58.499	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" | table eventID, userIdentity.userName, requestParameters.bucketName'
1103	2025-12-02 12:39:30.136	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" | table eventID, userIdentity.userName, requestParameters.bucketName'

	_time	user	action	search
1104	2025-12-02 12:39:28.504	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'
1105	2025-12-02 12:39:11.180	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'
1106	2025-12-02 12:38:28.511	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | fieldsummary | search field="*acl*" OR field="*ACL*"'
1107	2025-12-02 12:38:28.492	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats count by _time, eventID, userIdentity.userName | sort -_time'
1108	2025-12-02 12:38:24.219	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | fieldsummary | search field="*acl*" OR field="*ACL*"'
1109	2025-12-02 12:38:05.145	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats count by _time, eventID, userIdentity.userName | sort -_time'

	_time	user	action	search
1110	2025-12-02 12:37:58.578	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(eventName) as events | search events=*Bucket*'
1111	2025-12-02 12:37:58.500	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="[YOUR_EVENT_ID_HERE]" | spath | table *'
1112	2025-12-02 12:37:45.575	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values(eventName) as events | search events=*Bucket*'
1113	2025-12-02 12:37:33.241	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="[YOUR_EVENT_ID_HERE]" | spath | table *'
1114	2025-12-02 12:37:28.485	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | where isnotnull(requestParameters.acl) | stats count by requestParameters.acl'
1115	2025-12-02 12:37:17.471	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | where isnotnull(requestParameters.acl) | stats count by requestParameters.acl'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>116</td><td>2025-12-02 12:36:28.496</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'</td></tr>
<tr><td>117</td><td>2025-12-02 12:36:28.477</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'</td></tr>
<tr><td>118</td><td>2025-12-02 12:36:05.721</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'</td></tr>
<tr><td>119</td><td>2025-12-02 12:35:58.500</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'</td></tr>
<tr><td>120</td><td>2025-12-02 12:35:58.486</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | where (requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read") OR requestParameters.grantList LIKE "%AllUsers%" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'</td></tr>
<tr><td>121</td><td>2025-12-02 12:35:58.331</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'</td></tr>
</table>

	_time	user	action	search
1122	2025-12-02 12:35:53.559	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'
1123	2025-12-02 12:35:36.142	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | where (requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read") OR requestParameters.grantList LIKE "%AllUsers%" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1124	2025-12-02 12:35:28.526	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.grantList=*AllUsers* | table eventID'
1125	2025-12-02 12:35:28.510	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl=*public* OR requestParameters.grantList=*AllUsers* | table eventID'
1126	2025-12-02 12:35:28.487	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | search requestParameters.acl=*public* OR requestParameters.grantList=*AllUsers* | table eventID'
1127	2025-12-02 12:35:19.947	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.grantList=*AllUsers* | table eventID'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>1128</td><td>2025-12-02 12:35:08.746</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl=*public* OR requestParameters.grantList=*AllUsers* | table eventID'</td></tr>
<tr><td>1129</td><td>2025-12-02 12:35:00.436</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | search requestParameters.acl=*public* OR requestParameters.grantList=*AllUsers* | table eventID'</td></tr>
<tr><td>1130</td><td>2025-12-02 12:34:58.515</td><td>kimjoe</td><td>search</td><td>'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail eventName=\"PutBucketAcl\" u" max_time="1" count="50" use_cache=1'</td></tr>
<tr><td>1131</td><td>2025-12-02 12:34:58.504</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'</td></tr>
<tr><td>1132</td><td>2025-12-02 12:34:58.486</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'</td></tr>
<tr><td>1133</td><td>2025-12-02 12:34:48.195</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'</td></tr>
</table>

	_time	user	action	search
1134	2025-12-02 12:34:41.118	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'
1135	2025-12-02 12:34:28.510	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'
1136	2025-12-02 12:34:28.490	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'
1137	2025-12-02 12:34:28.475	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1138	2025-12-02 12:34:23.879	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'
1139	2025-12-02 12:34:20.250	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'

	_time ⇕	user ⇕	action ⇕	search ⇕
1140	2025-12-02 12:34:01.988	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1141	2025-12-02 12:33:58.478	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'
1142	2025-12-02 12:33:30.019	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'
1143	2025-12-02 12:33:28.619	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail eventName=\"PutBucketAcl\" u" max_time="1" count="50" use_cache=1'
1144	2025-12-02 12:33:28.496	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'
1145	2025-12-02 12:33:28.474	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'

	_time	user	action	search
1146	2025-12-02 12:33:09.442	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList | head 1'
1147	2025-12-02 12:32:58.472	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.grantList=*AllUsers* OR requestParameters.grantList=*Everyone* | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.grantList'
1148	2025-12-02 12:32:58.408	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="btaylor" | table eventID, _time, requestParameters.bucketName, requestParameters.acl'
1149	2025-12-02 12:32:48.750	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.grantList=*AllUsers* OR requestParameters.grantList=*Everyone* | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.grantList'
1150	2025-12-02 12:32:28.471	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1151	2025-12-02 12:32:28.457	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'

	_time	user	action	search
1152	2025-12-02 12:32:25.683	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1153	2025-12-02 12:32:13.420	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1154	2025-12-02 12:31:58.465	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1155	2025-12-02 12:31:55.276	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | search requestParameters.acl="public-read" OR requestParameters.acl="public-read-write" OR requestParameters.acl="authenticated-read" | table eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl'
1156	2025-12-02 12:30:28.468	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
1157	2025-12-02 12:30:17.854	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'

	_time	user	action	search
1158	2025-12-02 12:28:58.457	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
1159	2025-12-02 12:28:45.410	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
1160	2025-12-02 11:27:58.776	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count by host'
1161	2025-12-02 11:27:58.710	kimjoe	search	'search index=botsv3 sourcetype=hardware'
1162	2025-12-02 11:27:58.652	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'
1163	2025-12-02 11:27:50.654	kimjoe	search	'search index=botsv3 sourcetype=hardware'

	_time	user	action	search
1164	2025-12-02 11:27:34.520	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'
1165	2025-12-02 11:27:28.796	kimjoe	search	'search index=botsv3 sourcetype=hardware | regex host="(web|www|http|iis|apache|nginx)" | table host, processor'
1166	2025-12-02 11:27:28.751	kimjoe	search	'search index=botsv3 sourcetype=*http* | stats count by sourcetype, host'
1167	2025-12-02 11:27:16.502	kimjoe	search	'search index=botsv3 sourcetype=hardware | regex host="(web|www|http|iis|apache|nginx)" | table host, processor'
1168	2025-12-02 11:26:59.316	kimjoe	search	'| search (index=botsv3 sourcetype=hardware) | dedup host | table host, processor, os'
1169	2025-12-02 11:26:59.241	kimjoe	search	'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] '

	_time	user	action	search
1170	2025-12-02 11:26:53.030	kimjoe	search	'search index=botsv3 sourcetype=*http* | stats count by sourcetype, host'
1171	2025-12-02 11:26:31.187	kimjoe	search	'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] '
1172	2025-12-02 11:26:29.258	kimjoe	search	'| search (index=botsv3 sourcetype=hardware) | dedup host | table host, processor, os'
1173	2025-12-02 11:26:29.194	kimjoe	search	'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'
1174	2025-12-02 11:26:28.846	kimjoe	search	'search index=botsv3 sourcetype=stream:http | stats dc(host) as unique_web_hosts'
1175	2025-12-02 11:26:14.651	kimjoe	search	'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'

	_time	user	action	search
1176	2025-12-02 11:25:58.566	kimjoe	search	'search index=botsv3 sourcetype=hardware | search os=*Server* | stats values(processor) as server_processors by host | table host, server_processors'
1177	2025-12-02 11:25:53.102	kimjoe	search	'search index=botsv3 sourcetype=stream:http | stats dc(host) as unique_web_hosts'
1178	2025-12-02 11:25:28.636	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count by host | where (count > 0)'
1179	2025-12-02 11:25:28.570	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 | eval processors = mvdedup(processors) | table processors'
1180	2025-12-02 11:25:28.290	kimjoe	search	'search index=botsv3 sourcetype=hardware | search os=*Server* | stats values(processor) as server_processors by host | table host, server_processors'
1181	2025-12-02 11:25:01.335	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 | eval processors = mvdedup(processors) | table processors'

	_time	user	action	search
1182	2025-12-02 11:24:28.609	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count by host | where (count > 0)'
1183	2025-12-02 11:24:28.570	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'
1184	2025-12-02 11:24:10.542	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'
1185	2025-12-02 11:23:58.679	kimjoe	search	'| search (index=botsv3 sourcetype=stream:http) | stats count as http_events by host'
1186	2025-12-02 11:23:58.643	kimjoe	search	'search index=botsv3 sourcetype=hardware | search (host=*www* OR host=*web* OR host=*http* OR host=*iis* OR host=*apache*) | table host, processor'
1187	2025-12-02 11:23:58.586	kimjoe	search	'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'

	_time	user	action	search
1188	2025-12-02 11:23:56.089	kimjoe	search	'search index=botsv3 sourcetype=hardware | search (host=*www* OR host=*web* OR host=*http* OR host=*iis* OR host=*apache*) | table host, processor'
1189	2025-12-02 11:23:38.267	kimjoe	search	'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'
1190	2025-12-02 11:23:28.991	kimjoe	search	'search index=botsv3 sourcetype=hardware | search os=*Server* AND (processor=*) | table host, processor, os'
1191	2025-12-02 11:23:28.913	kimjoe	search	'search index=botsv3 sourcetype=* | search host=*web* OR category=*web* OR type=*web* OR os=*web* | table host, processor, os, category, type'
1192	2025-12-02 11:23:23.550	kimjoe	search	'search index=botsv3 sourcetype=hardware | search os=*Server* AND (processor=*) | table host, processor, os'
1193	2025-12-02 11:22:59.002	kimjoe	search	'| search (index=botsv3 sourcetype=hardware) | dedup host | table host, processor'

	_time	user	action	search
1194	2025-12-02 11:22:58.961	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'
1195	2025-12-02 11:22:33.863	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'
1196	2025-12-02 11:22:28.623	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host, processor, os, category, type'
1197	2025-12-02 11:22:28.549	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'
1198	2025-12-02 11:22:15.404	kimjoe	search	'search index=botsv3 sourcetype=hardware | table host, processor, os, category, type'
1199	2025-12-02 11:22:00.370	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'

	_time	user	action	search
1200	2025-12-02 11:21:40.154	kimjoe	search	'search index=botsv3 sourcetype=* | search host=*web* OR category=*web* OR type=*web* OR os=*web* | table host, processor, os, category, type'