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
101	2025-12-11 17:47:14.453	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
102	2025-12-11 17:42:48.310	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
103	2025-12-11 17:42:37.497	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
104	2025-12-11 17:39:18.321	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'

	_time	user	action	search
105	2025-12-11 17:39:11.850	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
106	2025-12-11 17:32:18.495	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
107	2025-12-11 17:31:58.144	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
108	2025-12-11 17:23:18.345	kimjoe	search	'typeahead prefix="metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000" max_time="1" count="50" use_cache=1'
109	2025-12-11 17:23:18.337	kimjoe	search	'|metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
110	2025-12-11 17:22:53.453	kimjoe	search	'|metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
111	2025-12-11 17:22:18.362	kimjoe	search	'|metasearch index=botsv3 sourcetype=aws:cloudtrail field user* |head 10000'
112	2025-12-11 17:22:18.343	kimjoe	search	'|metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000'

	_time	user	action	search
113	2025-12-11 17:22:14.806	kimjoe	search	'|metasearch index=botsv3 sourcetype=aws:cloudtrail field user* |head 10000'
114	2025-12-11 17:22:03.228	kimjoe	search	'|metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000'
115	2025-12-11 17:21:58.092	kimjoe	search	'typeahead prefix="metasearch index=botsv3 sourcetype=aws:cloudtrail field user* head 10000" max_time="1" count="50" use_cache=1'
116	2025-12-11 17:21:48.380	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:*'
117	2025-12-11 17:21:37.068	kimjoe	search	'| metasearch index=botsv3 sourcetype=aws:*'
118	2025-12-11 17:21:18.328	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
119	2025-12-11 17:21:08.544	kimjoe	search	'| metadata type=sourcetypes index=botsv3 stats values(sourcetype)'
120	2025-12-11 17:20:48.383	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values(userIdentity.sessionContext.attributes.mfaAuthenticated)'

	_time	user	action	search
121	2025-12-11 17:20:32.916	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values (userIdentity.sessionContext.attributes.mfaAuthenticated)'
122	2025-12-11 15:09:18.380	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values (userIdentity.sessionContext.attributes.mfaAuthenticated)'
123	2025-12-11 15:08:59.157	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values (userIdentity.sessionContext.attributes.mfaAuthenticated)'
124	2025-12-11 12:43:18.642	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values (userIdentity.sessionContext.attributes.mfaAuthenticated)'
125	2025-12-11 12:43:01.264	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values (userIdentity.sessionContext.attributes.mfaAuthenticated)'
126	2025-12-11 12:42:48.677	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values (userIdentity.userName)'
127	2025-12-11 12:42:27.919	kimjoe	search	'search index=botsv3 sourcetype="aws:cloudtrail" | stats values (userIdentity.userName)'
128	2025-12-11 12:42:18.366	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*" host=BSTOLL-L.froth.ly | stats values(EventCode)'

	_time	user	action	search
129	2025-12-11 12:42:09.351	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*" host=BSTOLL-L.froth.ly | stats values(EventCode)'
130	2025-12-11 01:17:30.071	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*" host=BSTOLL-L.froth.ly | stats values(EventCode)'
131	2025-12-11 01:17:05.446	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*" host=BSTOLL-L.froth.ly | stats values(EventCode)'
132	2025-12-11 01:17:00.139	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*" | stats count by host'
133	2025-12-11 01:16:37.499	kimjoe	search	'search index=botsv3 sourcetype="WinEventLog:*" | stats count by host'
134	2025-12-11 01:14:30.105	kimjoe	search	'search index=botsv3 sourcetype=WinHostMon host!=BSTOLL-L.froth.ly | stats values(os_version) by host'
135	2025-12-11 01:14:00.073	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* host=BSTOLL-L.froth.ly | rex field=_raw "(?<version>\d+\.\d+\.\d+)" | stats values(version)'
136	2025-12-11 01:14:00.056	kimjoe	search	'search index=botsv3 sourcetype=WinHostMon host=BSTOLL-L.froth.ly | table host os os_version build_number'

	_time	user	action	search
137	2025-12-11 01:13:56.189	kimjoe	search	'search index=botsv3 sourcetype=WinHostMon host!=BSTOLL-L.froth.ly | stats values(os_version) by host'
138	2025-12-11 01:13:42.621	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* host=BSTOLL-L.froth.ly | rex field=_raw "(?<version>\d+\.\d+\.\d+)" | stats values(version)'
139	2025-12-11 01:13:34.370	kimjoe	search	'search index=botsv3 sourcetype=WinHostMon host=BSTOLL-L.froth.ly | table host os os_version build_number'
140	2025-12-11 01:13:30.071	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:System host=BSTOLL-L.froth.ly | table _time ComputerName Version ProductName'
141	2025-12-11 01:13:20.250	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:System host=BSTOLL-L.froth.ly | table _time ComputerName Version ProductName'
142	2025-12-10 23:55:00.426	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval User=lower(mvindex(split(computer, "-"), 0)) | eval Role=case(match(computer, "BSTOLL-L\.froth\.ly"), "Suspect Workstation", match(computer, "SEPM"), "Security Server", match(computer, "-L\.froth\.ly$"), "Standard Workstation", true(), "Other") | stats count as TotalEvents, values(User) as AssociatedUser by computer, Role | sort -TotalEvents | eval SuspectDevice=if(match(computer, "BSTOLL-L"), "Suspect", "Normal") | eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 2) | table computer, AssociatedUser, Role, TotalEvents, RelativeActivity, SuspectDevice'

	_time	user	action	search
143	2025-12-10 23:54:24.837	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval User=lower(mvindex(split(computer, "-"), 0)) | eval Role=case(match(computer, "BSTOLL-L\.froth\.ly"), "Suspect Workstation", match(computer, "SEPM"), "Security Server", match(computer, "-L\.froth\.ly$"), "Standard Workstation", true(), "Other") | stats count as TotalEvents, values(User) as AssociatedUser by computer, Role | sort -TotalEvents | eval SuspectDevice=if(match(computer, "BSTOLL-L"), "Suspect", "Normal") | eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 2) | table computer, AssociatedUser, Role, TotalEvents, RelativeActivity, SuspectDevice'
144	2025-12-10 23:53:30.460	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count as TotalEvents by computer | eval RelativeActivity = round(TotalEvents*100/sum(TotalEvents), 2) | sort -TotalEvents'
145	2025-12-10 23:53:09.338	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count as TotalEvents by computer | eval RelativeActivity = round(TotalEvents*100/sum(TotalEvents), 2) | sort -TotalEvents'
146	2025-12-10 23:52:30.435	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval User=lower(mvindex(split(computer, "-"), 0)) | eval Role=case(match(computer, "BSTOLL-L\.froth\.ly"), "Suspect Workstation", match(computer, "SEPM"), "Security Server", match(computer, "-L\.froth\.ly$"), "Standard Workstation", true(), "Other") | stats count as TotalEvents, values(User) as AssociatedUser by computer, Role | sort -TotalEvents'

	_time	user	action	search
147	2025-12-10 23:52:13.347	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval User=lower(mvindex(split(computer, "-"), 0)) | eval Role=case(match(computer, "BSTOLL-L\.froth\.ly"), "Suspect Workstation", match(computer, "SEPM"), "Security Server", match(computer, "-L\.froth\.ly$"), "Standard Workstation", true(), "Other") | stats count as TotalEvents, values(User) as AssociatedUser by computer, Role | sort -TotalEvents'
148	2025-12-10 23:51:30.359	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern | sort -count'
149	2025-12-10 23:51:06.270	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval pattern = if(match(computer, "-L\.froth\.ly$"), "Client Pattern", "Different") | stats count by computer, pattern | sort -count'
150	2025-12-10 23:50:30.390	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
151	2025-12-10 23:50:10.621	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<fqdn>[^\s]+)" | stats count by fqdn'
152	2025-12-10 23:49:30.210	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*windows*" OR sourcetype="*win*" OR sourcetype="*os*"'

	_time	user	action	search
153	2025-12-10 23:49:13.237	kimjoe	search	'| metadata type=sourcetypes index=botsv3 | search sourcetype="*windows*" OR sourcetype="*win*" OR sourcetype="*os*"'
154	2025-12-10 23:47:30.404	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by host'
155	2025-12-10 23:47:06.728	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats count by host'
156	2025-12-10 23:46:30.191	kimjoe	search	'search
157	2025-12-10 23:46:26.099	kimjoe	search	'search
158	2025-12-10 23:45:30.137	kimjoe	search	'search
159	2025-12-10 23:44:59.005	kimjoe	search	'search
160	2025-12-10 23:44:30.153	kimjoe	search	'search

	_time	user	action	search
161	2025-12-10 23:44:14.145	kimjoe	search	'search
162	2025-12-10 23:43:30.218	kimjoe	search	'search
163	2025-12-10 23:43:24.463	kimjoe	search	'search
164	2025-12-10 23:42:30.167	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(requestParameters.bucketName) as bucketName'
165	2025-12-10 23:42:25.497	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(requestParameters.bucketName) as bucketName'
166	2025-12-10 23:40:30.195	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
167	2025-12-10 23:40:30.145	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
168	2025-12-10 23:40:00.235	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search requestParameters.bucketName="frothlywebcode" | head 5 | table _time, bucket, operation, key'

	_time	user	action	search
169	2025-12-10 23:39:34.583	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search requestParameters.bucketName="frothlywebcode" | head 5 | table _time, bucket, operation, key'
170	2025-12-10 23:39:07.302	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
171	2025-12-10 23:39:06.267	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
172	2025-12-10 23:38:00.158	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail requestParameters.bucketName="frothlywebcode" | stats count by eventName'
173	2025-12-10 23:37:32.506	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail requestParameters.bucketName="frothlywebcode" | stats count by eventName'
174	2025-12-10 23:37:00.151	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search bucket="frothlywebcode" | head 5 | table _time, bucket, operation, key'
175	2025-12-10 23:36:30.133	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search bucket="frothlywebcode" | head 5 | table _time, bucket, operation, key'
176	2025-12-10 23:36:00.151	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(requestParameters.bucketName) as bucketName'

	_time	user	action	search
1777	2025-12-10 23:35:45.716	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(requestParameters.bucketName) as bucketName'
1778	2025-12-10 23:35:00.134	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | head 5 | table _time, eventName, eventSource, sourceIPAddress'
1779	2025-12-10 23:34:40.864	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | head 5 | table _time, eventName, eventSource, sourceIPAddress'
1780	2025-12-10 23:34:00.216	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | stats count by eventName | sort -count'
1781	2025-12-10 23:33:31.935	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | stats count by eventName | sort -count'
1782	2025-12-10 23:32:30.161	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'
1783	2025-12-10 23:32:12.513	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'
1784	2025-12-10 23:30:30.208	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'

	_time	user	action	search
185	2025-12-10 23:30:30.133	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table'
186	2025-12-10 23:30:14.185	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
187	2025-12-10 23:30:08.078	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table'
188	2025-12-10 23:30:00.130	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table raw,*'
189	2025-12-10 23:29:52.656	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table raw,*'
190	2025-12-10 23:29:30.130	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
191	2025-12-10 23:29:07.979	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
192	2025-12-10 23:27:00.126	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'

	_time	user	action	search
193	2025-12-10 23:26:31.547	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
194	2025-12-10 23:24:30.127	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
195	2025-12-10 23:24:14.671	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
196	2025-12-10 23:23:30.118	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
197	2025-12-10 23:23:04.497	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
198	2025-12-10 23:23:00.114	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters, requestParameters.acl, requestParameters.grantList'
199	2025-12-10 23:22:54.609	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters, requestParameters.acl, requestParameters.grantList'

	_time	user	action	search
200	2025-12-10 20:47:23.046	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters, requestParameters.acl, requestParameters.grantList'