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
1601	2025-12-02 01:59:43.333	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
1602	2025-12-02 01:59:39.402	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrai" max_time="1" count="50" use_cache=1'
1603	2025-12-02 01:59:39.391	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"a" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1604	2025-12-02 01:59:39.379	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=" max_time="1" count="50" use_cache=1'
1605	2025-12-02 01:59:39.364	kimjoe	search	'typeahead prefix="index=\"botsv3\" so" max_time="1" count="50" use_cache=1'
1606	2025-12-02 01:59:39.349	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
1607	2025-12-02 01:59:34.751	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
1608	2025-12-02 01:58:39.328	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'
1609	2025-12-02 01:58:23.183	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | head 5 | table _time, eventName, userIdentity.*'

	_time	user	action	search
1610	2025-12-02 01:58:21.677	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"aws:cloudtrai" max_time="1" count="50" use_cache=1'
1611	2025-12-02 01:58:20.958	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=\"a" max_time="1" count="50" use_cache=1'
1612	2025-12-02 01:58:19.689	kimjoe	search	'typeahead prefix="index=\"botsv3\" sourcetype=" max_time="1" count="50" use_cache=1'
1613	2025-12-02 01:58:18.297	kimjoe	search	'typeahead prefix="index=\"botsv3\" so" max_time="1" count="50" use_cache=1'
1614	2025-12-02 01:58:09.387	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1615	2025-12-02 01:58:09.373	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'

	_time	user	action	search
1616	2025-12-02 01:58:09.354	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1617	2025-12-02 01:58:06.636	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1618	2025-12-02 01:57:56.111	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1619	2025-12-02 01:57:45.231	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1620	2025-12-02 01:57:39.341	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1621	2025-12-02 01:57:39.325	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'

	_time	user	action	search
1622	2025-12-02 01:57:18.414	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1623	2025-12-02 01:57:11.921	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1624	2025-12-02 01:57:09.386	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1625	2025-12-02 01:57:09.374	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1626	2025-12-02 01:57:06.203	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1627	2025-12-02 01:56:40.880	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'

	_time	user	action	search
1628	2025-12-02 01:56:39.348	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity, userIdentity.type, userIdentity.userName.*'
1629	2025-12-02 01:56:15.530	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity, userIdentity.type, userIdentity.userName.*'
1630	2025-12-02 01:56:09.375	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity, userIdentity.type, userIdentity.userName.'
1631	2025-12-02 01:55:57.139	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity, userIdentity.type, userIdentity.userName.'
1632	2025-12-02 01:55:09.392	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1633	2025-12-02 01:55:09.377	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'

	_time	user	action	search
1634	2025-12-02 01:55:09.366	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1635	2025-12-02 01:54:54.707	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1636	2025-12-02 01:54:52.033	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1637	2025-12-02 01:54:48.996	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1638	2025-12-02 01:54:39.328	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1639	2025-12-02 01:54:35.181	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'

	_time	user	action	search
1640	2025-12-02 01:50:09.366	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1641	2025-12-02 01:50:09.350	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1642	2025-12-02 01:50:08.413	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1643	2025-12-02 01:49:46.636	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1644	2025-12-02 01:49:39.336	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 10 | table _time, eventName, userIdentity.*'
1645	2025-12-02 01:49:39.322	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 10 | table _time, eventName, userIdentity.*'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>1646</td><td>2025-12-02 01:49:34.076</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | head 10 | table _time, eventName, userIdentity.*'</td></tr>
<tr><td>1647</td><td>2025-12-02 01:49:22.290</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | head 10 | table _time, eventName, userIdentity.*'</td></tr>
<tr><td>1648</td><td>2025-12-02 01:49:09.331</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'</td></tr>
<tr><td>1649</td><td>2025-12-02 01:49:03.745</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'</td></tr>
<tr><td>1650</td><td>2025-12-02 01:48:09.354</td><td>kimjoe</td><td>search</td><td>' search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",") '</td></tr>
<tr><td>1651</td><td>2025-12-02 01:48:09.347</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",")] | table unique_users, answer'</td></tr>
</table>

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>1652</td><td>2025-12-02 01:47:51.528</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats dc(userIdentity.userName) as unique_users | appendcols [search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = sort(usernames) | eval answer = mvjoin(usernames, ",")] | table unique_users, answer'</td></tr>
<tr><td>1653</td><td>2025-12-02 01:47:39.340</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'</td></tr>
<tr><td>1654</td><td>2025-12-02 01:47:39.328</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = sort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'</td></tr>
<tr><td>1655</td><td>2025-12-02 01:47:25.486</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | dedup userIdentity.userName | table userIdentity.userName'</td></tr>
<tr><td>1656</td><td>2025-12-02 01:47:11.675</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = sort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'</td></tr>
</table>

	_time	user	action	search
1657	2025-12-02 01:47:09.368	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = sort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
1658	2025-12-02 01:47:09.351	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
1659	2025-12-02 01:46:59.997	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames | eval usernames = mvdedup(usernames) | eval usernames = mvmap(usernames, lower(usernames)) | eval sorted_usernames = sort(usernames) | eval answer = mvjoin(sorted_usernames, ",") | table answer'
1660	2025-12-02 01:46:39.586	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
1661	2025-12-02 01:46:39.341	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'

	_time	user	action	search
1662	2025-12-02 01:46:16.132	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | head 5 | table _time, eventName, userIdentity.userName, userIdentity.type'
1663	2025-12-02 01:46:09.312	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1664	2025-12-02 01:45:48.125	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | head 5 | table _time, eventName, userIdentity.*'
1665	2025-12-02 01:20:39.350	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values (additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'
1666	2025-12-02 01:20:39.337	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'
1667	2025-12-02 01:20:35.844	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | stats values (additionalEventData.MFAUsed) AS MFAUsed, values(userIdentity.sessionContext.attributes.mfaAuthenticated) AS mfaAuthenticated'

<table>
<tr><th></th><th>_time</th><th>user</th><th>action</th><th>search</th></tr>
<tr><td>1668</td><td>2025-12-02 01:20:13.826</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count'</td></tr>
<tr><td>1669</td><td>2025-12-02 01:20:09.319</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | search "MFAUsed" | head 5 | table _time, eventName, additionalEventData.MFAUsed'</td></tr>
<tr><td>1670</td><td>2025-12-02 01:19:58.522</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail | search "MFAUsed" | head 5 | table _time, eventName, additionalEventData.MFAUsed'</td></tr>
<tr><td>1671</td><td>2025-12-02 01:19:39.340</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'</td></tr>
<tr><td>1672</td><td>2025-12-02 01:19:10.237</td><td>kimjoe</td><td>search</td><td>'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users)'</td></tr>
<tr><td>1673</td><td>2025-12-02 01:19:09.321</td><td>kimjoe</td><td>search</td><td>'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'</td></tr>
</table>

	_time	user	action	search
1674	2025-12-02 01:18:52.413	kimjoe	search	'search index="botsv3" sourcetype="aws:cloudtrail" | stats count by userIdentity.userName | rename userIdentity.userName AS "IAM_User"'
1675	2025-12-02 01:18:09.302	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users) | eval IAM_Users = replace(IAM_Users, "\s+", ",")'
1676	2025-12-02 01:18:05.555	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users) | eval IAM_Users = replace(IAM_Users, "\s+", ",")'
1677	2025-12-02 01:16:09.307	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search "*mfa*" OR "*MFA*" | head 1 | fieldsummary'
1678	2025-12-02 01:16:00.520	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search "*mfa*" OR "*MFA*" | head 1 | fieldsummary'
1679	2025-12-02 01:15:39.336	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users) | eval IAM_Users = replace(IAM_Users, "\s+", ",")'

	_time	user	action	search
1680	2025-12-02 01:15:09.650	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) AS IAM_Users | eval IAM_Users = mvdedup(IAM_Users) | eval IAM_Users = replace(IAM_Users, "\s+", ",")'
1681	2025-12-02 01:15:09.373	kimjoe	search	'search index=botsv3 | stats count'
1682	2025-12-02 01:14:57.936	kimjoe	search	'search index=botsv3 | stats count'
1683	2025-12-02 00:14:09.348	kimjoe	search	'search index=botsv3 | stats earliest(_time) as start, latest (_time) as end'
1684	2025-12-02 00:13:46.640	kimjoe	search	'search index=botsv3 | stats earliest(_time) as start, latest (_time) as end'
1685	2025-12-01 02:54:40.580	kimjoe	search	'search index=botsv3 | stats earliest(_time) as start, latest (_time) as end'

	_time	user	action	search
1686	2025-12-01 02:54:40.522	kimjoe	search	'search index=botsv3 | stats count by sourcetype index=botsv3 | stats earliest(_time) as start, latest(_time) as end'
1687	2025-12-01 02:54:24.766	kimjoe	search	'search index=botsv3 | stats earliest(_time) as start, latest(_time) as end'
1688	2025-12-01 02:54:16.848	kimjoe	search	'search index=botsv3 | stats count by sourcetype index=botsv3 | stats earliest(_time) as start, latest(_time) as end'
1689	2025-12-01 02:53:40.553	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
1690	2025-12-01 02:53:40.541	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
1691	2025-12-01 02:53:31.727	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'

	_time	user	action	search
1692	2025-12-01 02:53:18.677	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
1693	2025-12-01 02:53:10.576	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count'
1694	2025-12-01 02:53:10.562	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
1695	2025-12-01 02:53:03.723	kimjoe	search	'search index=botsv3 sourcetype=winhostmon | stats dc(host) as host_count by os | sort host_count'
1696	2025-12-01 02:52:55.117	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search http_method="PUT" http_status=200 | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri'
1697	2025-12-01 02:52:40.535	kimjoe	search	'typeahead prefix="index=botsv3 sourcetype=aws:s3:accesslogs" max_time="1" count="50" use_cache=1'

	_time	user	action	search
1698	2025-12-01 02:52:40.519	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
1699	2025-12-01 02:52:17.870	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
1700	2025-12-01 02:52:10.545	kimjoe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | search object="*.txt" OR uri="*.txt" | table _time, bucket, object, uri, http_method, http_status'