

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)

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
301	2025-12-10 20:05:23.033	kimjoe	search	'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 = mvsort(usernames) eval answer = mvjoin(usernames, ",")] table unique_users, answer'
302	2025-12-10 20:05:19.831	kimjoe	search	'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 = mvsort(usernames) eval answer = mvjoin(usernames, ",")] table unique_users, answer'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
303	2025-12-10 20:04:53.049	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 = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
304	2025-12-10 20:04:33.793	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 = mvsort(usernames) eval answer = mvjoin(sorted_usernames, ",") table answer'
305	2025-12-10 20:03:53.049	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
306	2025-12-10 20:03:41.726	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" stats values(userIdentity.userName) as usernames'
307	2025-12-10 20:02:23.112	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'

	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>
	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div>
308	2025-12-10 20:02:23.094	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, "SEP M"), "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'	
309	2025-12-10 20:02:17.809	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail head 5 table _time, eventName, userIdentity.*'	
310	2025-12-10 20:01:58.361	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, "SEP M"), "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	
3 1 1	2025-12-09 13:56:22.1 64	kimj oe	sear ch	'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, "SEP M"), "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'	
3 1 2	2025-12-09 13:55:52.1 61	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer'	
3 1 3	2025-12-09 13:55:51.0 87	kimj oe	sear ch	'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, "SEP M"), "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'	
3 1 4	2025-12-09 13:55:38.5 39	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer'	

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
315	2025-12-09 13:55:22.405	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, "SEP M"), "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'
316	2025-12-09 13:55:00.741	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, "SEP M"), "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'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
317	2025-12-09 13:53:22.283	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"), "**INVESTIGATION TARGET**", 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"), "Primary (bstoll'
318	2025-12-09 13:52:55.209	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"), "**INVESTIGATION TARGET**", 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"), "Primary (bstoll'
319	2025-12-09 13:52:52.337	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex "ComputerName=(?<computer>\\S+)" eval user_from_host=lower(mvindex(split(computer, "-"), 0)) where computer="BSTOLL-L.froth.ly" OR computer="SEPM" stats count as events by computer, user_from_host eval investigation_status=if(computer="BSTOLL-L.froth.ly", "PRIMARY TARGET - Bud'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
3 2 0	2025-12-09 13:52:30.088	kimj oe	search	'search index=botsv3 sourcetype=WinEventLog:* rex "ComputerName=(?<computer>\S+)" eval user_from_host=lower(mvindex(split(computer, "-"), 0)) where computer="BSTOLL-L.froth.ly" OR computer="SEPM" stats count as events by computer, user_from_host eval investigation_status=if(computer="BSTOLL-L.froth.ly", "PRIMARY TARGET - Bud'
3 2 1	2025-12-09 13:51:52.094	kimj oe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>^\s+)" eval ExtractedUser=lower(mvindex(split(computer, "-"), 0)) eval UserDeviceMatch=case(computer="BSTOLL-L.froth.ly" AND ExtractedUser="bstoll", "✓ Direct Match (Suspect)", match(computer, "-L\.froth\.ly\$"), "Standard User Device", true(), "Other/Server") eval Relevance=case(ExtractedUser="bstoll", "**PRIMARY SUSPECT** - Bud'
3 2 2	2025-12-09 13:51:42.555	kimj oe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>^\s+)" eval ExtractedUser=lower(mvindex(split(computer, "-"), 0)) eval UserDeviceMatch=case(computer="BSTOLL-L.froth.ly" AND ExtractedUser="bstoll", "✓ Direct Match (Suspect)", match(computer, "-L\.froth\.ly\$"), "Standard User Device", true(), "Other/Server") eval Relevance=case(ExtractedUser="bstoll", "**PRIMARY SUSPECT** - Bud'






	<div><div><div></div><div>_time</div><div></div></div></div>	<div><div><div></div><div>user</div><div></div></div></div>	<div><div><div></div><div>action</div><div></div></div></div>	<div><div><div></div><div>search</div><div></div></div></div>
323	2025-12-09 13:51:22.228	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"), "**INVESTIGATION TARGET**", 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"), "Primary (bstoll'
324	2025-12-09 13:51:22.152	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval User=lower(mvindex(split(computer, "-"), 0)) eval Pattern=case(match(computer, "BSTOLL-L\\.froth\\.ly"), "Primary Suspect'
325	2025-12-09 13:51:14.649	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"), "**INVESTIGATION TARGET**", 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"), "Primary (bstoll'
326	2025-12-09 13:50:53.651	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval User=lower(mvindex(split(computer, "-"), 0)) eval Pattern=case(match(computer, "BSTOLL-L\\.froth\\.ly"), "Primary Suspect'









	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
3 2 7	2025-12-09 13:48:52.233	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.froth\.ly"), "**Investigation Target** (bstol l'
3 2 8	2025-12-09 13:48:52.155	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.froth\.ly"), "**Investigation Target** (bstol l'
3 2 9	2025-12-09 13:48:48.084	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.froth\.ly"), "**Investigation Target** (bstol l'
3 3 0	2025-12-09 13:48:24.676	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.froth\.ly"), "**Investigation Target** (bstol l'
3 3 1	2025-12-09 13:48:22.148	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.froth\.ly"), "**Investigation Target** (bstol l'
3 3 2	2025-12-09 13:48:12.189	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.froth\.ly"), "**Investigation Target** (bstol l'

	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>
	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>	<div><div><div><div></div></div><div><div></div></div></div><div><div></div></div><div><div></div></div></div>
3	2025-12-09 13:47:52.2	kimj	sear	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw
3	24	oe	ch	"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(sp
3				lit(computer, "-"), 0)) stats count as ActivityCount by compu
				ter, User sort -ActivityCount eval is_bstoll=if(match(compu
				ter, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
3	2025-12-09 13:47:52.1	kimj	sear	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw
3	45	oe	ch	"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(sp
4				lit(computer, "-"), 0)) stats count as ActivityCount by compu
				ter, User sort -ActivityCount eval is_bstoll=if(match(compu
				ter, "BSTOLL-L"), "PRIMARY SUSPECT", "Other") eval RelativeAc
				tivity=round(TotalEvents*100/sum(TotalEvents), 1)'
3	2025-12-09 13:47:38.4	kimj	sear	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw
3	13	oe	ch	"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(sp
5				lit(computer, "-"), 0)) stats count as ActivityCount by compu
				ter, User sort -ActivityCount eval is_bstoll=if(match(compu
				ter, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
3	2025-12-09 13:47:24.0	kimj	sear	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw
3	89	oe	ch	"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(sp
6				lit(computer, "-"), 0)) stats count as ActivityCount by compu
				ter, User sort -ActivityCount eval is_bstoll=if(match(compu
				ter, "BSTOLL-L"), "PRIMARY SUSPECT", "Other") eval RelativeAc
				tivity=round(TotalEvents*100/sum(TotalEvents), 1)'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
3	2025-12-09 13:47:22.2	kimj	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw
3	25	oe		"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(split(computer, "-"), 0)) stats count as ActivityCount by computer, User sort -ActivityCount eval is_bstoll=if(match(computer, "BSTOLL-L"), "PRIMARY SUSPECT", "Other") eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 1) table computer, Role, TotalEvents, RelativeActivity'
7				
3	2025-12-09 13:47:22.1	kimj	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw
3	49	oe		"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(split(computer, "-"), 0)) stats count as ActivityCount by computer, User sort -ActivityCount eval is_bstoll=if(match(computer, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
8				
3	2025-12-09 13:47:08.7	kimj	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw
3	91	oe		"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(split(computer, "-"), 0)) stats count as ActivityCount by computer, User sort -ActivityCount eval is_bstoll=if(match(computer, "BSTOLL-L"), "PRIMARY SUSPECT", "Other") eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 1) table computer, Role, TotalEvents, RelativeActivity'
9				
3	2025-12-09 13:47:05.0	kimj	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw
4	35	oe		"ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(split(computer, "-"), 0)) stats count as ActivityCount by computer, User sort -ActivityCount eval is_bstoll=if(match(computer, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
0				






	_time ↕	user ↕ ✎	action ↕ ✎	search ↕
3 4 1	2025-12-09 13:45:52.1 49	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(sp lit(computer, "-"), 0)) stats count as ActivityCount by compu ter, User sort -ActivityCount eval is_bstoll=if(match(compu ter, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
3 4 2	2025-12-09 13:45:29.3 97	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(sp lit(computer, "-"), 0)) stats count as ActivityCount by compu ter, User sort -ActivityCount eval is_bstoll=if(match(compu ter, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
3 4 3	2025-12-09 13:45:22.2 17	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Pattern=case(match(c omputer, "BSTOLL-L\.\froth\.\ly"), "Primary Suspect'
3 4 4	2025-12-09 13:45:22.1 39	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.\froth\.\ly"), "**Investigation Target** (bstol l'
3 4 5	2025-12-09 13:45:02.2 23	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Pattern=case(match(c omputer, "BSTOLL-L\.\froth\.\ly"), "Primary Suspect'
3 4 6	2025-12-09 13:44:49.6 40	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.\froth\.\ly"), "**Investigation Target** (bstol l'









					
	_time	user	action	search	
3 4 7	2025-12-09 13:43:52.1 39	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.\froth\.\ly"), "**Investigation Target** (bstol l'	
3 4 8	2025-12-09 13:43:32.2 25	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Role=case(match(comp uter, "BSTOLL-L\.\froth\.\ly"), "**Investigation Target** (bstol l'	
3 4 9	2025-12-09 13:43:22.1 43	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Pattern=case(match(c omputer, "BSTOLL-L\.\froth\.\ly"), "Primary Suspect'	
3 5 0	2025-12-09 13:43:12.5 77	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval Pattern=case(match(c omputer, "BSTOLL-L\.\froth\.\ly"), "Primary Suspect'	
3 5 1	2025-12-09 13:42:52.2 13	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(sp lit(computer, "-"), 0)) stats count as ActivityCount by compu ter, User sort -ActivityCount eval is_bstoll=if(match(compu ter, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'	
3 5 2	2025-12-09 13:42:52.1 34	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as EventCount by computer sort -EventCount eval Percent=round(EventCount* 100/sum(EventCount), 1) table computer, EventCount, Percent'	







	 _time 	 user 	 action 	 search 
3 5 3	2025-12-09 13:42:47.9 09	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval User=upper(mvindex(split(computer, "-"), 0)) stats count as ActivityCount by computer, User sort -ActivityCount eval is_bstoll=if(match(computer, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
3 5 4	2025-12-09 13:42:32.8 44	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as EventCount by computer sort -EventCount eval Percent=round(EventCount*100/sum(EventCount), 1) table computer, EventCount, Percent'
3 5 5	2025-12-09 12:56:52.4 55	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as total_events by computer sort -total_events eval percentage=round(total_events*100/sum(total_events), 2)'
3 5 6	2025-12-09 12:56:22.5 92	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as total_events by computer sort -total_events eval percentage=round(total_events*100/sum(total_events), 2)'
3 5 7	2025-12-09 12:55:52.8 57	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* "BSTOLL-L.froth.ly" stats count by EventCode, EventType sort -count'
3 5 8	2025-12-09 12:55:24.1 77	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* "BSTOLL-L.froth.ly" stats count by EventCode, EventType sort -count'
3 5 9	2025-12-09 12:55:22.3 59	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as total_events by computer sort -total_events eval percentage=round(total_events*100/sum(total_events), 2)'

	<div><div></div><div>_time ↕</div></div>	<div><div></div><div>user ↕</div></div>	<div><div></div><div>action ↕</div></div>	<div><div></div><div>search ↕</div></div>	<div><div></div><div></div></div>
360	2025-12-09 12:54:52.181	kimjoe	search	'search index=botsv3 *bstoll* stats count'	
361	2025-12-09 12:54:49.809	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as total_events by computer sort -total_events eval percentage=round(total_events*100/sum(total_events), 2)'	
362	2025-12-09 12:54:22.319	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer search computer="*BSTOLL*"'	
363	2025-12-09 12:54:02.359	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer search computer="*BSTOLL*"'	
364	2025-12-09 12:53:52.437	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* stats count by user'	
365	2025-12-09 12:53:31.356	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* stats count by user'	
366	2025-12-09 12:53:11.444	kimjoe	search	'search index=botsv3 *bstoll* stats count'	
367	2025-12-09 12:52:22.536	kimjoe	search	'search index=botsv3 search *bstoll* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer sort -count'	

	<u>_time</u> ⚙	user ⚙	action ⚙	search ⚙
368	2025-12-09 12:47:55.464	kimjoe	search	'search index=botsv3 search *bstoll* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer sort -count'
369	2025-12-09 12:46:52.159	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* (user=bstoll OR userName=bstoll OR userIdentity.userName=bstoll) rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as EventCount by computer sort -EventCount'
370	2025-12-09 12:46:38.682	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* (user=bstoll OR userName=bstoll OR userIdentity.userName=bstoll) rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count as EventCount by computer sort -EventCount'
371	2025-12-09 12:46:22.135	kimjoe	search	'search index=botsv3 (user=bstoll OR userName=bstoll) sourcetype=WinEventLog:* stats count by ComputerName sort -count'
372	2025-12-09 12:46:15.270	kimjoe	search	'search index=botsv3 (user=bstoll OR userName=bstoll) sourcetype=WinEventLog:* stats count by ComputerName sort -count'
373	2025-12-09 12:45:52.151	kimjoe	search	'search index=botsv3 user=bstoll OR userName=bstoll stats count by eventName, host, computer sort -count'
374	2025-12-09 12:45:40.902	kimjoe	search	'search index=botsv3 user=bstoll OR userName=bstoll stats count by eventName, host, computer sort -count'

					
	_time	user	action	search	
3 7 5	2025-12-09 12:40:52.4 16	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval pattern = if(match(computer, "-L\.froth\.ly\$"), "Client Pattern", "Different") stats count by computer, pattern'	
3 7 6	2025-12-09 12:40:22.1 84	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval pattern = if(match(computer, "-L\.froth\.ly\$"), "Client Pattern", "Different") stats count by computer, pattern search pattern="Different"'	
3 7 7	2025-12-09 12:40:17.8 69	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval pattern = if(match(computer, "-L\.froth\.ly\$"), "Client Pattern", "Different") stats count by computer, pattern'	
3 7 8	2025-12-09 12:39:54.2 79	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" eval pattern = if(match(computer, "-L\.froth\.ly\$"), "Client Pattern", "Different") stats count by computer, pattern search pattern="Different"'	
3 7 9	2025-12-09 12:29:52.3 35	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="BSTOLL-L.froth.ly"'	
3 8 0	2025-12-09 12:29:21.2 95	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="BSTOLL-L.froth.ly"'	
3 8 1	2025-12-09 12:28:22.1 95	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="FYODOR-L.froth.ly"'	

	 _time 	 user 	 action 	 search 
3 8 2	2025-12-09 12:27:57.6 02	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="FYODOR-L. froth.ly"'
3 8 3	2025-12-09 12:27:52.4 10	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="ABUNGST- L.froth.ly"'
3 8 4	2025-12-09 12:27:10.3 38	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="ABUNGST- L.froth.ly"'
3 8 5	2025-12-09 12:25:52.6 29	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="BSTOLL-L. froth.ly"'
3 8 6	2025-12-09 12:25:52.3 74	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer'
3 8 7	2025-12-09 12:25:34.6 17	kimj oe	sear ch	'search index=botstv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" search computer="BSTOLL-L. froth.ly"'
3 8 8	2025-12-09 12:25:22.2 57	kimj oe	sear ch	' search (index=botstv3 sourcetype=aws:cloudtrail "userIdentit y.type"="IAMUser") stats values(userIdentity.userName) as use rnames eval usernames=mvdedup(usernames) eval usernames=mvs ort(usernames) eval answer=mvjoin(usernames,",")'

					
	_time	user	action	search	
3 8 9	2025-12-09 12:25:22.202	kimjoe	search	'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 = mvsort(usernames) eval answer = mvjoin(usernames, ",")] table unique_users, answer'	
3 9 0	2025-12-09 12:25:14.144	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer'	
3 9 1	2025-12-09 12:24:56.921	kimjoe	search	'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 = mvsort(usernames) eval answer = mvjoin(usernames, ",")] table unique_users, answer'	
3 9 2	2025-12-09 04:43:11.523	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer'	
3 9 3	2025-12-09 04:42:54.877	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* rex field=_raw "ComputerName=(?<computer>[^\s]+)" stats count by computer'	
3 9 4	2025-12-09 04:40:41.425	kimjoe	search	'search	

	<div><div><div></div><div>_time</div><div></div></div></div>	<div><div><div></div><div>user</div><div></div></div></div>	<div><div><div></div><div>action</div><div></div></div></div>	<div><div><div></div><div>search</div><div></div></div></div>	<div><div><div></div><div></div><div></div></div></div>
395	2025-12-09 04:40:20.812	kimjoe	search	'search	
396	2025-12-09 04:40:11.407	kimjoe	search	'search	
397	2025-12-09 04:39:42.420	kimjoe	search	'search	
398	2025-12-09 04:37:41.410	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" stats values(requestParameters.bucketName) as bucketName'	
399	2025-12-09 04:37:14.367	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" stats values(requestParameters.bucketName) as bucketName'	
400	2025-12-09 04:36:41.447	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" table requestParameters.bucketName'	