

# 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)

		user	acti	
		♦	on ♦	
	_time	✍	✍	search ✍
3	2025-12-10 20:05:23.0	kimj	sear	'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'
0	33	oe	ch	
1				
3	2025-12-10 20:05:19.8	kimj	sear	'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'
0	31	oe	ch	
2				

		user	acti	on	search
3	2025-12-10 20:04:53.0	kimj	sear		'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'
0	49	oe	ch		
3	2025-12-10 20:04:33.7	kimj	sear		'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'
0	93	oe	ch		
4					
3	2025-12-10 20:03:53.0	kimj	sear		'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"   stats values(userIdentity.userName) as usernames'
0	49	oe	ch		
5					
3	2025-12-10 20:03:41.7	kimj	sear		'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser"   stats values(userIdentity.userName) as usernames'
0	26	oe	ch		
6					
3	2025-12-10 20:02:23.1	kimj	sear		'search index=botsv3 sourcetype=aws:cloudtrail   head 5   table _time, eventName, userIdentity.*'
0	12	oe	ch		
7					

			user	acti	on	search	
_time	3 0 8	2025-12-10 20:02:23.0	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\.ly"), "Suspect Workstation", match(computer, "SEP M"), "Security Server", match(computer, "-L\\.froth\\.ly\$"), "Sta ndard Workstation", true(), "Other" )   stats count as TotalEve nts, values(User) as AssociatedUser by computer, Role   sort -T otalEvents   eval SuspectDevice;if(match(computer, "BSTOLL-L"), "Suspect", "Normal")   eval RelativeActivity=round(TotalEvents* 100/sum(TotalEvents), 2)   table computer, AssociatedUser, Rol e, TotalEvents, RelativeActivity, SuspectDevice'		
3 0 9	2025-12-10 20:02:17.8	kimj oe	sear ch	'search index=botsv3 sourcetype=aws:cloudtrail   head 5   table _time, eventName, userIdentity.*'			
3 1 0	2025-12-10 20:01:58.3	kimj oe	sear ch	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\.ly"), "Suspect Workstation", match(computer, "SEP M"), "Security Server", match(computer, "-L\\.froth\\.ly\$"), "Sta ndard Workstation", true(), "Other" )   stats count as TotalEve nts, values(User) as AssociatedUser by computer, Role   sort -T otalEvents   eval SuspectDevice;if(match(computer, "BSTOLL-L"), "Suspect", "Normal")   eval RelativeActivity=round(TotalEvents* 100/sum(TotalEvents), 2)   table computer, AssociatedUser, Rol e, TotalEvents, RelativeActivity, SuspectDevice'			

			user	acti	on		
						search	♦
3	2025-12-09 13:56:22.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\.ly"), "Suspect Workstation", match(computer, "SEP M"), "Security Server", match(computer, "-L\\.froth\\.ly\$"), "Sta ndard Workstation", true(), "Other" )   stats count as TotalEve nts, values(User) as AssociatedUser by computer, Role   sort -T otalEvents   eval SuspectDevice;if(match(computer, "BSTOLL-L"), "Suspect", "Normal")   eval RelativeActivity=round(TotalEvents* 100/sum(TotalEvents), 2)   table computer, AssociatedUser, Rol e, TotalEvents, RelativeActivity, SuspectDevice'			
1	64	oe	ch				
1							
3	2025-12-09 13:55:52.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   stats count by computer'			
1	61	oe	ch				
2							
3	2025-12-09 13:55:51.0	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\.ly"), "Suspect Workstation", match(computer, "SEP M"), "Security Server", match(computer, "-L\\.froth\\.ly\$"), "Sta ndard Workstation", true(), "Other" )   stats count as TotalEve nts, values(User) as AssociatedUser by computer, Role   sort -T otalEvents   eval SuspectDevice;if(match(computer, "BSTOLL-L"), "Suspect", "Normal")   eval RelativeActivity=round(TotalEvents* 100/sum(TotalEvents), 2)   table computer, AssociatedUser, Rol e, TotalEvents, RelativeActivity, SuspectDevice'			
1	87	oe	ch				
3							
3	2025-12-09 13:55:38.5	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   stats count by computer'			
1	39	oe	ch				
4							

		user	acti	on	search
_time	◆				◆
3	2025-12-09 13:55:22.4	kimj	sear		'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\.ly"), "Suspect Workstation", match(computer, "SEP M"), "Security Server", match(computer, "-L\\.froth\\.ly\$"), "Sta ndard Workstation", true(), "Other" )   stats count as TotalEve nts, values(User) as AssociatedUser by computer, Role   sort -T otalEvents   eval SuspectDevice;if(match(computer, "BSTOLL-L"), "Suspect", "Normal")   eval RelativeActivity=round(TotalEvents* 100/sum(TotalEvents), 2)   table computer, AssociatedUser, Rol e, TotalEvents, RelativeActivity, SuspectDevice'
1	05	oe	ch		
5					
3	2025-12-09 13:55:00.7	kimj	sear		'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\.ly"), "Suspect Workstation", match(computer, "SEP M"), "Security Server", match(computer, "-L\\.froth\\.ly\$"), "Sta ndard Workstation", true(), "Other" )   stats count as TotalEve nts, values(User) as AssociatedUser by computer, Role   sort -T otalEvents   eval SuspectDevice;if(match(computer, "BSTOLL-L"), "Suspect", "Normal")   eval RelativeActivity=round(TotalEvents* 100/sum(TotalEvents), 2)   table computer, AssociatedUser, Rol e, TotalEvents, RelativeActivity, SuspectDevice'
1	41	oe	ch		
6					

			user	acti		
			on	on		
					search	sort
3	2025-12-09 13:53:22.2	kimj	sear	ch	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval User=lower(mvindex(split(	
1	83	oe			lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-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'	
7						
3	2025-12-09 13:52:55.2	kimj	sear	ch	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval User=lower(mvindex(split(	
1	09	oe			lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-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'	
8						
3	2025-12-09 13:52:52.3	kimj	sear	ch	'search index=botsv3 sourcetype=WinEventLog:*   rex "ComputerNa	
1	37	oe			me=(?<computer>\\S+)"   eval user_from_host=lower(mvindex(split(	
9					(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'	

			user	acti	on	search
_time						
3	2025-12-09 13:52:30.0	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex "ComputerNa		
2	88	oe	ch	me=(?<computer>\S+)"   eval user_from_host=lower(mvindex(split		
0				(computer, "-"), 0))   where computer="BSTOLL-L.froth.ly" OR co		
				mputer="SEPM"   stats count as events by computer, user_from_ho		
				st   eval investigation_status;if(computer="BSTOLL-L.froth.ly",		
				"PRIMARY TARGET - Bud'		
3	2025-12-09 13:51:52.0	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw		
2	94	oe	ch	"ComputerName=(?<computer>[^\\s]+)"   eval ExtractedUser=lower(m		
1				vindex(split(computer, "-"), 0))   eval UserDeviceMatch=case( c		
				omputer="BSTOLL-L.froth.ly" AND ExtractedUser="bstoll", "✓ Dir		
				ect Match (Suspect)", match(computer, "-L\\.froth\\.ly\$"), "Stand		
				ard User Device", true(), "Other/Server" )   eval Relevance=cas		
				e( ExtractedUser="bstoll", "**PRIMARY SUSPECT** - Bud'		
3	2025-12-09 13:51:42.5	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw		
2	55	oe	ch	"ComputerName=(?<computer>[^\\s]+)"   eval ExtractedUser=lower(m		
2				vindex(split(computer, "-"), 0))   eval UserDeviceMatch=case( c		
				omputer="BSTOLL-L.froth.ly" AND ExtractedUser="bstoll", "✓ Dir		
				ect Match (Suspect)", match(computer, "-L\\.froth\\.ly\$"), "Stand		
				ard User Device", true(), "Other/Server" )   eval Relevance=cas		
				e( ExtractedUser="bstoll", "**PRIMARY SUSPECT** - Bud'		

			user	acti	on	search
_time						
3	2025-12-09 13:51:22.2	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\ly"), "**INVESTIGATION TARGET**", match(computer, "SEPM"), "Security Server", match(computer, "-L\\.froth\\ly\$"), "Standard Workstation", true(), "Other" )   stats count as Tota lEvents, values(User) as AssociatedUser by computer, Role   sor t -TotalEvents   eval SuspectDevice;if(match(computer, "BSTOLL- L"), "Primary (bstoll'		
2	28	oe	ch			
3	2025-12-09 13:51:22.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Pattern=case( match(computer, "B STOLL-L\\.froth\\ly"), "Primary Suspect'		
2	52	oe	ch			
4						
3	2025-12-09 13:51:14.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Role=case( match(computer, "BSTO LL-L\\.froth\\ly"), "**INVESTIGATION TARGET**", match(computer, "SEPM"), "Security Server", match(computer, "-L\\.froth\\ly\$"), "Standard Workstation", true(), "Other" )   stats count as Tota lEvents, values(User) as AssociatedUser by computer, Role   sor t -TotalEvents   eval SuspectDevice;if(match(computer, "BSTOLL- L"), "Primary (bstoll'		
2	49	oe	ch			
5						
3	2025-12-09 13:50:53.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=lower(mvindex(sp lit(computer, "-"), 0))   eval Pattern=case( match(computer, "B STOLL-L\\.froth\\ly"), "Primary Suspect'		
2	51	oe	ch			
6						

		user	acti on	search
_time				
3	2025-12-09 13:48:52.2	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "***Investigation Target** (bstol 1'
2	33	oe	ch	
7				
3	2025-12-09 13:48:52.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "***Investigation Target** (bstol 1'
2	55	oe	ch	
8				
3	2025-12-09 13:48:48.0	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "***Investigation Target** (bstol 1'
2	84	oe	ch	
9				
3	2025-12-09 13:48:24.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "***Investigation Target** (bstol 1'
3	76	oe	ch	
0				
3	2025-12-09 13:48:22.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "***Investigation Target** (bstol 1'
3	48	oe	ch	
1				
3	2025-12-09 13:48:12.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "***Investigation Target** (bstol 1'
3	89	oe	ch	
2				

		user	acti	on	search
_time		⌗	⌗	⌗	⌗
3	2025-12-09 13:47:52.2	kimj	sear	'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	24	oe	ch		
3					
3	2025-12-09 13:47:52.1	kimj	sear	'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")   eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 1)'	
3	45	oe	ch		
4					
3	2025-12-09 13:47:38.4	kimj	sear	'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	13	oe	ch		
5					
3	2025-12-09 13:47:24.0	kimj	sear	'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")   eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 1)'	
3	89	oe	ch		
6					

		user	acti	on	search
_time	time	kimj	sear	oe	ch
3	2025-12-09 13:47:22.2	kimj	sear	oe	ch
3	25				
7					
					'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=upper(mvindex(splitted(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'
3	2025-12-09 13:47:22.1	kimj	sear	oe	ch
3	49				
8					
					'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=upper(mvindex(splitted(computer, "-"), 0))   stats count as ActivityCount by computer, User   sort -ActivityCount   eval is_bstoll;if(match(computer, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'
3	2025-12-09 13:47:08.7	kimj	sear	oe	ch
3	91				
9					
					'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=upper(mvindex(splitted(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'
3	2025-12-09 13:47:05.0	kimj	sear	oe	ch
4	35				
0					
					'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval User=upper(mvindex(splitted(computer, "-"), 0))   stats count as ActivityCount by computer, User   sort -ActivityCount   eval is_bstoll;if(match(computer, "BSTOLL-L"), "PRIMARY SUSPECT", "Other")'

			user	acti	on		search	sort
3	2025-12-09 13:45:52.1	kimj	sear	'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")'				
4	49	oe	ch					
1								
3	2025-12-09 13:45:29.3	kimj	sear	'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")'				
4	97	oe	ch					
2								
3	2025-12-09 13:45:22.2	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Pattern=case( match(c omputer, "BSTOLL-L\\.froth\\.ly"), "Primary Suspect'				
4	17	oe	ch					
3								
3	2025-12-09 13:45:22.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Role=case( match(comp uter, "BSTOLL-L\\.froth\\.ly"), "**Investigation Target** (bstol 1'				
4	39	oe	ch					
4								
3	2025-12-09 13:45:02.2	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Pattern=case( match(c omputer, "BSTOLL-L\\.froth\\.ly"), "Primary Suspect'				
4	23	oe	ch					
5								
3	2025-12-09 13:44:49.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Role=case( match(comp uter, "BSTOLL-L\\.froth\\.ly"), "**Investigation Target** (bstol 1'				
4	40	oe	ch					
6								

		user	acti on	search
_time				
3	2025-12-09 13:43:52.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "**Investigation Target** (bstoll1'
4	39	oe	ch	
7				
3	2025-12-09 13:43:32.2	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Role=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "**Investigation Target** (bstoll1'
4	25	oe	ch	
8				
3	2025-12-09 13:43:22.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Pattern=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "Primary Suspect"
4	43	oe	ch	
9				
3	2025-12-09 13:43:12.5	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   eval Pattern=case( match(computer, "BSTOLL-L\\.froth\\.ly"), "Primary Suspect"
5	77	oe	ch	
0				
3	2025-12-09 13:42:52.2	kimj	sear	'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")'
5	13	oe	ch	
1				
3	2025-12-09 13:42:52.1	kimj	sear	'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'
5	34	oe	ch	
2				

		user	acti on	search
_time				
3	2025-12-09 13:42:47.9	kimj	sear	'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")'
5	09	oe	ch	
3	2025-12-09 13:42:32.8	kimj	sear	'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'
5	44	oe	ch	
4				
3	2025-12-09 12:56:52.4	kimj	sear	'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)'
5	55	oe	ch	
5				
3	2025-12-09 12:56:22.5	kimj	sear	'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)'
5	92	oe	ch	
6				
3	2025-12-09 12:55:52.8	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:* "BSTOLL-L.froth.ly"   stats count by EventCode, EventType   sort -count'
5	57	oe	ch	
7				
3	2025-12-09 12:55:24.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:* "BSTOLL-L.froth.ly"   stats count by EventCode, EventType   sort -count'
5	77	oe	ch	
8				
3	2025-12-09 12:55:22.3	kimj	sear	'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)'
5	59	oe	ch	
9				

		user	acti	
		on	on	
				search
_time				
3	2025-12-09 12:54:52.1	kimj	sear	'search index=botsv3 *bstoll*   stats count'
6	81	oe	ch	
0				
3	2025-12-09 12:54:49.8	kimj	sear	'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)'
6	09	oe	ch	
1				
3	2025-12-09 12:54:22.3	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   stats count by computer   search computer="*BSTOLL*"'
6	19	oe	ch	
2				
3	2025-12-09 12:54:02.3	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   stats count by computer   search computer="*BSTOLL*"'
6	59	oe	ch	
3				
3	2025-12-09 12:53:52.4	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   stats count by user'
6	37	oe	ch	
4				
3	2025-12-09 12:53:31.3	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   stats count by user'
6	56	oe	ch	
5				
3	2025-12-09 12:53:11.4	kimj	sear	'search index=botsv3 *bstoll*   stats count'
6	44	oe	ch	
6				
3	2025-12-09 12:52:22.5	kimj	sear	'search index=botsv3   search *bstoll*   rex field=_raw "ComputerName=(?<computer>[^\\s]+)"   stats count by computer   sort -count'
6	36	oe	ch	
7				

		user	acti on	search
_time				
3	2025-12-09 12:47:55.4	kimj	sear	'search index=botsv3   search *bstoll*   rex field=_raw "Comput
6	64	oe	ch	erName=(?<computer>[^\\s ]+)"   stats count by computer   sort -
8				count'
3	2025-12-09 12:46:52.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:* (user=bstoll OR u
6	59	oe	ch	serName=bstoll OR userIdentity.userName=bstoll)   rex field=_ra
9				w "ComputerName=(?<computer>[^\\s ]+)"   stats count as EventCoun
				t by computer   sort -EventCount'
3	2025-12-09 12:46:38.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:* (user=bstoll OR u
7	82	oe	ch	serName=bstoll OR userIdentity.userName=bstoll)   rex field=_ra
0				w "ComputerName=(?<computer>[^\\s ]+)"   stats count as EventCoun
				t by computer   sort -EventCount'
3	2025-12-09 12:46:22.1	kimj	sear	'search index=botsv3 (user=bstoll OR userName=bstoll) sourcetyp
7	35	oe	ch	e=WinEventLog:*   stats count by ComputerName   sort -count'
1				
3	2025-12-09 12:46:15.2	kimj	sear	'search index=botsv3 (user=bstoll OR userName=bstoll) sourcetyp
7	70	oe	ch	e=WinEventLog:*   stats count by ComputerName   sort -count'
2				
3	2025-12-09 12:45:52.1	kimj	sear	'search index=botsv3 user=bstoll OR userName=bstoll   stats cou
7	51	oe	ch	nt by eventName, host, computer   sort -count'
3				
3	2025-12-09 12:45:40.9	kimj	sear	'search index=botsv3 user=bstoll OR userName=bstoll   stats cou
7	02	oe	ch	nt by eventName, host, computer   sort -count'
4				

		user	acti on	search
_time		⌗	⌗	⌗
3	2025-12-09 12:40:52.4	kimj	sear	'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'
7	16	oe	ch	
5				
3	2025-12-09 12:40:22.1	kimj	sear	'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   search pattern="Different"'
7	84	oe	ch	
6				
3	2025-12-09 12:40:17.8	kimj	sear	'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'
7	69	oe	ch	
7				
3	2025-12-09 12:39:54.2	kimj	sear	'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   search pattern="Different"'
7	79	oe	ch	
8				
3	2025-12-09 12:29:52.3	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   search computer="BSTOLL-L.froth.ly"'
7	35	oe	ch	
9				
3	2025-12-09 12:29:21.2	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   search computer="BSTOLL-L.froth.ly"'
8	95	oe	ch	
0				
3	2025-12-09 12:28:22.1	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   search computer="FYODOR-L.froth.ly"'
8	95	oe	ch	
1				

		user	acti on	search
_time				
3	2025-12-09 12:27:57.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw
8	02	oe	ch	"ComputerName=(?<computer>[\^\\s]+)"   search computer="FY0D0R-L.
2				froth.ly"'
3	2025-12-09 12:27:52.4	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw
8	10	oe	ch	"ComputerName=(?<computer>[\^\\s]+)"   search computer="ABUNGST-
3				L.froth.ly"'
3	2025-12-09 12:27:10.3	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw
8	38	oe	ch	"ComputerName=(?<computer>[\^\\s]+)"   search computer="ABUNGST-
4				L.froth.ly"'
3	2025-12-09 12:25:52.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw
8	29	oe	ch	"ComputerName=(?<computer>[\^\\s]+)"   search computer="BST0LL-L.
5				froth.ly"'
3	2025-12-09 12:25:52.3	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw
8	74	oe	ch	"ComputerName=(?<computer>[\^\\s]+)"   stats count by computer'
6				
3	2025-12-09 12:25:34.6	kimj	sear	'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw
8	17	oe	ch	"ComputerName=(?<computer>[\^\\s]+)"   search computer="BST0LL-L.
7				froth.ly"'
3	2025-12-09 12:25:22.2	kimj	sear	'   search (index=botsv3 sourcetype=aws:cloudtrail "userIdentit
8	57	oe	ch	y.type"="IAMUser")   stats values(userIdentity.userName) as use
8				rnames   eval usernames=mvededup(usernames)   eval usernames=mvsort(usernames)   eval answer=mvjoin(usernames, ",")'

		user	acti	on		
_time	♦	kimj	sear	oe	ch	search
3	2025-12-09 12:25:22.2		'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'			♦
8	02					
9						
3	2025-12-09 12:25:14.1		'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   stats count by computer'			♦
9	44					
0						
3	2025-12-09 12:24:56.9		'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'			♦
9	21					
1						
3	2025-12-09 04:43:11.5		'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   stats count by computer'			♦
9	23					
2						
3	2025-12-09 04:42:54.8		'search index=botsv3 sourcetype=WinEventLog:*   rex field=_raw "ComputerName=(?<computer>[\^\\s]+)"   stats count by computer'			♦
9	77					
3						
3	2025-12-09 04:40:41.4		'search			♦
9	25					
4						

		user	acti		
		♦	on	♦	
	_time				search
3	2025-12-09 04:40:20.8	kimj	sear	'search	
9	12	oe	ch		
5					
3	2025-12-09 04:40:11.4	kimj	sear	'search	
9	07	oe	ch		
6					
3	2025-12-09 04:39:42.4	kimj	sear	'search	
9	20	oe	ch		
7					
3	2025-12-09 04:37:41.4	kimj	sear	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBu	
9	10	oe	ch	cketAcl"   stats values(requestParameters.bucketName) as bucket	
8				Name'	
3	2025-12-09 04:37:14.3	kimj	sear	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBu	
9	67	oe	ch	cketAcl"   stats values(requestParameters.bucketName) as bucket	
9				Name'	
4	2025-12-09 04:36:41.4	kimj	sear	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBu	
0	47	oe	ch	cketAcl"   table requestParameters.bucketName'	
0					