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
1	2025-12-15 09:58:31.977	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
2	2025-12-15 09:57:32.495	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'
3	2025-12-15 09:57:13.443	kimjoe	search	'search index=_audit action="search" user="kimjoe" "botsv3" | table _time user action search | sort - _time'

	_time	user	action	search
4	2025-12-15 09:54:02.724	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$"), "Standard Workstation", true(), "Other") | stats count as TotalEvents, values(User) as AssociatedUser by computer, Role | sort -TotalEvents | eval SuspectDevice=if(match(computer, "BSTOLL-L"), "Suspect", "Normal") | eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 2) | table computer, AssociatedUser, Role, TotalEvents, RelativeActivity, SuspectDevice'
5	2025-12-15 09:53:45.337	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval User=lower(mvindex(split(computer, "-"), 0)) | eval Role=case(match(computer, "BSTOLL-L\.froth\.ly"), "Suspect Workstation", match(computer, "SEPM"), "Security Server", match(computer, "-L\.froth\.ly$"), "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'
6	2025-12-12 21:04:24.329	kimjoe	search	botsv3
7	2025-12-12 21:04:24.293	kimjoe	search	botsv3

	_time	user	action	search
8	2025-12-12 21:04:04.912	kimjoe	search	botsv3
9	2025-12-12 21:03:59.307	kimjoe	search	botsv3
10	2025-12-12 21:00:54.278	kimjoe	search	*index=botsv3*
11	2025-12-12 21:00:31.751	kimjoe	search	*index=botsv3*
12	2025-12-12 21:00:24.327	kimjoe	search	*index=botsv3*
13	2025-12-12 21:00:24.303	kimjoe	search	*index=botsv3*
14	2025-12-12 21:00:24.282	kimjoe	search	*index=botsv3*
15	2025-12-12 21:00:23.362	kimjoe	search	*index=botsv3*
16	2025-12-12 21:00:14.117	kimjoe	search	*index=botsv3*
17	2025-12-12 20:59:56.173	kimjoe	search	*index=botsv3*

	_time	user	action	search
1	2025-12-12 20:59:54.349	kim	sea	'search index=botsv3 | eval case_id="INV-2024-BUD-S3-COMPROMISE" | eval timeline=strftime(_time, "%Y-%m-%d %H:%M:%S") | eval data_source=case(match(sourcetype, "cloudtrail"), "AWS CloudTrail", match(sourcetype, "s3:accesslogs"), "S3 Access Logs", match(sourcetype, "hardware"), "System Inventory", match(sourcetype, "WinEventLog"), "Windows Security Logs", true(), sourcetype) | rex field=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "ComputerName=(?<endpoint>[^\s|]+)" | rex field=_raw "key=(?<s3_key>[^\s|]+)" | rex field=_raw "filename=(?<filename>[^\s|]+)" | eval finding_category=case(eventName="PutBucketAct" AND userIdentity.userName="bstoll", "MAIN COMPROMISE EVENT", sourcetype="aws:s3:accesslogs" AND bucket="frothlywebcode" AND http_method="PUT", "DATA EXFILTRATION", match(processor, "E5-2676"), "INFRASTRUCTURE DETAIL", match(endpoint, "BSTOLL-L\.froth\.ly"), "SUSPECT ENDPOINT ACTIVITY", true(), "BACKGROUND CONTEXT") | eval finding_summary=case(finding_category="MAIN COMPROMISE EVENT", "Bud (bstoll) executed PutBucketAct on " + requestParameters.bucketName + " (Event: " + eventID + ")", finding_category="DATA EXFILTRATION", "File uploaded to S3: " + coalesce(filename, s3_key), finding_category="INFRASTRUCTURE DETAIL", "Web server processor identified: " + replace(processor, "^.*(E5-\d+).*$", "\1"), finding_category="SUSPECT ENDPOINT ACTIVITY", "Primary suspect workstation identified: " + endpoint + " (Belongs to bstoll)", true(), data_source + " log entry") | eval evidence_chain=case(eventID="ab45689d-69cd-41e7-8705-5350402cf7ac", "PUT 1: Initial bucket modification", filename="OPEN_BUCKET_PLEASE_FIX.txt", "PUT 2: Malicious file upload", endpoint="BSTOLL-L.froth.ly", "PUT 3: Source endpoint identification") | eval investigation_notes=case(match(finding_summary, "Bud"), "**CRITICAL** - User bstoll made S3 bucket public", match(finding_summary, "OPEN_BUCKET"), "**CRITICAL
18	49	joe	rch	

_time	user	action	search
			** - Malicious file uploaded", match(finding_summary, "BSTOLL-L"), "**KEY FINDING** - Suspect workstation identified", match(finding_summary, "E5-2676"), "**CONTEXT** - Infrastructure detail", true(), "Supporting evidence") | search finding_category!="BACKGROUND CONTEXT" OR evidence_chain="*" | stats earliest(timeline) as First_Seen, latest(timeline) as Last_Seen, values(finding_summary) as Findings, values(evidence_chain) as Evidence_Chain, values(investigation_notes) as Priority by finding_category | sort finding_category | table finding_category, Findings, Evidence_Chain, First_Seen, Last_Seen, Priority | rename finding_category as "Investigation Category", Findings as "Key Evidence", Evidence_Chain as "Attack Sequence", Priority as "Investigation Priority"'

	_time	user	action	search
1	2025-12-12 20:58:54.288	kim	search	'search index=botsv3 ((sourcetype=aws:cloudtrail eventName="PutBucketAct" userIdentity.userName=bstoll) OR (sourcetype=aws:s3:accesslogs bucket="frothlywebcode") OR (sourcetype=hardware) OR (sourcetype=WinEventLog:*)) | eval Investigation_Phase=case(match(sourcetype, "cloudtrail"), "1. AWS CloudTrail Analysis", match(sourcetype, "s3:accesslogs"), "2. S3 Access Logs", match(sourcetype, "hardware"), "3. Infrastructure Details", match(sourcetype, "WinEventLog"), "4. Endpoint Investigation", true(), "Other") | rex field=_raw "ComputerName=(?<endpoint>[^\s]+)" | rex field=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "key=(?<s3_key>[^\s]+)" | eval bucket_name=if(eventName="PutBucketAct", requestParameters.bucketName, null()) | eval event_id=if(eventName="PutBucketAct", eventID, null()) | eval mfa_field="userIdentity.sessionContext.attributes.mfaAuthenticated" | eval bud_username="bstoll" | eval target_bucket="frothlywebcode" | eval endpoint_user=lower(mvindex(split(endpoint, "-"), 0)) | eval endpoint_relevance=if(endpoint="BSTOLL-L.froth.ly", "PRIMARY SUSPECT WORKSTATION (Bud'
9	88	joe	search	

	_time	user	action	search
2 0	2025-12-12 20:58:06.788	kim joe	search	'search index=botsv3 | eval case_id="INV-2024-BUD-S3-COMPROMISE" | eval timeline=strftime(_time, "%Y-%m-%d %H:%M:%S") | eval data_source=case(match(sourcetype, "cloudtrail"), "AWS CloudTrail", match(sourcetype, "s3:accesslogs"), "S3 Access Logs", match(sourcetype, "hardware"), "System Inventory", match(sourcetype, "WinEventLog"), "Windows Security Logs", true(), sourcetype) | rex field=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "ComputerName=(?<endpoint>[^\s|]+)" | rex field=_raw "key=(?<s3_key>[^\s|]+)" | rex field=_raw "filename=(?<filename>[^\s|]+)" | eval finding_category=case(eventName="PutBucketAct" AND userIdentity.userName="bstoll", "MAIN COMPROMISE EVENT", sourcetype="aws:s3:accesslogs" AND bucket="frothlywebcode" AND http_method="PUT", "DATA EXFILTRATION", match(processor, "E5-2676"), "INFRASTRUCTURE DETAIL", match(endpoint, "BSTOLL-L\.froth\.ly"), "SUSPECT ENDPOINT ACTIVITY", true(), "BACKGROUND CONTEXT") | eval finding_summary=case(finding_category="MAIN COMPROMISE EVENT", "Bud (bstoll) executed PutBucketAct on " + requestParameters.bucketName + " (Event: " + eventID + ")", finding_category="DATA EXFILTRATION", "File uploaded to S3: " + coalesce(filename, s3_key), finding_category="INFRASTRUCTURE DETAIL", "Web server processor identified: " + replace(processor, "^.*(E5-\d+).*$", "\1"), finding_category="SUSPECT ENDPOINT ACTIVITY", "Primary suspect workstation identified: " + endpoint + " (Belongs to bstoll)", true(), data_source + " log entry") | eval evidence_chain=case(eventID="ab45689d-69cd-41e7-8705-5350402cf7ac", "PUT 1: Initial bucket modification", filename="OPEN_BUCKET_PLEASE_FIX.txt", "PUT 2: Malicious file upload", endpoint="BSTOLL-L.froth.ly", "PUT 3: Source endpoint identification") | eval investigation_notes=case(match(finding_summary, "Bud"), "**CRITICAL** - User bstoll made S3 bucket public", match(finding_summary, "OPEN_BUCKET"), "**CRITICAL

_time	user	action	search
			** - Malicious file uploaded", match(finding_summary, "BSTOLL-L"), "**KEY FINDING** - Suspect workstation identified", match(finding_summary, "E5-2676"), "**CONTEXT** - Infrastructure detail", true(), "Supporting evidence") | search finding_category!="BACKGROUND CONTEXT" OR evidence_chain="*" | stats earliest(timeline) as First_Seen, latest(timeline) as Last_Seen, values(finding_summary) as Findings, values(evidence_chain) as Evidence_Chain, values(investigation_notes) as Priority by finding_category | sort finding_category | table finding_category, Findings, Evidence_Chain, First_Seen, Last_Seen, Priority | rename finding_category as "Investigation Category", Findings as "Key Evidence", Evidence_Chain as "Attack Sequence", Priority as "Investigation Priority"'

	_time	user	action	search
2	2025-12-12 20:57:54.3	kim	sea	'search index=botsv3 ((sourcetype=aws:cloudtrail eventName="Put
1	54	joe	rch	BucketAct" userIdentity.userName=bstoll) OR (sourcetype=aws:s3:a ccesslogs bucket="frothlywebcode") OR (sourcetype=hardware) OR (sourcetype=WinEventLog:*)) | eval Investigation_Phase=case(ma tch(sourcetype, "cloudtrail"), "1. AWS CloudTrail Analysis", mat ch(sourcetype, "s3:accesslogs"), "2. S3 Access Logs", match(sour cetype, "hardware"), "3. Infrastructure Details", match(sourcety pe, "WinEventLog"), "4. Endpoint Investigation", true(), "Other") | rex field=_raw "ComputerName=(?<endpoint>[^\s]+)" | rex fiel d=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "key=(?<s3 _key>[^\s]+)" | eval bucket_name=if(eventName="PutBucketAct", re questParameters.bucketName, null()) | eval event_id=if(eventName ="PutBucketAct", eventID, null()) | eval mfa_field="userIdentit y.sessionContext.attributes.mfaAuthenticated" | eval bud_usernam e="bstoll" | eval target_bucket="frothlywebcode" | eval endpoint _user=lower(mvindex(split(endpoint, "-"), 0)) | eval endpoint_re levance=if(endpoint="BSTOLL-L.froth.ly", "PRIMARY SUSPECT WORKST ATION (Bud'

	_time	user	action	search
2	2025-12-12 20:57:47.566	kim	search	'search index=botsv3 ((sourcetype=aws:cloudtrail eventName="PutBucketAct" userIdentity.userName=bstoll) OR (sourcetype=aws:s3:accesslogs bucket="frothlywebcode") OR (sourcetype=hardware) OR (sourcetype=WinEventLog:*)) | eval Investigation_Phase=case(match(sourcetype, "cloudtrail"), "1. AWS CloudTrail Analysis", match(sourcetype, "s3:accesslogs"), "2. S3 Access Logs", match(sourcetype, "hardware"), "3. Infrastructure Details", match(sourcetype, "WinEventLog"), "4. Endpoint Investigation", true(), "Other") | rex field=_raw "ComputerName=(?<endpoint>[^\s]+)" | rex field=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "key=(?<s3_key>[^\s]+)" | eval bucket_name=if(eventName="PutBucketAct", requestParameters.bucketName, null()) | eval event_id=if(eventName="PutBucketAct", eventID, null()) | eval mfa_field="userIdentity.sessionContext.attributes.mfaAuthenticated" | eval bud_username="bstoll" | eval target_bucket="frothlywebcode" | eval endpoint_user=lower(mvindex(split(endpoint, "-"), 0)) | eval endpoint_relevance=if(endpoint="BSTOLL-L.froth.ly", "PRIMARY SUSPECT WORKSTATION (Bud'
2	66	joe	rch	

	_time	user	action	search
2	2025-12-12 20:57:46.7	kim	sea	'search index=botsv3 ((sourcetype=aws:cloudtrail eventName="Put
3	14	joe	rch	BucketAct" userIdentity.userName=bstoll) OR (sourcetype=aws:s3:a ccesslogs bucket="frothlywebcode") OR (sourcetype=hardware) OR (sourcetype=WinEventLog:*)) | eval Investigation_Phase=case(ma tch(sourcetype, "cloudtrail"), "1. AWS CloudTrail Analysis", mat ch(sourcetype, "s3:accesslogs"), "2. S3 Access Logs", match(sour cetype, "hardware"), "3. Infrastructure Details", match(sourcety pe, "WinEventLog"), "4. Endpoint Investigation", true(), "Other") | rex field=_raw "ComputerName=(?<endpoint>[^\s]+)" | rex fiel d=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "key=(?<s3 _key>[^\s]+)" | eval bucket_name=if(eventName="PutBucketAct", re questParameters.bucketName, null()) | eval event_id=if(eventName ="PutBucketAct", eventID, null()) | eval mfa_field="userIdentit y.sessionContext.attributes.mfaAuthenticated" | eval bud_usernam e="bstoll" | eval target_bucket="frothlywebcode" | eval endpoint _user=lower(mvindex(split(endpoint, "-"), 0)) | eval endpoint_re levance=if(endpoint="BSTOLL-L.froth.ly", "PRIMARY SUSPECT WORKST ATION (Bud'

	_time	user	action	search
2	2025-12-12 20:57:24.2	kim	sea	'search index=botsv3 ((sourcetype=aws:cloudtrail eventName="Put
4	83	joe	rch	BucketAct" userIdentity.userName=bstoll) OR (sourcetype=aws:s3:a ccesslogs bucket="frothlywebcode") OR (sourcetype=hardware) OR (sourcetype=WinEventLog:*)) | eval Investigation_Phase=case(ma tch(sourcetype, "cloudtrail"), "1. AWS CloudTrail Analysis", mat ch(sourcetype, "s3:accesslogs"), "2. S3 Access Logs", match(sour cetype, "hardware"), "3. Infrastructure Details", match(sourcety pe, "WinEventLog"), "4. Endpoint Investigation", true(), "Other") | rex field=_raw "ComputerName=(?<endpoint>[^\s]+)" | rex fiel d=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "key=(?<s3 _key>[^\s]+)" | eval bucket_name=if(eventName="PutBucketAct", re questParameters.bucketName, null()) | eval event_id=if(eventName ="PutBucketAct", eventID, null()) | eval mfa_field="userIdentit y.sessionContext.attributes.mfaAuthenticated" | eval bud_usernam e="bstoll" | eval target_bucket="frothlywebcode" | eval endpoint _user=lower(mvindex(split(endpoint, "-"), 0)) | eval endpoint_re levance=if(endpoint="BSTOLL-L.froth.ly", "PRIMARY SUSPECT WORKST ATION (Bud'

	_time	user	action	search
2	2025-12-12 20:57:02.3	kim	sea	'search index=botsv3 ((sourcetype=aws:cloudtrail eventName="Put
5	32	joe	rch	BucketAct" userIdentity.userName=bstoll) OR (sourcetype=aws:s3:a ccesslogs bucket="frothlywebcode") OR (sourcetype=hardware) OR (sourcetype=WinEventLog:*)) | eval Investigation_Phase=case(ma tch(sourcetype, "cloudtrail"), "1. AWS CloudTrail Analysis", mat ch(sourcetype, "s3:accesslogs"), "2. S3 Access Logs", match(sour cetype, "hardware"), "3. Infrastructure Details", match(sourcety pe, "WinEventLog"), "4. Endpoint Investigation", true(), "Other") | rex field=_raw "ComputerName=(?<endpoint>[^\s]+)" | rex fiel d=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "key=(?<s3 _key>[^\s]+)" | eval bucket_name=if(eventName="PutBucketAct", re questParameters.bucketName, null()) | eval event_id=if(eventName ="PutBucketAct", eventID, null()) | eval mfa_field="userIdentit y.sessionContext.attributes.mfaAuthenticated" | eval bud_usernam e="bstoll" | eval target_bucket="frothlywebcode" | eval endpoint _user=lower(mvindex(split(endpoint, "-"), 0)) | eval endpoint_re levance=if(endpoint="BSTOLL-L.froth.ly", "PRIMARY SUSPECT WORKST ATION (Bud'

	_time	user	action	search
2	2025-12-12 20:56:54.2	kim	sea	'search index=botsv3 | eval case_id="INV-2024-BUD-S3-COMPROMISE"
6	78	joe	rch	| eval timeline=strftime(_time, "%Y-%m-%d %H:%M:%S") | eval data _source=case(match(sourcetype, "cloudtrail"), "AWS CloudTrail", match(sourcetype, "s3:accesslogs"), "S3 Access Logs", match(sour cetype, "hardware"), "System Inventory", match(sourcetype, "WinE ventLog"), "Windows Security Logs", true(), sourcetype) | rex f ield=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "Comput erName=(?<endpoint>[^\s|]+)" | rex field=_raw "key=(?<s3_key>[^ \s|]+)" | rex field=_raw "filename=(?<filename>[^\s|]+)" | eval finding_category=case(eventName="PutBucketAct" AND userIdentit y.userName="bstoll", "MAIN COMPROMISE EVENT", sourcetype="aws:s 3:accesslogs" AND bucket="frothlywebcode" AND http_method="PUT", "DATA EXFILTRATION", match(processor, "E5-2676"), "INFRASTRUCTUR E DETAIL", match(endpoint, "BSTOLL-L\.froth\.ly"), "SUSPECT ENDP OINT ACTIVITY", true(), "BACKGROUND CONTEXT") | eval finding_su mmary=case(finding_category="MAIN COMPROMISE EVENT", "Bud (bsto ll) executed PutBucketAct on " + requestParameters.bucketName + " (Event: " + eventID + ")", finding_category="DATA EXFILTRATIO N", "File uploaded to S3: " + coalesce(filename, s3_key), findin g_category="INFRASTRUCTURE DETAIL", "Web server processor identi fied: " + replace(processor, "^.*(E5-\d+).*$", "\1"), finding_ca tegory="SUSPECT ENDPOINT ACTIVITY", "Primary suspect workstation identified: " + endpoint + " (Belongs to bstoll)", true(), data_ source + " log entry") | eval evidence_chain=case(eventID="ab4 5689d-69cd-41e7-8705-5350402cf7ac", "PUT 1: Initial bucket modif ication", filename="OPEN_BUCKET_PLEASE_FIX.txt", "PUT 2: Malicio us file upload", endpoint="BSTOLL-L.froth.ly", "PUT 3: Source en dpoint identification") | eval investigation_notes=case(match (finding_summary, "Bud"), "**CRITICAL** - User bstoll made S3 bu cket public", match(finding_summary, "OPEN_BUCKET"), "**CRITICAL

_time	user	action	search
			** - Malicious file uploaded", match(finding_summary, "BSTOLL-L"), "**KEY FINDING** - Suspect workstation identified", match(finding_summary, "E5-2676"), "**CONTEXT** - Infrastructure detail", true(), "Supporting evidence") | search finding_category!="BACKGROUND CONTEXT" OR evidence_chain="*" | stats earliest(timeline) as First_Seen, latest(timeline) as Last_Seen, values(finding_summary) as Findings, values(evidence_chain) as Evidence_Chain, values(investigation_notes) as Priority by finding_category | sort finding_category | table finding_category, Findings, Evidence_Chain, First_Seen, Last_Seen, Priority | rename finding_category as "Investigation Category", Findings as "Key Evidence", Evidence_Chain as "Attack Sequence", Priority as "Investigation Priority"'

	_time	user	action	search
2	2025-12-12 20:56:34.165	kim	sea	'search index=botsv3 | eval case_id="INV-2024-BUD-S3-COMPROMISE" | eval timeline=strftime(_time, "%Y-%m-%d %H:%M:%S") | eval data_source=case(match(sourcetype, "cloudtrail"), "AWS CloudTrail", match(sourcetype, "s3:accesslogs"), "S3 Access Logs", match(sourcetype, "hardware"), "System Inventory", match(sourcetype, "WinEventLog"), "Windows Security Logs", true(), sourcetype) | rex field=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "ComputerName=(?<endpoint>[^\s|]+)" | rex field=_raw "key=(?<s3_key>[^\s|]+)" | rex field=_raw "filename=(?<filename>[^\s|]+)" | eval finding_category=case(eventName="PutBucketAct" AND userIdentity.userName="bstoll", "MAIN COMPROMISE EVENT", sourcetype="aws:s3:accesslogs" AND bucket="frothlywebcode" AND http_method="PUT", "DATA EXFILTRATION", match(processor, "E5-2676"), "INFRASTRUCTURE DETAIL", match(endpoint, "BSTOLL-L\.froth\.ly"), "SUSPECT ENDPOINT ACTIVITY", true(), "BACKGROUND CONTEXT") | eval finding_summary=case(finding_category="MAIN COMPROMISE EVENT", "Bud (bstoll) executed PutBucketAct on " + requestParameters.bucketName + " (Event: " + eventID + ")", finding_category="DATA EXFILTRATION", "File uploaded to S3: " + coalesce(filename, s3_key), finding_category="INFRASTRUCTURE DETAIL", "Web server processor identified: " + replace(processor, "^.*(E5-\d+).*$", "\1"), finding_category="SUSPECT ENDPOINT ACTIVITY", "Primary suspect workstation identified: " + endpoint + " (Belongs to bstoll)", true(), data_source + " log entry") | eval evidence_chain=case(eventID="ab45689d-69cd-41e7-8705-5350402cf7ac", "PUT 1: Initial bucket modification", filename="OPEN_BUCKET_PLEASE_FIX.txt", "PUT 2: Malicious file upload", endpoint="BSTOLL-L.froth.ly", "PUT 3: Source endpoint identification") | eval investigation_notes=case(match(finding_summary, "Bud"), "**CRITICAL** - User bstoll made S3 bucket public", match(finding_summary, "OPEN_BUCKET"), "**CRITICAL
27	65	joe	rch	| eval timeline=strftime(_time, "%Y-%m-%d %H:%M:%S") | eval data_source=case(match(sourcetype, "cloudtrail"), "AWS CloudTrail", match(sourcetype, "s3:accesslogs"), "S3 Access Logs", match(sourcetype, "hardware"), "System Inventory", match(sourcetype, "WinEventLog"), "Windows Security Logs", true(), sourcetype) | rex field=_raw "CPU_TYPE\s+(?<processor>.+)" | rex field=_raw "ComputerName=(?<endpoint>[^\s|]+)" | rex field=_raw "key=(?<s3_key>[^\s|]+)" | rex field=_raw "filename=(?<filename>[^\s|]+)" | eval finding_category=case(eventName="PutBucketAct" AND userIdentity.userName="bstoll", "MAIN COMPROMISE EVENT", sourcetype="aws:s3:accesslogs" AND bucket="frothlywebcode" AND http_method="PUT", "DATA EXFILTRATION", match(processor, "E5-2676"), "INFRASTRUCTURE DETAIL", match(endpoint, "BSTOLL-L\.froth\.ly"), "SUSPECT ENDPOINT ACTIVITY", true(), "BACKGROUND CONTEXT") | eval finding_summary=case(finding_category="MAIN COMPROMISE EVENT", "Bud (bstoll) executed PutBucketAct on " + requestParameters.bucketName + " (Event: " + eventID + ")", finding_category="DATA EXFILTRATION", "File uploaded to S3: " + coalesce(filename, s3_key), finding_category="INFRASTRUCTURE DETAIL", "Web server processor identified: " + replace(processor, "^.*(E5-\d+).*$", "\1"), finding_category="SUSPECT ENDPOINT ACTIVITY", "Primary suspect workstation identified: " + endpoint + " (Belongs to bstoll)", true(), data_source + " log entry") | eval evidence_chain=case(eventID="ab45689d-69cd-41e7-8705-5350402cf7ac", "PUT 1: Initial bucket modification", filename="OPEN_BUCKET_PLEASE_FIX.txt", "PUT 2: Malicious file upload", endpoint="BSTOLL-L.froth.ly", "PUT 3: Source endpoint identification") | eval investigation_notes=case(match(finding_summary, "Bud"), "**CRITICAL** - User bstoll made S3 bucket public", match(finding_summary, "OPEN_BUCKET"), "**CRITICAL

	_time	user	action	search
				** - Malicious file uploaded", match(finding_summary, "BSTOLL-L"), "**KEY FINDING** - Suspect workstation identified", match(finding_summary, "E5-2676"), "**CONTEXT** - Infrastructure detail", true(), "Supporting evidence") | search finding_category!="BACKGROUND CONTEXT" OR evidence_chain="*" | stats earliest(timeline) as First_Seen, latest(timeline) as Last_Seen, values(finding_summary) as Findings, values(evidence_chain) as Evidence_Chain, values(investigation_notes) as Priority by finding_category | sort finding_category | table finding_category, Findings, Evidence_Chain, First_Seen, Last_Seen, Priority | rename finding_category as "Investigation Category", Findings as "Key Evidence", Evidence_Chain as "Attack Sequence", Priority as "Investigation Priority"'
2	2025-12-12 20:35:54.272	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
2	2025-12-12 20:35:41.449	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
3	2025-12-12 03:18:20.755	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'

	_time	user	action	search
31	2025-12-12 03:18:06.429	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" userIdentity.userName="bstoll" | table eventID, requestParameters.bucketName, requestParameters.acl, requestParameters.grantList'
32	2025-12-12 03:17:50.764	kim joe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
33	2025-12-12 03:17:48.874	kim joe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
34	2025-12-12 00:08:21.015	kim joe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
35	2025-12-12 00:08:12.238	kim joe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
36	2025-12-12 00:07:20.818	kim joe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
37	2025-12-12 00:07:20.793	kim joe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
38	2025-12-12 00:07:06.754	kim joe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
39	2025-12-12 00:06:51.596	kim joe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
40	2025-12-12 00:06:50.767	kim joe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'

	_time	user	action	search
41	2025-12-12 00:06:34.046	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
42	2025-12-12 00:02:50.849	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$"), "Standard Workstation", true(), "Other") | stats count as TotalEvents, values(User) as AssociatedUser by computer, Role | sort -TotalEvents | eval SuspectDevice=if(match(computer, "BSTOLL-L"), "Suspect", "Normal") | eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 2) | table computer, AssociatedUser, Role, TotalEvents, RelativeActivity, SuspectDevice'
43	2025-12-12 00:02:22.760	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | eval User=lower(mvindex(split(computer, "-"), 0)) | eval Role=case(match(computer, "BSTOLL-L\.froth\.ly"), "Suspect Workstation", match(computer, "SEPM"), "Security Server", match(computer, "-L\.froth\.ly$"), "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'
44	2025-12-12 00:02:20.861	kimjoe	search	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer'

	_time	user	action	search
4 5	2025-12-12 00:02:13.795	kim joe	sea rch	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer'
4 6	2025-12-12 00:00:20.851	kim joe	sea rch	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer'
4 7	2025-12-12 00:00:02.580	kim joe	sea rch	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw "ComputerName=(?<computer>[^\s]+)" | stats count by computer'
4 8	2025-12-11 23:59:20.863	kim joe	sea rch	'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
4	2025-12-11 23:59:02.169	kim	sea	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw
9		joe	rch	"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$"), "Standard Workstation", true(), "Other") | stats count as TotalEvents, values(User) as AssociatedUser by computer, Role | sort -TotalEvents | eval SuspectDevice=if(match(computer, "BSTOLL-L"), "Suspect", "Normal") | eval RelativeActivity=round(TotalEvents*100/sum(TotalEvents), 2) | table computer, AssociatedUser, Role, TotalEvents, RelativeActivity, SuspectDevice'
5	2025-12-11 23:58:50.837	kim	sea	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw
0		joe	rch	"ComputerName=(?<computer>[^\s]+)" | eval Role=case(match(computer, "BSTOLL-L"), "Suspect Workstation", match(computer, "-L\.froth\.ly$"), "Standard Workstation", match(computer, "SEPM"), "Security Server", true(), "Other") | stats count by computer, Role'
5	2025-12-11 23:58:21.155	kim	sea	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw
1		joe	rch	"ComputerName=(?<computer>[^\s]+)" | eval Role=case(match(computer, "BSTOLL-L"), "Suspect Workstation", match(computer, "-L\.froth\.ly$"), "Standard Workstation", match(computer, "SEPM"), "Security Server", true(), "Other") | stats count by computer, Role'
5	2025-12-11 23:58:20.829	kim	sea	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw
2		joe	rch	"ComputerName=(?<computer>[^\s]+)" | stats count by computer'
5	2025-12-11 23:57:53.973	kim	sea	'search index=botsv3 sourcetype=WinEventLog:* | rex field=_raw
3		joe	rch	"ComputerName=(?<computer>[^\s]+)" | stats count by computer'

	_time	user	action	search
5 4	2025-12-11 23:29:20.788	kim joe	search	'search
5 5	2025-12-11 23:29:11.435	kim joe	search	'search
5 6	2025-12-11 23:27:50.835	kim joe	search	'search
5 7	2025-12-11 23:27:50.803	kim joe	search	'search
5 8	2025-12-11 23:27:42.175	kim joe	search	'search
5 9	2025-12-11 23:27:22.009	kim joe	search	'search
6 0	2025-12-11 23:25:50.823	kim joe	search	'search
6 1	2025-12-11 23:25:45.248	kim joe	search	'search
6 2	2025-12-11 23:24:50.804	kim joe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | rex field=_raw "^(?<bucket_owner>[^\s]+)\s+..." | search bucket="frothlywebcode" http_status="200" operation="REST.PUT.OBJECT" | table _time, bucket, operation, key, http_status'
6 3	2025-12-11 23:24:35.762	kim joe	search	'search index=botsv3 sourcetype=aws:s3:accesslogs | rex field=_raw "^(?<bucket_owner>[^\s]+)\s+..." | search bucket="frothlywebcode" http_status="200" operation="REST.PUT.OBJECT" | table _time, bucket, operation, key, http_status'

	_time	user	action	search
64	2025-12-11 23:20:20.882	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(requestParameters.bucketName) as bucketName'
65	2025-12-11 23:20:02.240	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(requestParameters.bucketName) as bucketName'
66	2025-12-11 23:13:50.978	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | stats count by eventName'
67	2025-12-11 23:13:35.478	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | stats count by eventName'
68	2025-12-11 23:12:20.898	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'
69	2025-12-11 23:11:59.899	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'
70	2025-12-11 23:11:50.979	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | stats count by eventName'
71	2025-12-11 23:11:40.990	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.userName="bstoll" | stats count by eventName'
72	2025-12-11 23:10:50.900	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'
73	2025-12-11 23:10:37.326	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | stats values(userIdentity.userName) as user'

	_time	user	action	search
74	2025-12-11 23:08:51.002	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
75	2025-12-11 23:08:50.919	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
76	2025-12-11 23:08:46.623	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
77	2025-12-11 23:08:23.838	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
78	2025-12-11 23:08:21.405	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
79	2025-12-11 23:08:10.909	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID="ab45689d-69cd-41e7-8705-5350402cf7ac" | spath | table *'
80	2025-12-11 23:07:50.888	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID=" ab45689d-69cd-41e7-8705-5350402cf7ac " | spath | table *'
81	2025-12-11 23:07:38.960	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventID=" ab45689d-69cd-41e7-8705-5350402cf7ac " | spath | table *'
82	2025-12-11 23:04:20.908	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'
83	2025-12-11 23:04:01.572	kim joe	search	'search index=botsv3 sourcetype=aws:cloudtrail eventName="PutBucketAcl" | table _time, eventID, userIdentity.userName, requestParameters.bucketName'

	_time	user	action	search
84	2025-12-11 23:01:50.897	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
85	2025-12-11 23:01:20.927	kimjoe	search	'search index=botsv3 sourcetype=hardware | rex field=_raw "CPU_TYPE\s+(?<processor>[^\n]+)" | table host, processor'
86	2025-12-11 22:58:50.896	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
87	2025-12-11 22:58:20.370	kimjoe	search	'search index=botsv3 sourcetype=hardware | head 10 | table host, processor, os, category, type'
88	2025-12-11 22:57:21.182	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count, values'
89	2025-12-11 22:56:53.826	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count, values'
90	2025-12-11 18:00:48.402	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count, values'
91	2025-12-11 18:00:42.716	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | fieldsummary | search field="*mfa*" OR field="*MFA*" | table field, count, values'
92	2025-12-11 17:59:18.381	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('
93	2025-12-11 17:59:10.728	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | foreach * [eval <<FIELD>>_exists = if(isnotnull('

	_time	user	action	search
94	2025-12-11 17:57:48.399	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) | table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated'
95	2025-12-11 17:57:40.925	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" | where isnull(userIdentity.sessionContext.attributes.mfaAuthenticated) | table _time, eventName, userIdentity.sessionContext.attributes.mfaAuthenticated'
96	2025-12-11 17:51:48.367	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
97	2025-12-11 17:51:31.361	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail | search *MFA* | fieldsummary | search field="*MFA*"'
98	2025-12-11 17:49:18.344	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'
99	2025-12-11 17:48:50.375	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'

	_time	user	action	search
1	2025-12-11 17:47:18.334	kim	search	'search index=botsv3 sourcetype=aws:cloudtrail userIdentity.type="IAMUser" | stats values(userIdentity.userName) as usernames'
0		joe		
0				