

Threat Hunting Lab Scenario 4: Excessive Resource Creation / Deletion

09/30/2025

Explanation

This query will be used to monitor and identify potential security or operational risks in an Azure environment by flagging high-volume resource creation or deletion activities. A high number of such operations can indicate unusual behavior, such as unauthorized access, automation misconfigurations, or even malicious activity. By pinpointing Callers performing 5 or more successful resource writes or deletions, this query helps administrators quickly focus on entities that may require further investigation or corrective action, enhancing overall security posture and operational governance.

Whenever a user or service performs resource creation or deletion activities in Azure, the corresponding logs are captured in the "AzureActivity" table, which is forwarded to the Log Analytics Workspace utilized by Microsoft Sentinel, our SIEM. Within Sentinel, we will define an alert to trigger when a Caller performs 10 or more successful resource creation ("WRITE") or deletion ("DELETE") operations. While not all alerts may represent true positives, this provides an opportunity to investigate potential unauthorized access, automation misconfigurations, or unusual activity patterns, ensuring better governance and security oversight of our Azure environment.

*Threshold 5 is configurable. In a lab, it's fine. In production, we may want 10 or more.

Part 1: Create Alert Rule (Excessive Resource Creation or Deletion)

I will create a query that identifies users or entities (Callers) who have performed 5 or more successful resource creation ("WRITE") or deletion ("DELETE") operations in Azure, highlighting potential unusual or risky activity. Exclude any writing or deleting of incidents and alert rules.

Created a Virtual Machine at: <https://portal.azure.com/>

Virtual machine		Networking	
Computer name	Win11BruceSept3	Public IP address	-
Operating system	Windows (Windows 11 Pro)	Public IP address (IPv6)	-
VM generation	V2	Private IP address	10.1.1.7
VM architecture	x64	Private IP address (IPv6)	-
Agent status	Ready	Virtual network/subnet	Cyber-Range-2-VNet/Cyber-Range-2-Subnet

The firewall has been disabled for this Virtual Machine, through Bastion.

Alert Rule Creation through Microsoft Azure Sentinel: <https://portal.azure.com/>

```
let lookback = 7d;
let threshold = 5;
AzureActivity
| where TimeGenerated >= ago(lookback)
| where ActivityStatusValue == "Success"
| where OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/ALERTRULES"
  and OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/INCIDENTS"
| extend ClaimsJson = parse_json(Claims)
| extend ObjectIdentifier =
  tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
| extend OpNameLower = tolower(OperationNameValue)
| summarize
  NumberOfResourceCreations = countif(OpNameLower endswith_cs "write"),
  NumberOfResourceDeletions = countif(OpNameLower endswith_cs "delete")
  by Caller, ObjectIdentifier, CallerIpAddress
| where NumberOfResourceCreations >= threshold or NumberOfResourceDeletions >=
threshold
| order by NumberOfResourceCreations desc, NumberOfResourceDeletions desc, Caller asc
```

This query passes:

[Home](#) > [Microsoft Sentinel](#) | [Analytics](#) >

Analytics rule wizard - Create a new Scheduled rule ...



Alert Rule Successfully Created.

Creation time

09/30/25, 12:36 PM

Part 2: Alert Has Been Triggered

09/30/25, 12:36:37 PM

This alert did not require my assistance to be triggered.

Microsoft Sentinel | Incidents

Selected workspace: 'law-cyber-range'

+ Create incident (Preview) Refresh Last 24 hours Actions Delete Security efficiency workbook Columns Guides & Feedback

446 Open incidents 445 New incidents 1 Active incidents

Open incidents by severity: High (46) Medium (348) Low (0) Informational (52)

Search by ID, title, tags, owner or product Severity: All Status: 2 selected Incident Provider name: All More (2)

Auto-refresh incidents

Severity	Incident number	Title	Alerts	Incident provider na...	Alert product name	Created time
Medium	187885	Bruce Thornton Exce...	1	Azure Sentinel	Microsoft Sentinel	09/30/25, 12:36 PM
Medium	187623	Kyle - Sign-ins from ...	4	Azure Sentinel	Microsoft Sentinel	09/29/25, 09:36 PM
Medium	187884	sfondi - Alert Rule (B...	1	Azure Sentinel	Microsoft Sentinel	09/30/25, 12:33 PM
High	187830	SL_Encoded PowerSh...	5	Azure Sentinel	Microsoft Sentinel	09/30/25, 08:29 AM
Medium	187883	E2B - Create Alert Ru...	1	Azure Sentinel	Microsoft Sentinel	09/30/25, 12:27 PM
Medium	187882	A_Gaucha Alert Rule...	1	Azure Sentinel	Microsoft Sentinel	09/30/25, 12:27 PM
Medium	187881	Majoka-Brute Fore A...	1	Azure Sentinel	Microsoft Sentinel	09/30/25, 12:25 PM
Medium	187880	Yusuf- Create rule al...	1	Azure Sentinel	Microsoft Sentinel	09/30/25, 12:11 PM

View full details Actions

Bruce Thornton Excessive Resource Creation or Deletion

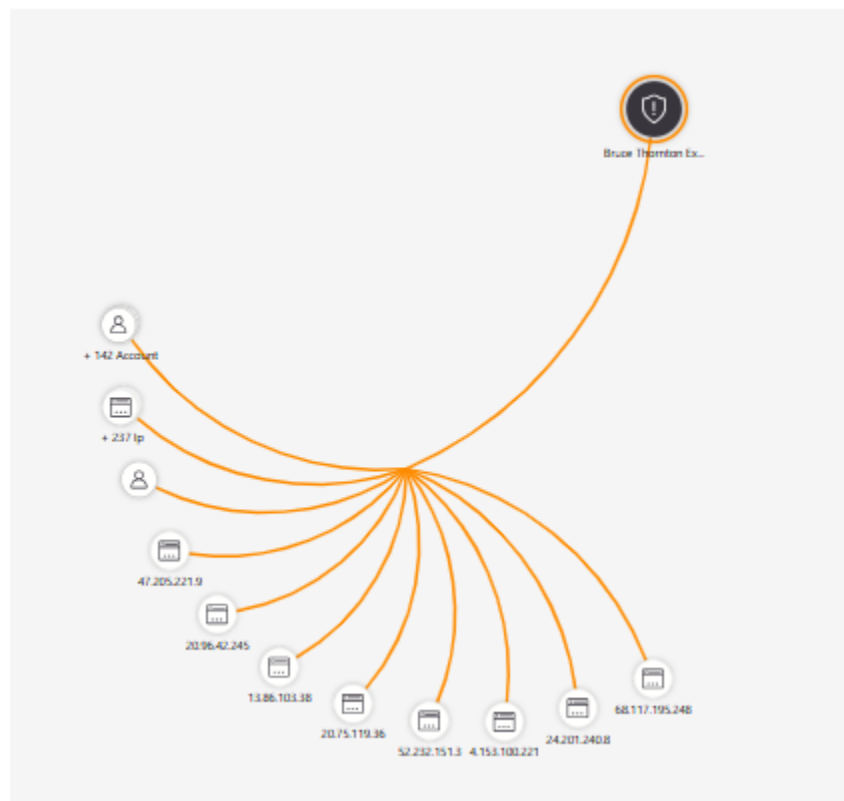
Incident number 187885

Unassigned Owner New Status Medium Severity

Description: Identifies users or entities (Callers) who have performed 5 or more successful resource creation ("WRITE") or deletion ("DELETE") operations in Azure, highlighting potential unusual or risky activity. This query is used to monitor and identify potential security or operational risks in an Azure environment by flagging ...

Alert product names: Microsoft Sentinel

Evidence: 245 Events 1 Alerts 0 Bookmarks



I will assign this Incident to myself, assigning its status as “Active.”

Part 3: Working the Incident

*Incident response guidance is from NIST SP 800-61r2.

I will gather relevant evidence and assess impact, investigate individual accounts using a KQL query within Log Analytics to see exactly what they have been creating or deleting, and take note if something looks different from unusual behavior.

Initial KQL query used:

Successful WRITE/DELETE events in the last 7 days. A very broad range.

```
AzureActivity
| where TimeGenerated >= ago(7d)
| where ActivityStatusValue == "Success"
| where OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/ALERTRULES"
  and OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/INCIDENTS"
| extend ClaimsJson = parse_json(Claims)
| extend ObjectIdentifier =
tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
| extend OpNameLower = tolower(OperationNameValue)
| where OpNameLower endswith_cs "write" or OpNameLower endswith_cs "delete"
| project TimeGenerated, Caller, ObjectIdentifier, CallerIpAddress, SubscriptionId,
ResourceGroup, ResourceId, OperationNameValue
| order by TimeGenerated desc
```

Microsoft Sentinel | Logs

Selected workspace: 'law-cyber-range'

New Query 1*

Run Time range: Set in query Show: 1000 results KQL mode

```

182 | project TimeGenerated, Caller, ObjectIdentifier, CallerIpAddress, SubscriptionId, ResourceGroup, OperationNameValue
183 | order by TimeGenerated desc
184 AzureActivity
185 | where TimeGenerated >= ago(7d)
186 | where ActivityStatusValue == "Success"
187 | where OperationNameValue istartswith "MICROSOFT.SECURITYINSIGHTS/ALERTRULES"
188 | and OperationNameValue istartswith "MICROSOFT.SECURITYINSIGHTS/INCIDENTS"
189 | extend ClaimsJson = parse_json(Claims)
190 | extend ObjectIdentifier = tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
191 | extend OpNameLower = tolower(OperationNameValue)
192 | where OpNameLower ends with cs "write" or OpNameLower ends with cs "delete"

```

Results Chart Add bookmark

TimeGenerated [UTC]	Caller	ObjectIdentifier	CallerIpAddress	SubscriptionId	ResourceGroup	OperationNameValue
> 9/30/2025, 6:04:06.734 PM	d0861d71f5ba3788ef51557346...	1ede8735-d033-4104-a4e7-3f9...	2601:c2:f01:930:5db9:2813:5dc...	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-D0861D71F5BA3...	MICROSOFT.COMPUTE/VIRTUA...
> 9/30/2025, 6:04:06.125 PM	d0861d71f5ba3788ef51557346...	1ede8735-d033-4104-a4e7-3f9...	2601:c2:f01:930:5db9:2813:5dc...	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-D0861D71F5BA3...	MICROSOFT.RESOURCES/DEPL...
> 9/30/2025, 6:04:01.971 PM	0d8cc27d007c0b6c12a903a55f...	04f4dea8-a2ae-4b77-a316-8ea...	2600:1702:5bc5:0:2157:b496a9...	3c95e63a-895a-4386-991e-edb...	STUDENT-RG-0D8CC27D007C...	MICROSOFT.NETWORK/PUBLIC...
> 9/30/2025, 6:04:01.715 PM	0d8cc27d007c0b6c12a903a55f...	04f4dea8-a2ae-4b77-a316-8ea...	2600:1702:5bc5:0:2157:b496a9...	3c95e63a-895a-4386-991e-edb...	STUDENT-RG-0D8CC27D007C...	MICROSOFT.NETWORK/NETWO...
> 9/30/2025, 6:04:00.840 PM	0d8cc27d007c0b6c12a903a55f...	04f4dea8-a2ae-4b77-a316-8ea...	2600:1702:5bc5:0:2157:b496a9...	3c95e63a-895a-4386-991e-edb...	STUDENT-RG-0D8CC27D007C...	MICROSOFT.NETWORK/NETWO...
> 9/30/2025, 6:03:59.227 PM	0d8cc27d007c0b6c12a903a55f...	04f4dea8-a2ae-4b77-a316-8ea...	2600:1702:5bc5:0:2157:b496a9...	3c95e63a-895a-4386-991e-edb...	STUDENT-RG-0D8CC27D007C...	MICROSOFT.RESOURCES/DEPL...

1s 71ms Display time (UTC+00:00) Query details 1 - 7 of 1000

This shows 1-7 rows/entries out of 1000.

Now I will narrow down the amount of results.

Go to Microsoft Sentinel in the Azure Portal.

Threat management → Incidents.

Click into the **Incident** you're investigating.

In the incident panel, look for **Entities** or **Alerts**.

- Click on one of the **Entities** (account, IP, etc.).
- Sentinel offers you options like *Investigate* or *View in Logs*.

When you click **View in Logs**, Sentinel automatically opens the **Logs blade** with the **SecurityAlert** table pre-queried.

Query:

SecurityAlert

```

| summarize arg_max(TimeGenerated, *) by SystemAlertId
| where SystemAlertId in ("03310710-5511-cdf5-c88f-5f0f45b38b9a")
| project SystemAlertId, Entities
| extend Entities = iff(isempty(Entities), todynamic(['{"dummy": ""}']), todynamic(Entities))
| mvexpand Entities
| evaluate bag_unpack(Entities)
| extend Type = columnifexists("Type", "")

```

SystemAlertId	Sid	IsDomainJoined	Type
03310710-5511-cdf5-c88f-5f0f45b38b9a	130	false	account

Now I will plug in this value from the ObjectIdentifier table:

04cd29c3-f1d4-4305-963b-32598abbd847

Query:

```
let AlertedId = "04cd29c3-f1d4-4305-963b-32598abbd847";
```

```
AzureActivity
```

```
| where TimeGenerated >= ago(7d)
```

```
| extend ClaimsJson = parse_json(Claims)
```

```
| extend ActorObjectId =  
tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
```

```
| where ActorObjectId == AlertedId
```

```
| where ActivityStatusValue == "Success"
```

| where OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/ALERTRULES"

and OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/INCIDENTS"

| extend OpNameLower = tolower(OperationNameValue)

| where OpNameLower endswith _cs "write" or OpNameLower endswith _cs "delete"

| project TimeGenerated, Caller, ActorObjectId, CallerIpAddress, SubscriptionId,
ResourceGroup, ResourceId, OperationNameValue

| order by TimeGenerated desc

Microsoft Sentinel | Logs

Selected workspace: 'law-cyber-range'

New Query 1* ... +

Save Share ... Queries hub

Time range: Set in query Show: 1000 results KQL mode

```
150 | extend Type = columnifexists("Type", "")
151
152 let AlertedId = "04cd29c3-f1d4-4305-963b-32598abbd847";
153 AzureActivity
154 | where TimeGenerated >= ago(7d)
155 | extend ClaimsJson = parse_json(Claims)
156 | extend ActorObjectId = tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
157 | where ActorObjectId == AlertedId
158 | where ActivityStatusValue == "Success"
159 | where OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/ALERTRULES"
160 | and OperationNameValue !startswith "MICROSOFT.SECURITYINSIGHTS/INCIDENTS"
```

Results Chart Add bookmark

<input type="checkbox"/>	TimeGenerated [UTC]	Caller	ActorObjectId	CallerIpAddress	SubscriptionId	ResourceGroup	OperationNameValue
<input type="checkbox"/>	> 9/29/2025, 6:52:00.727 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-41DF752ADCCD...	MICROSOFT.NETWORK/PUBLIC...
<input type="checkbox"/>	> 9/29/2025, 6:51:55.956 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-41DF752ADCCD...	MICROSOFT.NETWORK/NETWO...
<input type="checkbox"/>	> 9/29/2025, 6:44:30.057 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-41DF752ADCCD...	MICROSOFT.COMPUTE/VIRTUA...
<input type="checkbox"/>	> 9/29/2025, 6:44:29.437 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-41DF752ADCCD...	MICROSOFT.RESOURCES/DEPL...
<input type="checkbox"/>	> 9/29/2025, 6:42:01.128 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-41DF752ADCCD...	MICROSOFT.NETWORK/PUBLIC...
<input type="checkbox"/>	> 9/29/2025, 6:42:00.696 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-41DF752ADCCD...	MICROSOFT.NETWORK/NETWO...
<input type="checkbox"/>	> 9/29/2025, 6:42:00.113 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35	cd015a7d-a927-49c6-896a-67d...	STUDENT-RG-41DF752ADCCD...	MICROSOFT.NETWORK/NETWO...

1s 129ms | Display time (UTC+00:00) Query details | 1 - 7 of 16

This returns 16 entries that span 3 different CallerIpAddresses coming from this specific Caller:

<input type="checkbox"/>	TimeGenerated [UTC]	Caller	ActorObjectId	CallerIpAddress
<input type="checkbox"/>	> 9/29/2025, 6:42:00.113 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35
<input type="checkbox"/>	> 9/29/2025, 6:41:55.211 PM	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	185.255.198.35
<input type="checkbox"/>	> 9/25/2025, 12:57:01.996 ...	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	111.249.69.112
<input type="checkbox"/>	> 9/24/2025, 12:09:07.799 P...	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	14.198.39.113
<input type="checkbox"/>	> 9/24/2025, 12:08:59.374 P...	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	14.198.39.113
<input type="checkbox"/>	> 9/24/2025, 12:08:55.343 P...	41df752adccd0f0b74e799730b...	04cd29c3-f1d4-4305-963b-325...	14.198.39.113

And narrowing it down to allow us to see the activity for this lab even more clearly, I have ran this query which will summarize counts for easier documentation:

```
let AlertedId = "04cd29c3-f1d4-4305-963b-32598abbd847";
```

```
AzureActivity
```

```
| where TimeGenerated >= ago(7d)
```

```
| extend ClaimsJson = parse_json(Claims)
```

```
| extend ActorObjectId =  
tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
```

```
| where ActorObjectId == AlertedId
```

```
| where ActivityStatusValue == "Success"
```

```
| extend OpNameLower = tolower(OperationNameValue)
```

```
| summarize
```

```
Writes = countif(OpNameLower endswith_cs "write"),
```

```
Deletes = countif(OpNameLower endswith_cs "delete")
```

```
by ActorObjectId, Caller, CallerIpAddress
```

The screenshot shows the Microsoft Sentinel Logs interface. At the top, it says "Microsoft Sentinel | Logs" and "Selected workspace: 'law-cyber-range'". Below this, there's a "New Query 1*" tab. The query editor shows the following KQL query:

```
166 let AlertedId = "04cd29c3-f1d4-4305-963b-32598abbd847";  
167 AzureActivity  
168 | where TimeGenerated >= ago(7d)  
169 | extend ClaimsJson = parse_json(Claims)  
170 | extend ActorObjectId = tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])  
171 | where ActorObjectId == AlertedId  
172 | where ActivityStatusValue == "Success"  
173 | extend OpNameLower = tolower(OperationNameValue)  
174 | summarize  
175     Writes = countif(OpNameLower endswith_cs "write"),  
176     Deletes = countif(OpNameLower endswith_cs "delete")
```

The results are displayed in a table with the following columns: ActorObjectId, Caller, CallerIpAddress, Writes, and Deletes. There are three rows of data:

ActorObjectId	Caller	CallerIpAddress	Writes	Deletes
> 04cd29c3-f1d4-4305-963b-32598abbd847	41df752adccd0f0b74e799730b...	14.198.39.113	6	1
> 04cd29c3-f1d4-4305-963b-32598abbd847	41df752adccd0f0b74e799730b...	111.249.69.112	0	1
> 04cd29c3-f1d4-4305-963b-32598abbd847	41df752adccd0f0b74e799730b...	185.255.198.35	8	0

At the bottom, it shows "1s 200ms" and "Display time (UTC+00:00)". The footer indicates "Query details" and "1 - 3 of 3".

Results		Chart	Add bookmark		
<input type="checkbox"/> ActorObjectId	Caller	CallerIpAddress	Writes	Deletes	
<input type="checkbox"/> > 04cd29c3-f1d4-4305-963b-32598abbd847	41df752adccd0f0b74e799730b...	14.198.39.113	6	1	
<input type="checkbox"/> > 04cd29c3-f1d4-4305-963b-32598abbd847	41df752adccd0f0b74e799730b...	111.249.69.112	0	1	
<input type="checkbox"/> > 04cd29c3-f1d4-4305-963b-32598abbd847	41df752adccd0f0b74e799730b...	185.255.198.35	8	0	

Findings for Account: 04cd29c3-f1d4-4305-963b-32598abbd847

- **Caller (service principal or UPN hash):** 41df752adccd0f0b74e799730b...
- **Multiple IP addresses involved:**
 - 14.198.39.113 → 6 writes, 1 delete
 - 111.249.69.112 → 0 writes, 1 delete
 - 185.255.198.35 → 8 writes, 0 deletes
- **Total activity:** 14 successful resource creation (WRITE) operations and 2 successful resource deletion (DELETE) operations in the last 7 days.
- **Behavior:** High churn of resource creation/deletion from different public IPs, which can look suspicious (automation, possible compromised identity, or scripted activity).

This query gives us a timeline view:

```
let AlertedId = "04cd29c3-f1d4-4305-963b-32598abbd847";
```

```
AzureActivity
```

```
| where TimeGenerated >= ago(7d)
```

```
| extend ClaimsJson = parse_json(Claims)
```

```
| extend ActorObjectId =
```

```
tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
```

```

| where ActorObjectId == AlertedId

| where ActivityStatusValue == "Success"

| extend OpNameLower = tolower(OperationNameValue)

| summarize

    Writes = countif(OpNameLower endswith_cs "write"),

    Deletes = countif(OpNameLower endswith_cs "delete")

by bin(TimeGenerated, 1h)

| order by TimeGenerated asc

```

Microsoft Sentinel | Logs ...
 Selected workspace: 'law-cyber-range'

New Query 1* ... × +

Run Time range: Set in query Show: 1000 results

```

180 AzureActivity
181 | where TimeGenerated >= ago(7d)
182 | extend ClaimsJson = parse_json(Claims)
183 | extend ActorObjectId = tostring(ClaimsJson["http://schemas.microsoft.com/identity/claims/objectidentifier"])
184 | where ActorObjectId == AlertedId
185 | where ActivityStatusValue == "Success"
186 | extend OpNameLower = tolower(OperationNameValue)
187 | summarize
188 |     Writes = countif(OpNameLower endswith_cs "write"),
189 |     Deletes = countif(OpNameLower endswith_cs "delete")
190 | by bin(TimeGenerated, 1h)

```

Results Chart Add bookmark

<input type="checkbox"/>	TimeGenerated [UTC]	Writes	Deletes
<input type="checkbox"/>	> 9/24/2025, 11:00:00.000 AM	0	1
<input type="checkbox"/>	> 9/24/2025, 12:00:00.000 PM	6	0
<input type="checkbox"/>	> 9/25/2025, 12:00:00.000 AM	0	1
<input type="checkbox"/>	> 9/29/2025, 6:00:00.000 PM	8	0

We can say when those writes/deletes happened.

This has been classified as: **True Positive**

The account 04cd29c3-f1d4-4305-963b-32598abbd847 executed 14 resource creation events and 2 deletions across 3 distinct public IP addresses within the past 7 days. The activity pattern, including multiple originating IPs and volume of operations, deviates from expected behavior and may indicate a compromised account or unauthorized automation. Immediate containment actions are recommended, including disabling the account and reviewing recent sign-ins from the observed IPs.

Incident Summary

An analytics rule triggered in Microsoft Sentinel identifying an account that performed excessive Azure resource creation and deletion operations.

- **Account (ObjectIdentifier):** 04cd29c3-f1d4-4305-963b-32598abbd847
- **Caller:** 41df752adccd0f0b74e799730b...
- **Source IPs observed:**
 - 14.198.39.113 → 6 writes, 1 delete
 - 111.249.69.112 → 0 writes, 1 delete
 - 185.255.198.35 → 8 writes, 0 deletes
- **Total operations (7-day lookback):** 14 writes, 2 deletes

The activity originated from **multiple public IP addresses**, indicating possible automation or suspicious behavior.

MITRE ATT&CK Mapping

- **Technique T1485 – Data Destruction** (resource deletions may represent destructive activity)
- **Technique T1496 – Resource Hijacking** (rapid resource creation can indicate resource abuse or crypto-mining attempts)

NIST SP 800-61r2 — Incident Response Lifecycle

1. Preparation

- Tools used: Microsoft Sentinel, Log Analytics Workspace, AzureActivity logs.
- Roles: SOC Analyst (student), Incident Handler.
- Playbooks available for disabling accounts and escalating to management.

2. Detection & Analysis

- Analytics rule fired after detecting ≥ 5 writes/deletes in a 7-day period.
- Sentinel Incident captured `ObjectIdentifier = 04cd29c3-f1d4-4305-963b-32598abbd847`.
- KQL investigation confirmed **14 writes + 2 deletes** tied to this identity, spread across three distinct public IPs.
- Behavior deviates from expected single-source or low-volume provisioning.

Assessment: Potential compromise or unauthorized automation.

3. Containment, Eradication, Recovery

- **Containment:** In a real environment, the account would be disabled in Entra ID, and tokens revoked.
- **Eradication:** Investigate associated automation scripts, service principals, or keys tied to the account.
- **Recovery:** Re-enable account only after investigation, reset credentials, and monitor post-remediation.

4. Post-Incident Activity

- Documented findings in Sentinel Incident.

- Recommend tuning the alert threshold if too noisy.
- Consider Azure Policy or conditional access rules to restrict excessive resource creation from non-corporate IPs.

Lessons Learned:

Multi-IP origin for a single identity is a strong indicator for additional monitoring rules.

Incident Closure

- **Disposition:** Mark as **True Positive** (lab context).
- **Notes:** The account was observed creating and deleting resources in a pattern inconsistent with normal usage. Activity spanned multiple IP addresses. Containment and remediation steps outlined.
- Incident closed per NIST SP 800-61r2 lifecycle.