**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.

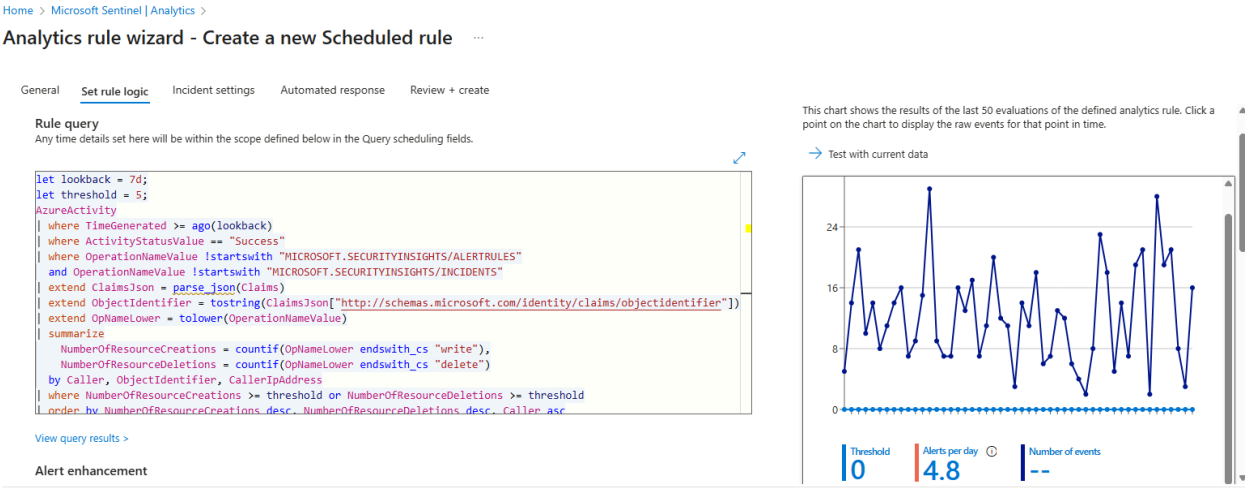
**Created a Virtual Machine at:** https://portal.azure.com/


**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**:




**Alert Rule Successfully Created**.

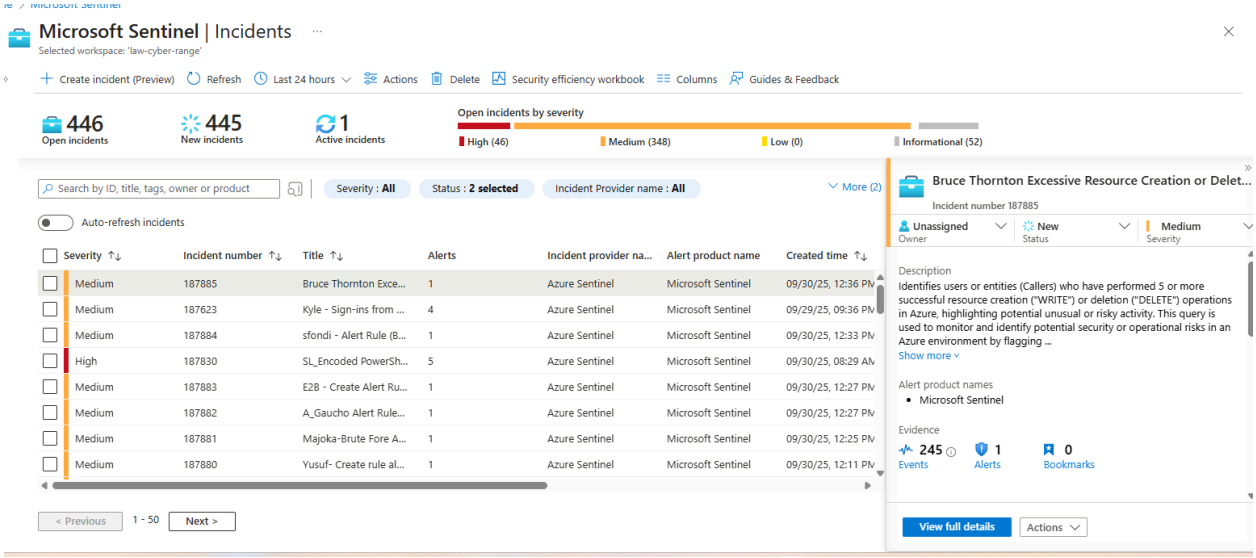
Creation time
09/30/25, 12:36 PM

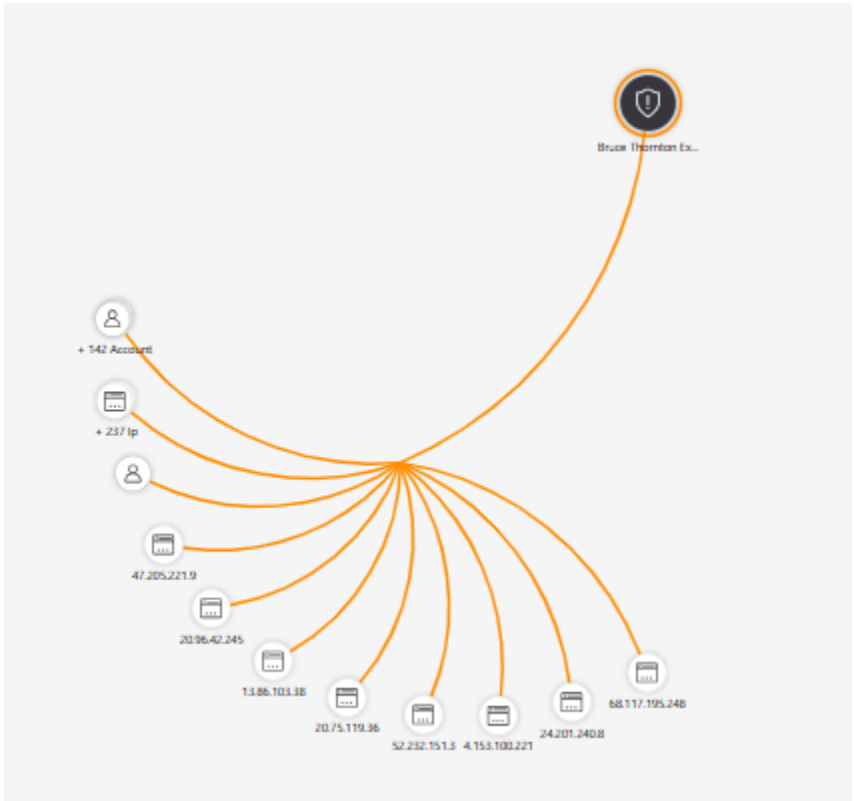
---

## Part 2: Alert Has Been Triggered

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

This alert did not require my assistance to be triggered.



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

---

**Part 3: Working the Incident**

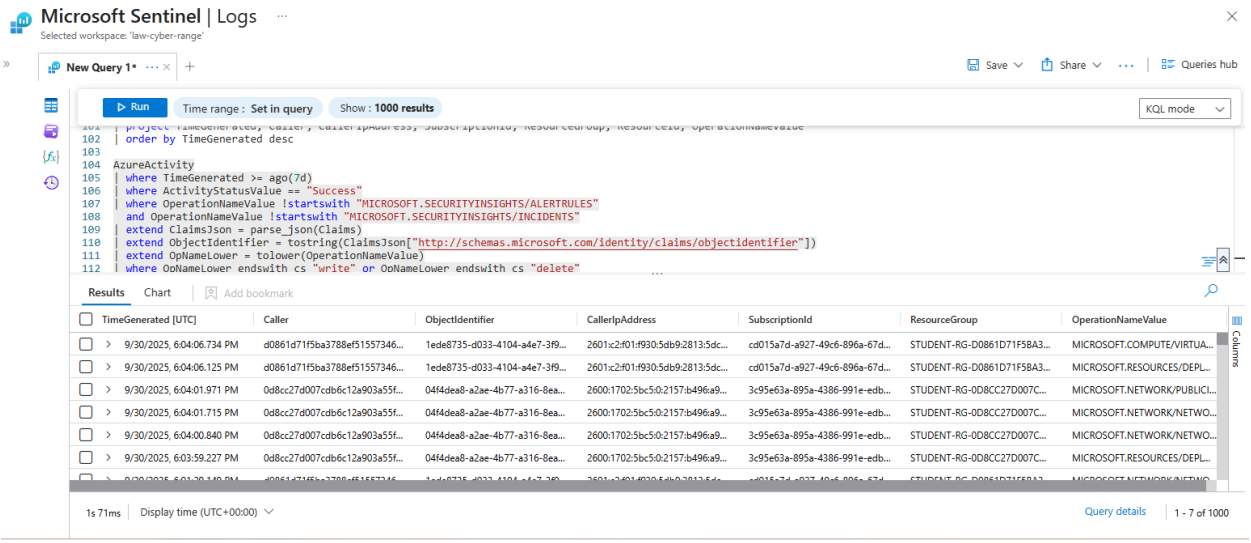
*Incident response guidance is from NIST SP 800-61r2.

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
```




**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")

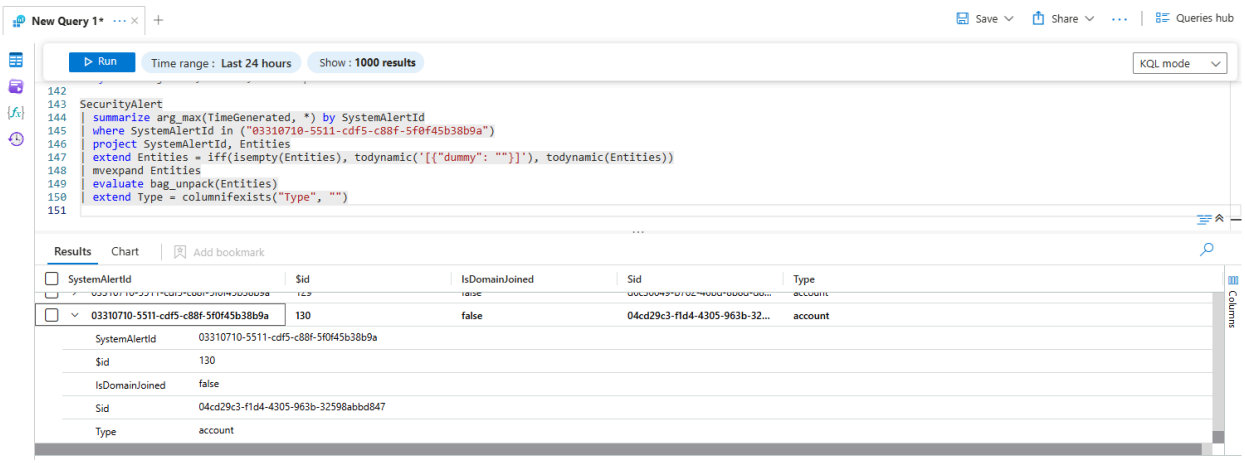
| project SystemAlertId, Entities

| extend Entities = iff(isempty(Entities), todynamic('[{"dummy": ""}]'), todynamic(Entities))

| mvexpand Entities

| evaluate bag_unpack(Entities)

| extend Type = columnifexists("Type", "")




**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)

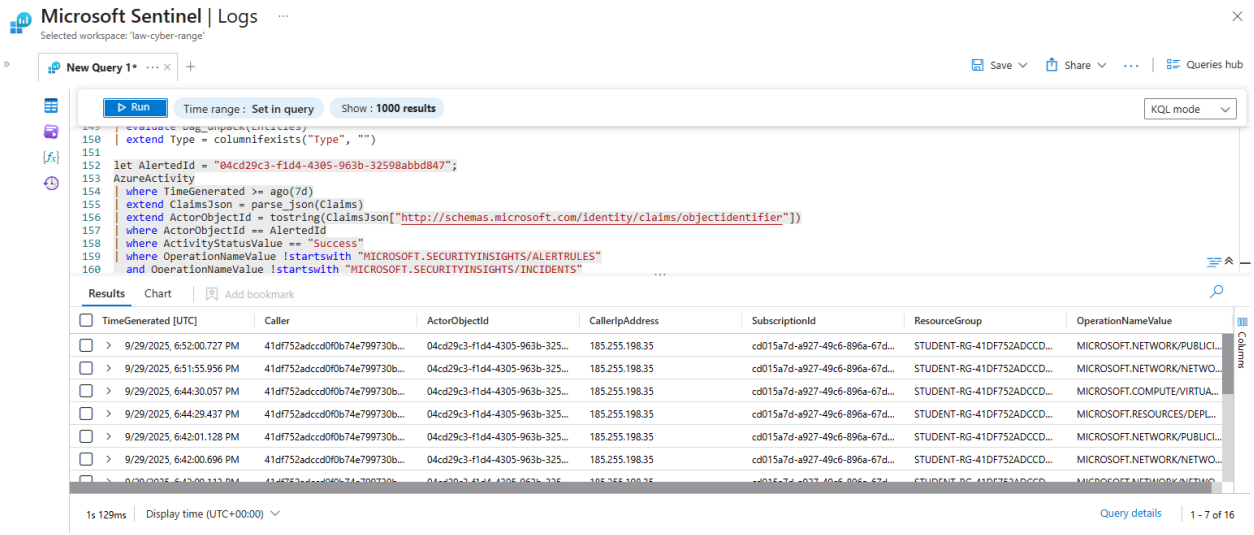
| extend ClaimsJson = parse_json(Claims)

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

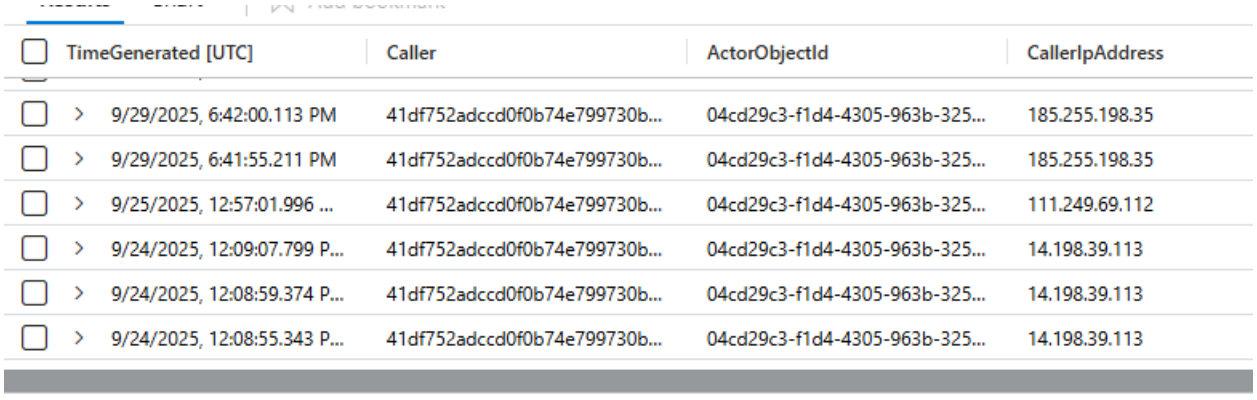
| where ActorObjectId == AlertedId

| 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
```

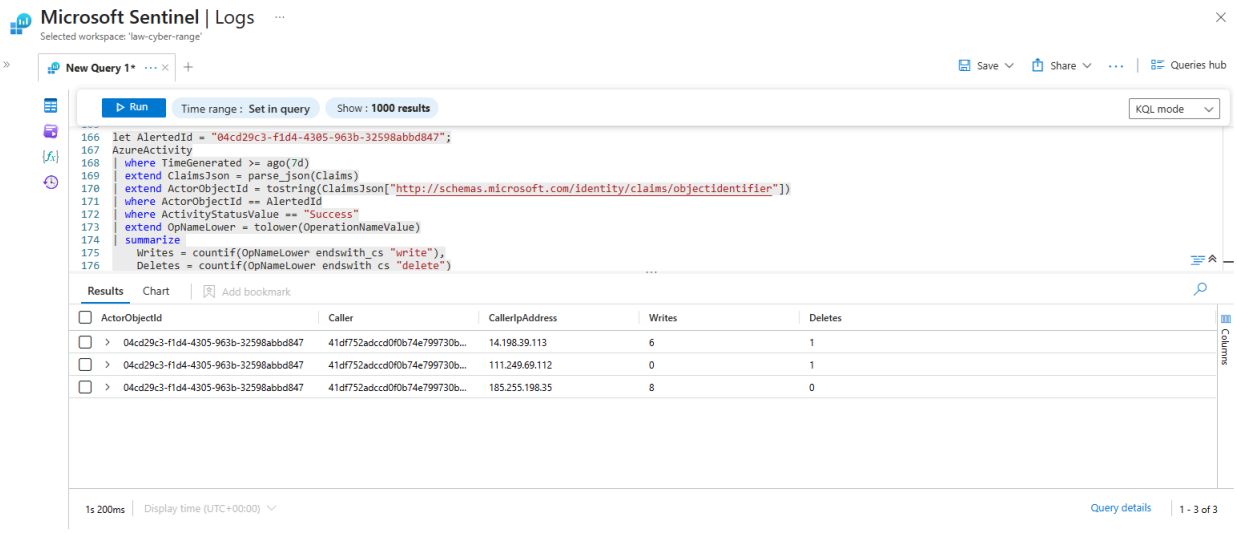


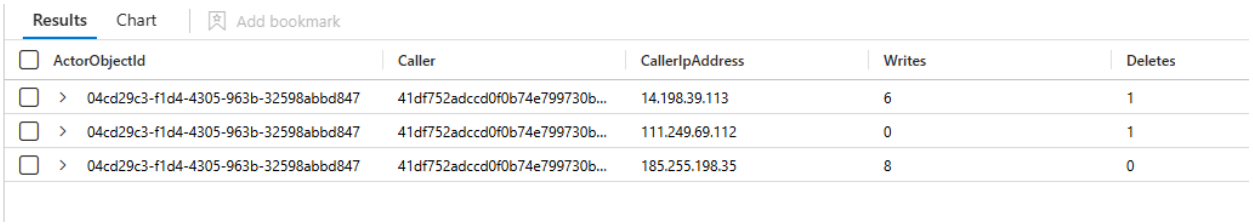

**This returns 16 entries that span 3 different CallerIpAddresses coming from this specific Caller**:



**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
```





Results | Chart | Add bookmark

| 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 |

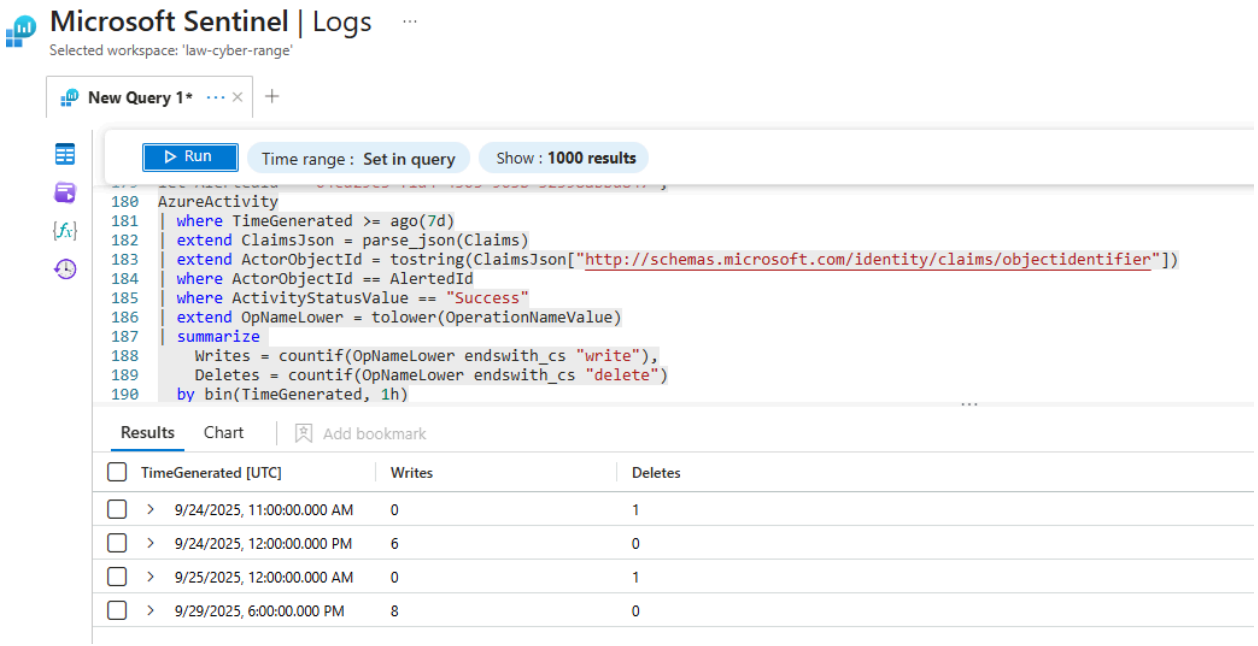
## Findings for Account: `04cd29c3-f1d4-4305-963b-32598abbd847`

- **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
```




**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.