Understanding the “Solorigate Network Beacon” Incident

Intro (What & Why)

The **Solorigate Network Beacon** incident represents a detection related to the SolarWinds supply chain compromise.

In this scenario, Microsoft Sentinel identified network activity matching a known **malicious domain IOC** associated with the SolarWinds campaign.

This typically means:

- A host in the environment attempted communication with a suspicious domain
- That domain matches a known threat intelligence indicator
- The analytics rule triggered based on IOC correlation

However, an alert does not automatically mean compromise.

Our goal as SOC analysts is to determine:

- Did a system actually communicate with a known malicious domain?
- Was it DNS resolution only, or a full network connection?
- Which host initiated the activity?
- Is the IOC still active and valid?
- Are there related events indicating lateral movement or persistence?

Investigation Objective

In this investigation, we will:

- Identify the affected host
- Validate the domain IOC
- Review raw logs that triggered the alert
- Confirm the timeline of activity
- Check for additional related alerts

- Determine whether the alert represents:
    - A **true positive** (confirmed suspicious activity), or
    - A **false positive** (benign or lab-generated simulation)

What Confirms a True Positive?

Indicators of a true positive may include:

- Confirmed communication with a malicious domain
- Multiple connections over time
- Related suspicious activity from the same host
- IOC confidence score is high
- Domain tied to known campaign behavior

What Suggests a False Positive?

Indicators of a false positive may include:

- IOC expired or low confidence
- Only a single DNS lookup without connection
- Lab-generated synthetic data
- No follow-up suspicious behaviour

Steps

1. Locate the Incident

We need to first identify the Solorigate incident.

We should:

- Sort incidents by severity and take the High risk alert for investigation
- Check incident status (New / Active)

In this training solution, multiple alerts are **grouped together under one incident**.

This means:

- One incident
- Multiple related alerts
- Same campaign context (Solorigate)

Inside the incident page, you will notice a **grouped alerts icon / alert count indicator**.

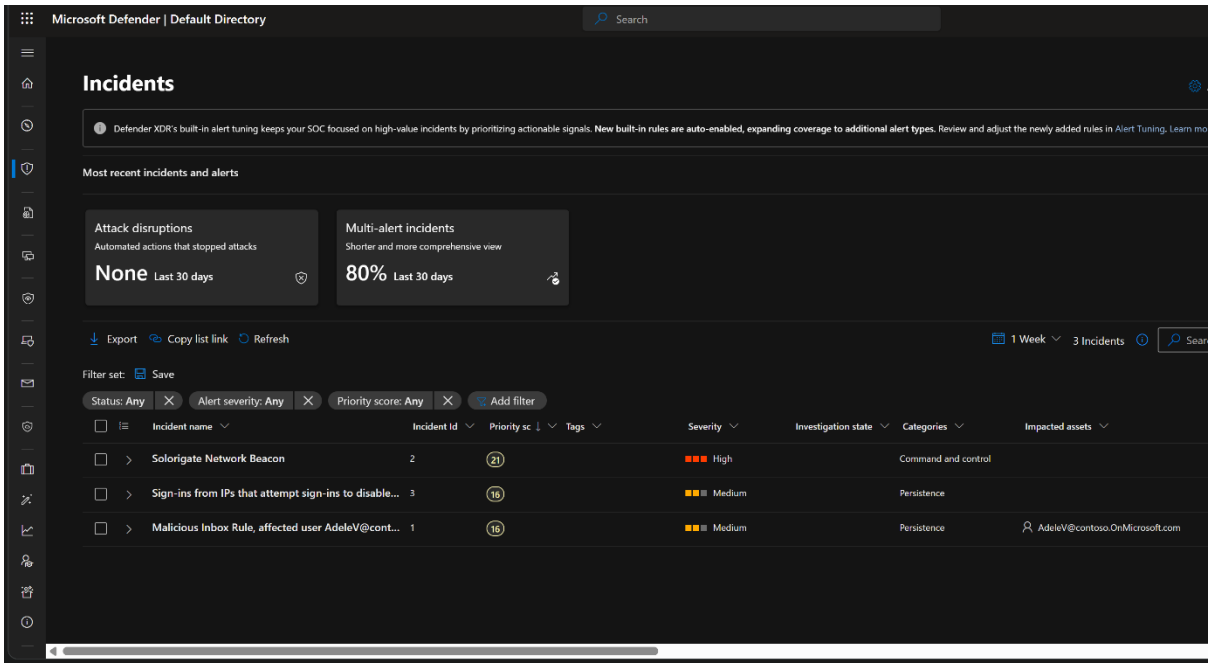
When we select that grouped alert indicator:

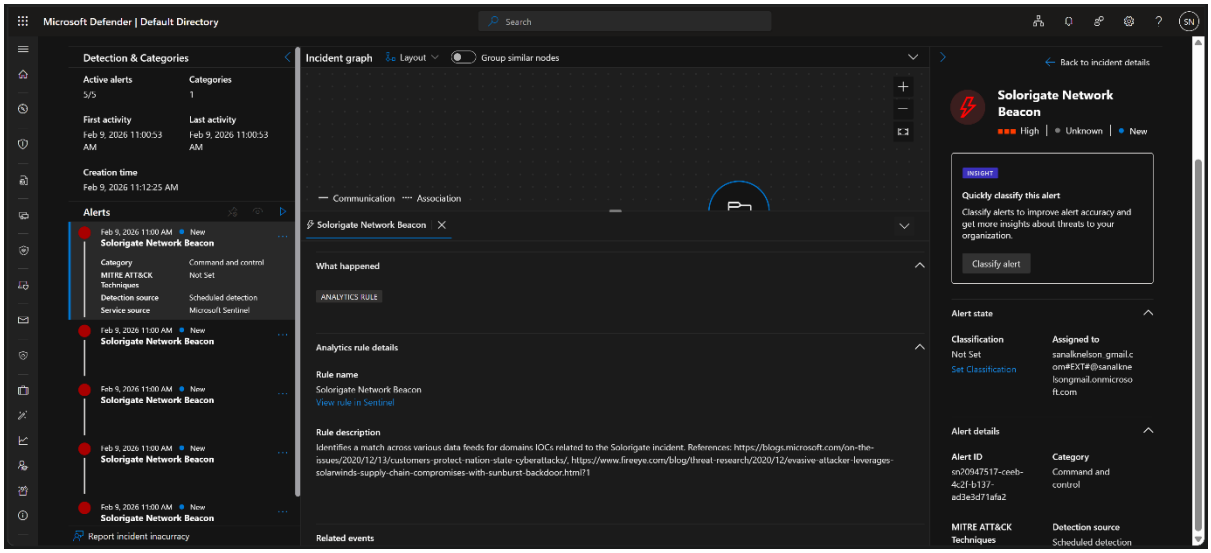
- It opens a **separate detailed alert window**
- Each alert has its own page
- This page contains deeper technical evidence

This is the correct workflow in the new Defender portal.

GUI Flow (Microsoft Defender Portal)

Browser → https://security.microsoft.com → Microsoft Sentinel → Incidents





1A. Take Ownership of the Incident

Before starting any investigation, we must formally take ownership of the incident.

This ensures:

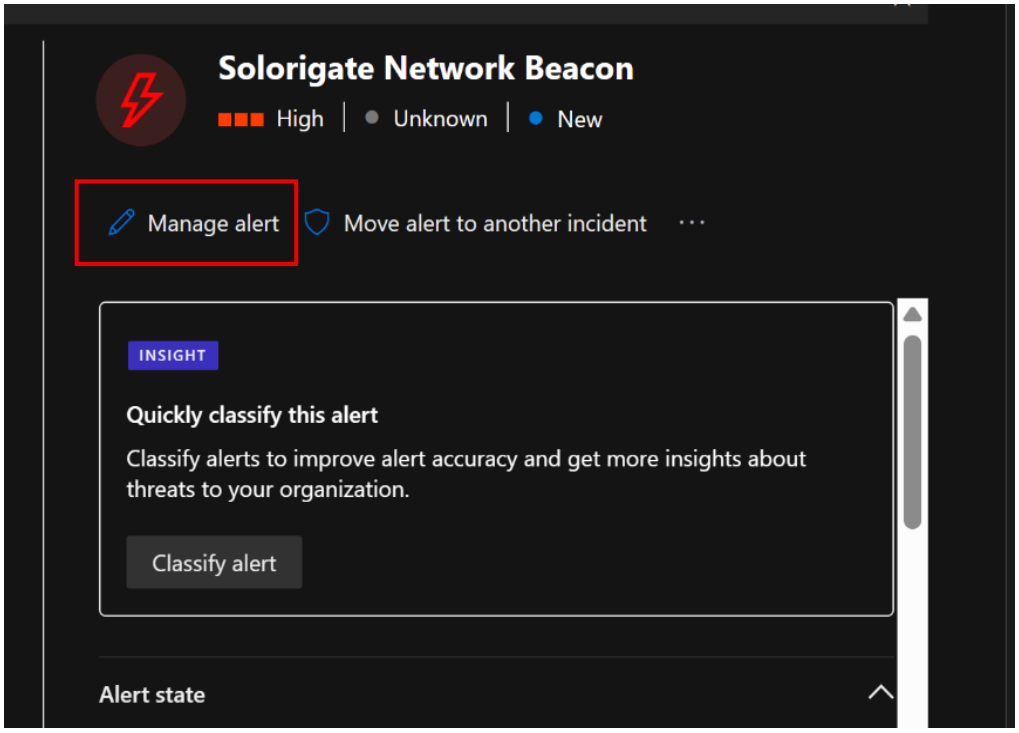
- Clear accountability
- Avoidance of duplicate investigations
- Proper SOC workflow tracking

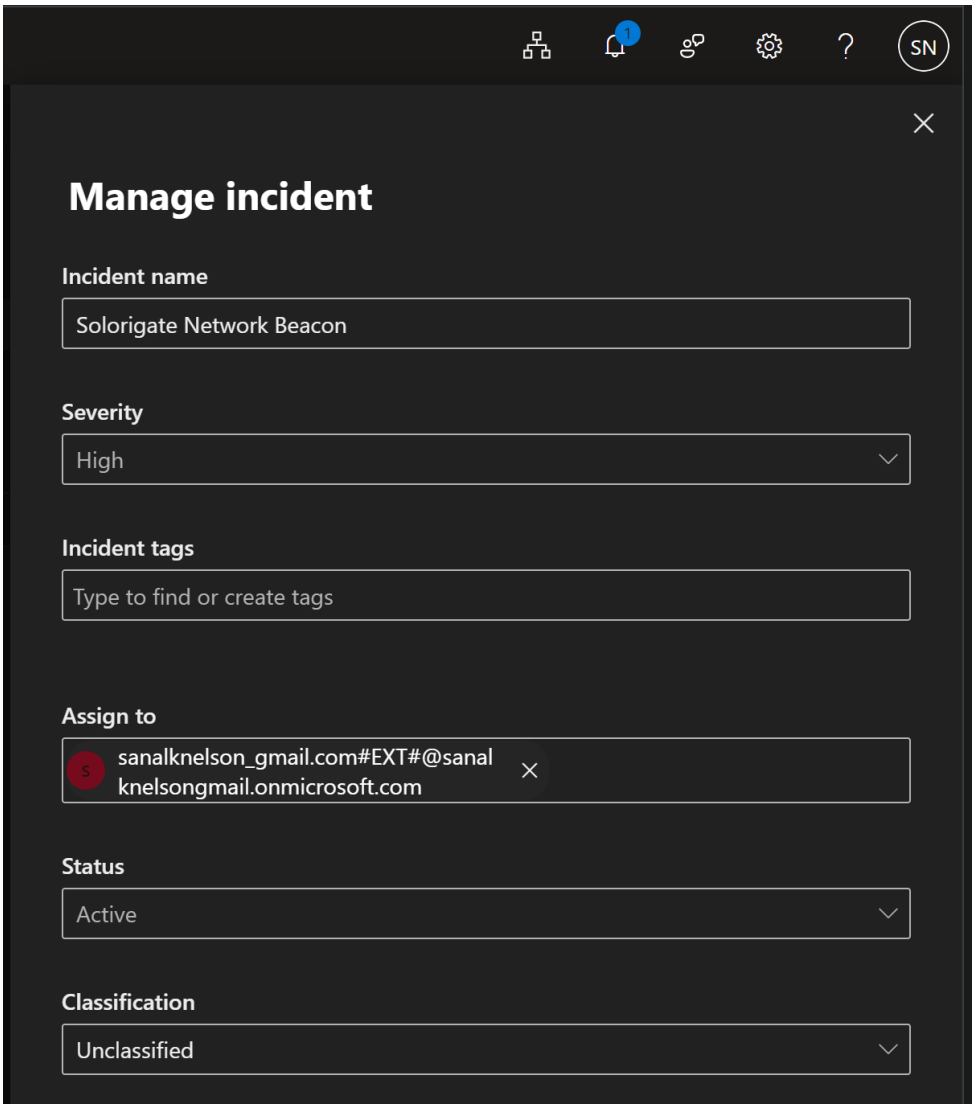
We should:

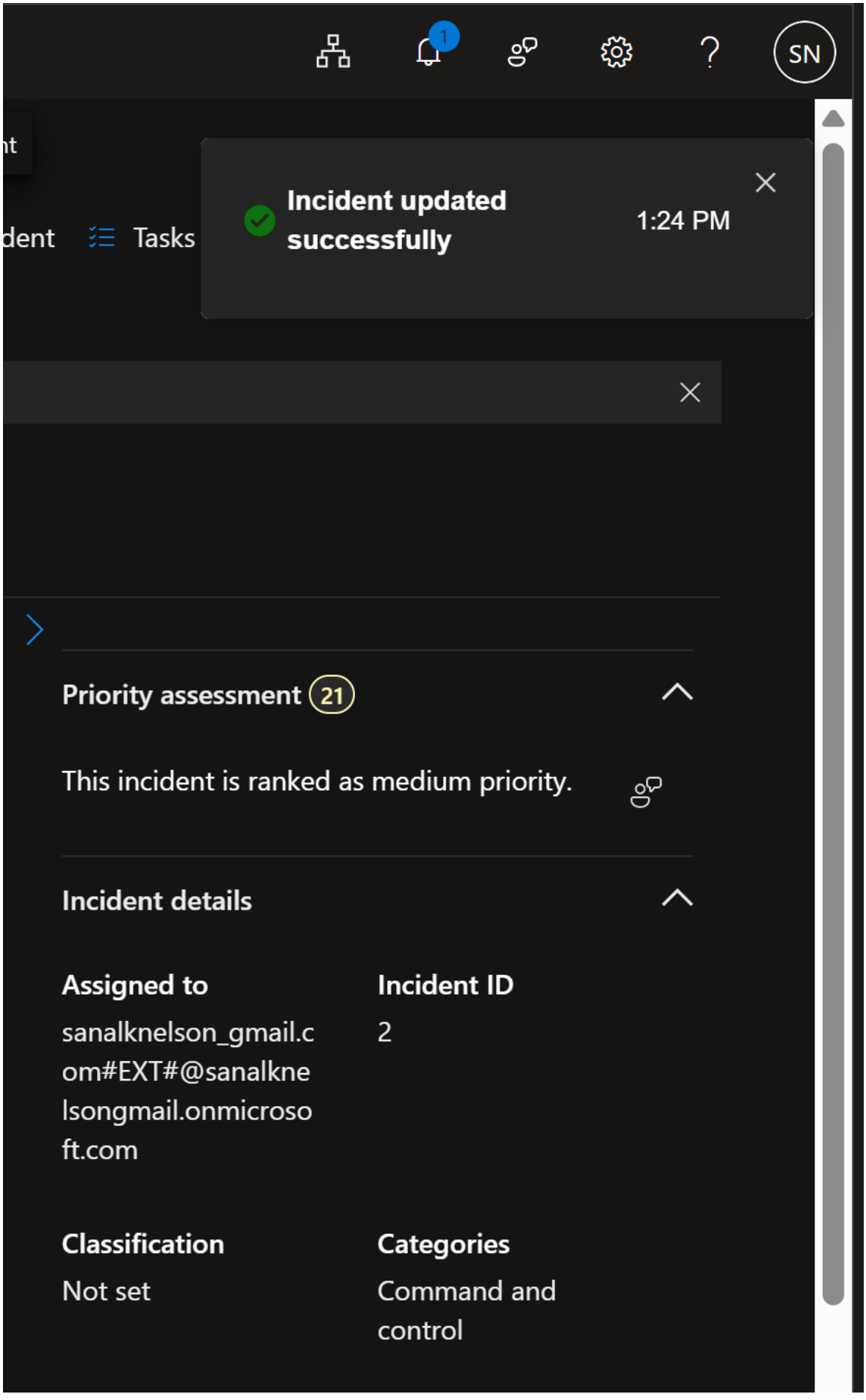
- Change status from **New → Active**
- Assign the incident to ourselves
- Confirm ownership is reflected in the incident header

GUI Flow (Microsoft Defender Portal)

Browser → https://security.microsoft.com → Microsoft Sentinel → Incidents → Select an Incident → Manage Incident → Follow Screenshots


Solorigate Network Beacon
High
Unknown
New
Manage alert
Move alert to another incident
INSIGHT
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.
Classify alert
Alert state


SN
Manage incident
Incident name
Solorigate Network Beacon
Severity
High
Incident tags
Type to find or create tags
Assign to
sanalknelson_gmail.com#EXT#@sanal knelsongmail.onmicrosoft.com
Status
Active
Classification
Unclassified


1
SN
dent
Tasks
Incident updated successfully
1:24 PM
Priority assessment 21
This incident is ranked as medium priority.
Incident details
Assigned to
sanalknelson_gmail.com#EXT#@sanalknelsongmail.onmicrosoft.com
Incident ID
2
Classification
Not set
Categories
Command and control

2. Review Incident Overview

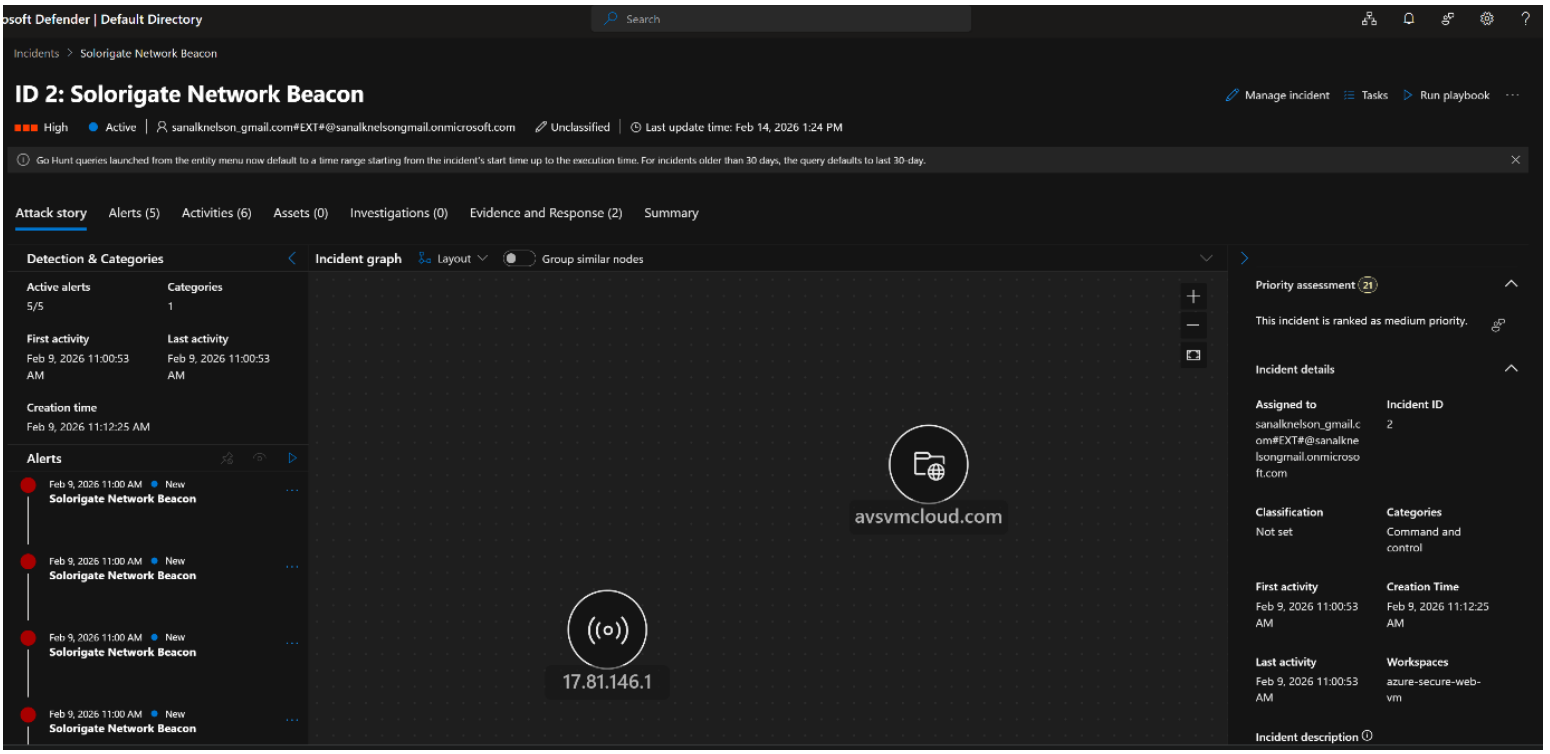
Open the incident and review:

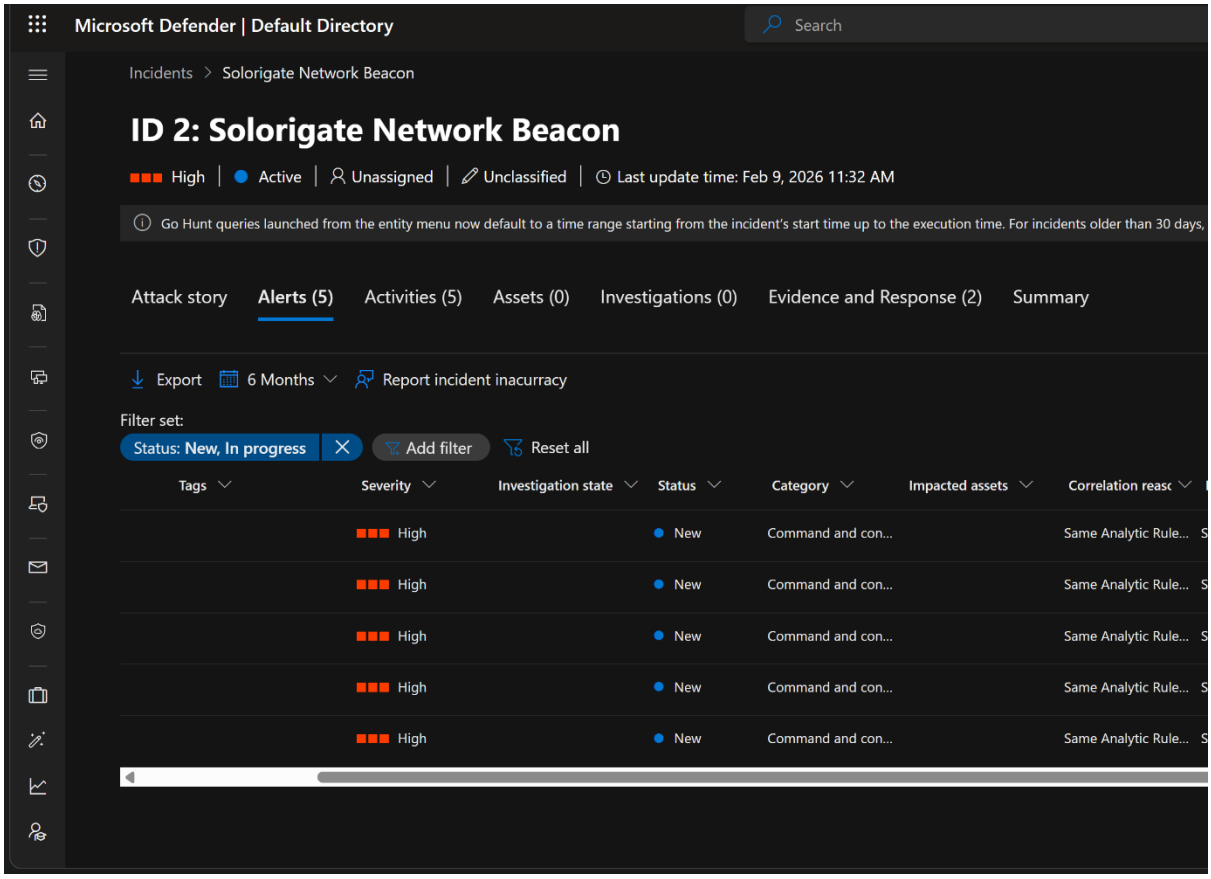
- Description
- Severity
- MITRE tactics
- Alert count
- Detection source

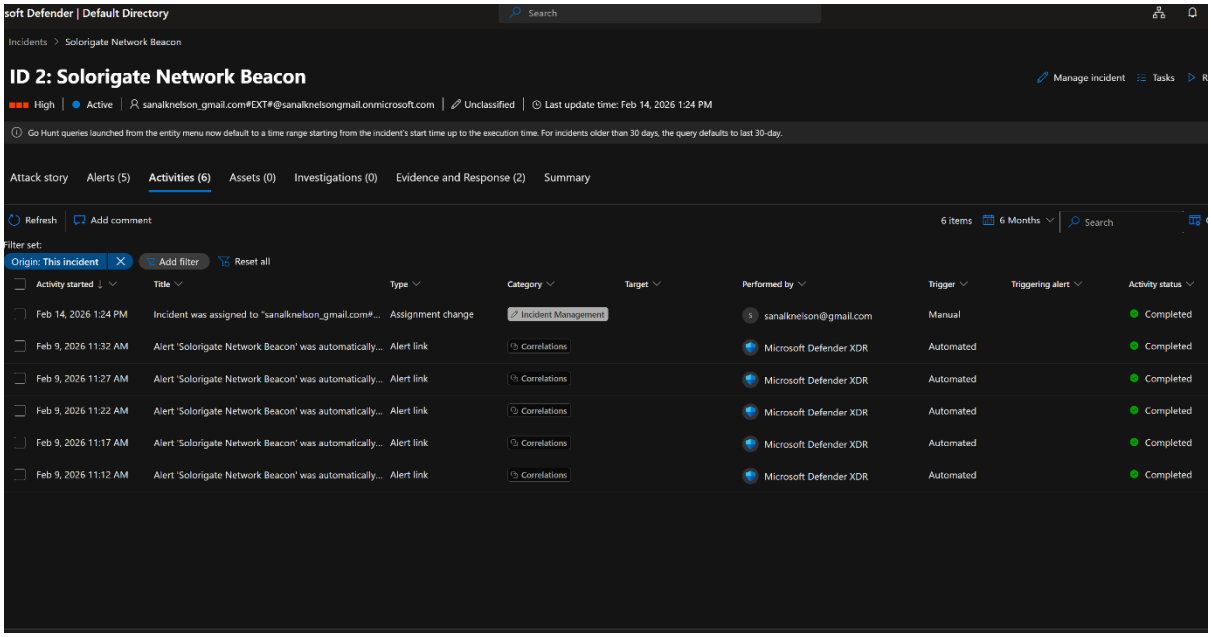
We should:

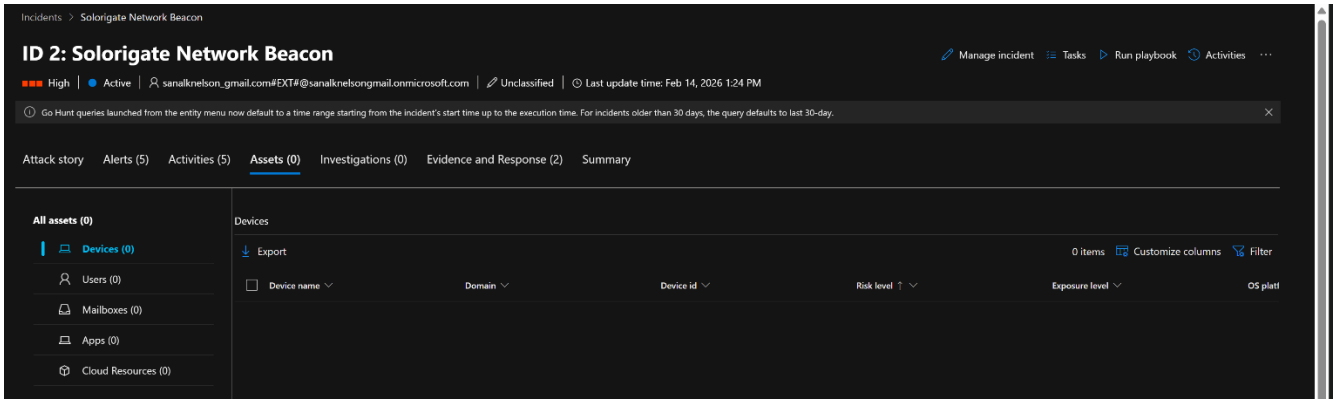
- Understand why the rule triggered
- Confirm which analytics rule created it

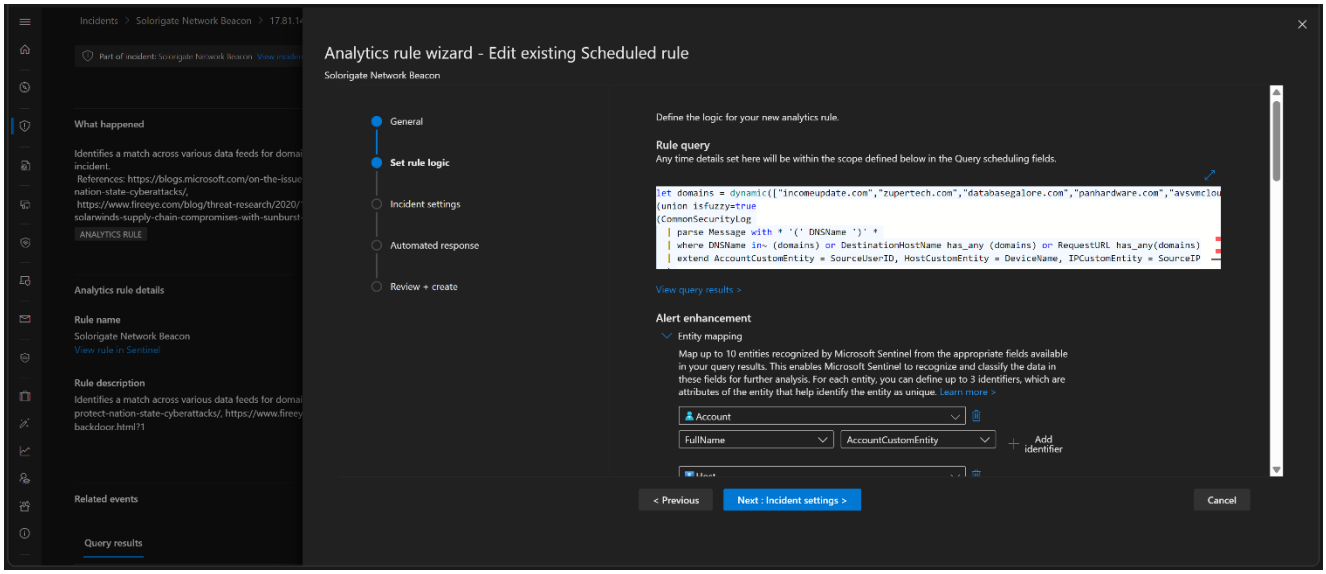
This step is basic triage.




Microsoft Defender | Default Directory
Search
Incidents > Solorigate Network Beacon
ID 2: Solorigate Network Beacon
High | Active | Unassigned | Unclassified | Last update time: Feb 9, 2026 11:32 AM
Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days,
Attack story
Alerts (5)
Activities (5)
Assets (0)
Investigations (0)
Evidence and Response (2)
Summary
Export
6 Months
Report incident inacurracy
Filter set:
Status: New, In progress
Add filter
Reset all
Tags
Severity
Investigation state
Status
Category
Impacted assets
Correlation reasc
High
New
Command and con...
Same Analytic Rule...


soft Defender | Default Directory
Search
Incidents > Solorigate Network Beacon
ID 2: Solorigate Network Beacon
Manage incident
Tasks
High | Active | sanalknelson_gmail.com#EXT#@sanalknelsongmail.onmicrosoft.com | Unclassified | Last update time: Feb 14, 2026 1:24 PM
Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.
Attack story
Alerts (5)
Activities (6)
Assets (0)
Investigations (0)
Evidence and Response (2)
Summary
Refresh
Add comment
6 items
6 Months
Search
Filter set:
Origin: This incident
Add filter
Reset all
Activity started
Title
Type
Category
Target
Performed by
Trigger
Triggering alert
Activity status
Feb 14, 2026 1:24 PM
Incident was assigned to "sanalknelson_gmail.com#...
Assignment change
Incident Management
sanalknelson@gmail.com
Manual
Completed
Feb 9, 2026 11:32 AM
Alert 'Solorigate Network Beacon' was automatically...
Alert link
Correlations
Microsoft Defender XDR
Automated
Completed
Feb 9, 2026 11:27 AM
Alert 'Solorigate Network Beacon' was automatically...
Alert link
Correlations
Microsoft Defender XDR
Automated
Completed
Feb 9, 2026 11:22 AM
Alert 'Solorigate Network Beacon' was automatically...
Alert link
Correlations
Microsoft Defender XDR
Automated
Completed
Feb 9, 2026 11:17 AM
Alert 'Solorigate Network Beacon' was automatically...
Alert link
Correlations
Microsoft Defender XDR
Automated
Completed
Feb 9, 2026 11:12 AM
Alert 'Solorigate Network Beacon' was automatically...
Alert link
Correlations
Microsoft Defender XDR
Automated
Completed





(Rule that triggered the incident. To view check " Analytics rule details")

3. Analyze Entities

Go to the **Entities tab**.

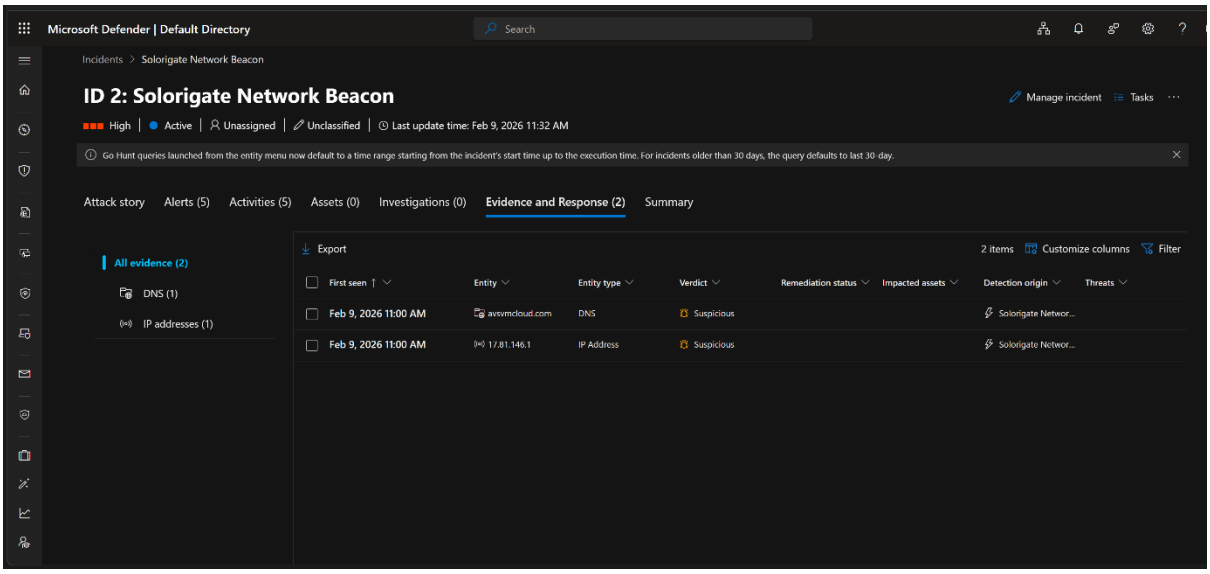
We should see:

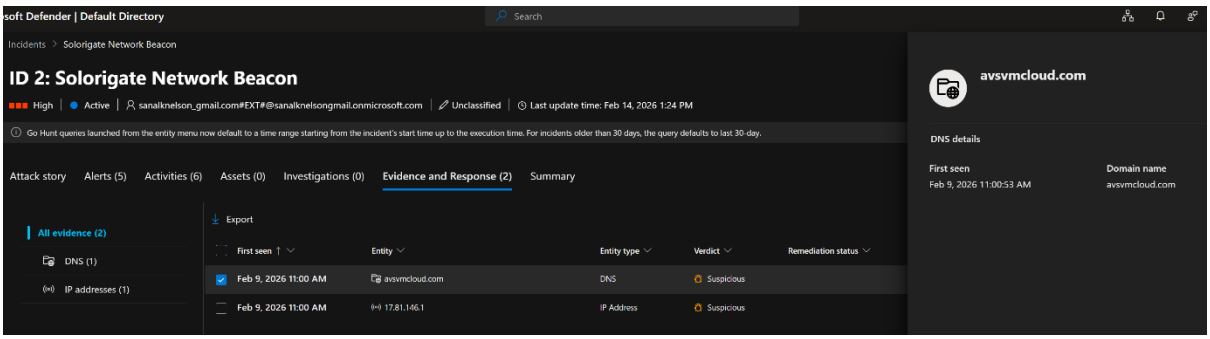
- Domain IOC (example: avsvmcloud.com)
- Possibly related hosts
- Possibly related IP addresses

Click the domain entity to inspect:

- Related alerts
- First seen / Last seen
- Related activities

This confirms the domain IOC match.





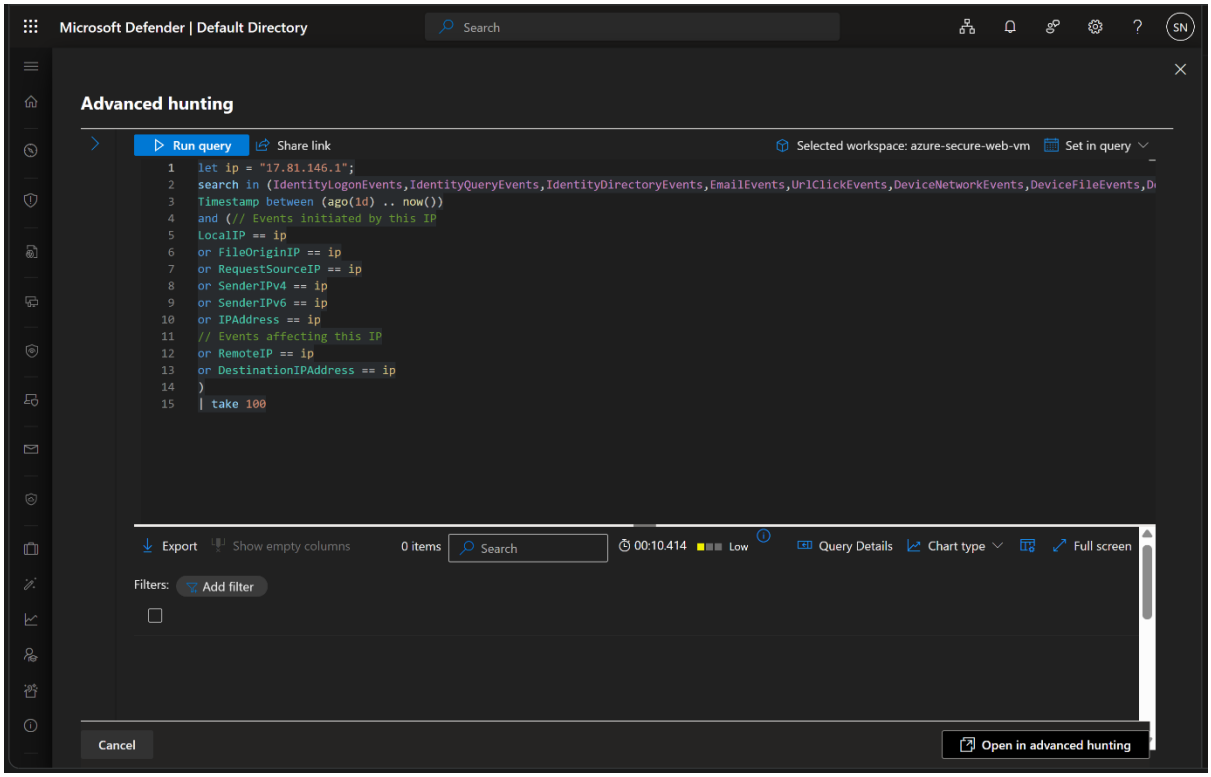
4. Use “Go Hunt” for Advanced Analysis

The Defender portal provides a built-in option:

Go hunt

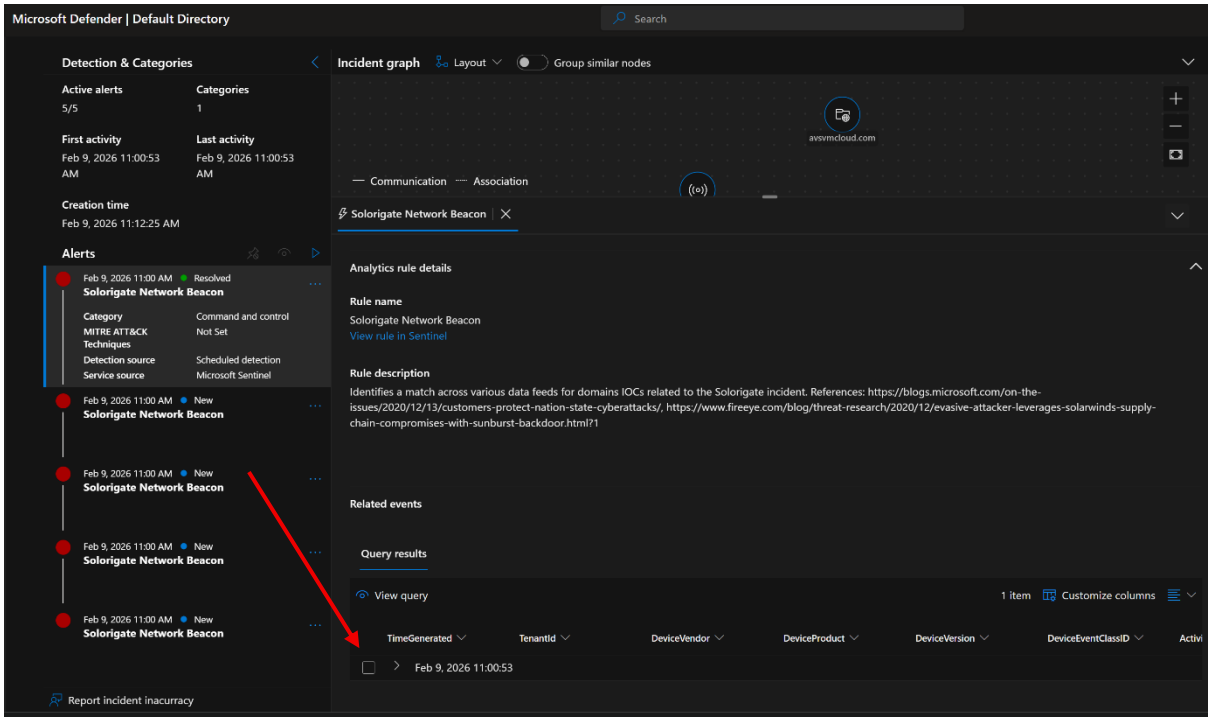
This allows us to pivot directly into advanced hunting using the context of the alert.

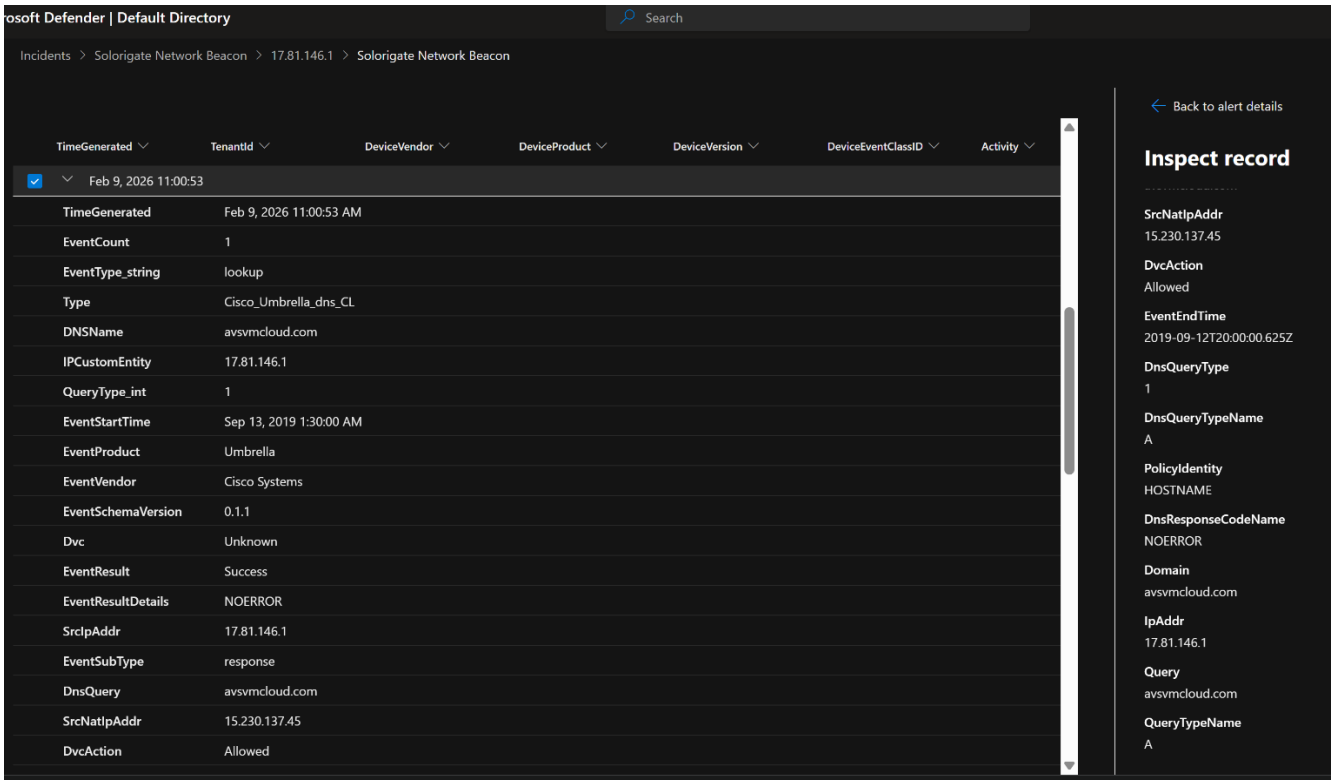
Instead of manually copying indicators, we let Defender auto-build a hunting query.



(This pre-built search queries a wide range of tables related to the incident)

5. Pivot to Raw Logs





From this log you can understand the details of one DNS request made by a machine to a domain, and that it was allowed.

Key points in simple words:

- **Product/source**: Log comes from Cisco Umbrella DNS (field: Type = Cisco_Umbrella_dns_CL, EventProduct = Umbrella, EventVendor = Cisco Systems).
- **What happened**: A DNS lookup/response event (field: EventType_string = lookup, EventSubType = response, EventResult = Success, EventResultDetails = NOERROR).
- **Domain**: The machine queried avsvmcloud.com (fields: DNSName and DnsQuery).
- **Client IP**: Internal/source IP is 17.81.146.1 (fields: IPCustomEntity, SrcIpAddr, IpAddr).
- **External IP**: SrcNatIpAddr = 15.230.137.45 shows the public/NAT address used on the internet.

- **Time**: The DNS event happened around Sep 13, 2019 1:30 AM to Sep 13, 2019 11:00:53 AM (fields: EventStartTime, TimeGenerated, EventEndTime 2019-09-12T20:00:00.625Z).
- **Action**: DvcAction = Allowed means Umbrella let this DNS traffic go through; it was not blocked.

Why this is important for the Solarigate/Sunburst lab:

- avsvmcloud.com is a known malicious C2 domain used in the SolarWinds Solorigate attack, so this log is evidence that the host 17.81.146.1 contacted that bad domain via DNS and the request succeeded.
- As a SOC analyst, you would treat this as a strong indicator that this host may be compromised and needs deeper investigation (check processes, connections, other alerts, isolate if needed).

The suspicious DNS avsvmcloud.com and the IP 17.81.146.1 are two representations of the same communication path in this incident.

- The DNS name is the **domain** the system tried to resolve or contact (an IOC related to Solorigate).
- The IP address is the **resolved network endpoint** that the DNS name pointed to at the time, or an IP that communicated in relation to that domain (e.g., outbound connection after DNS resolution).
- Defender links both as **evidence** in the same incident because traffic involving avsvmcloud.com either resolved to, or was associated with, 17.81.146.1, indicating possible command-and-control communication.

6. Correlate with Threat Intelligence (Optional but Strong)

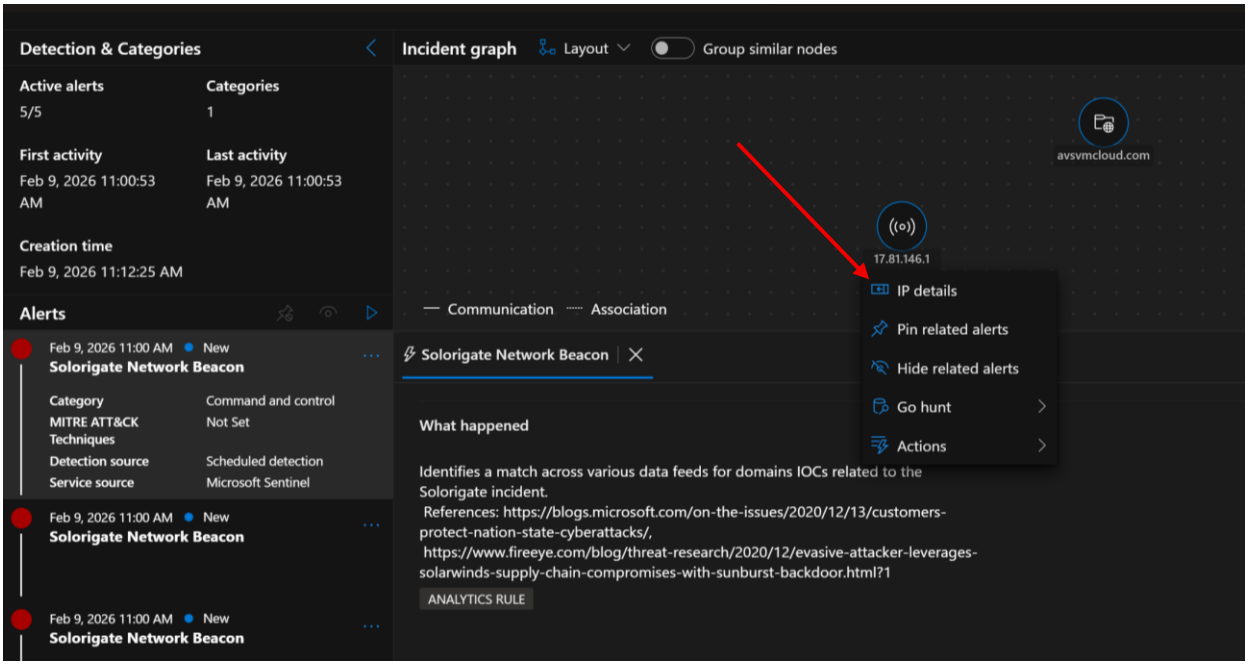
If Threat Intelligence is enabled:

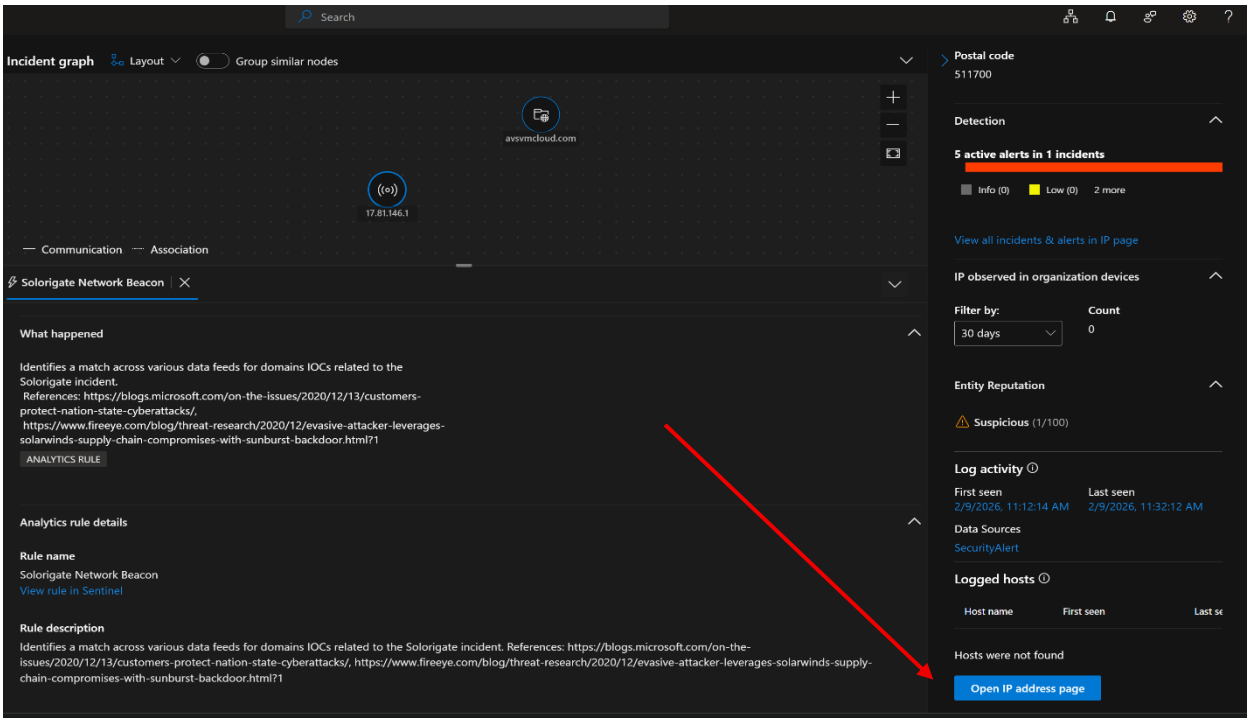
Microsoft Sentinel → Threat intelligence → Search IP

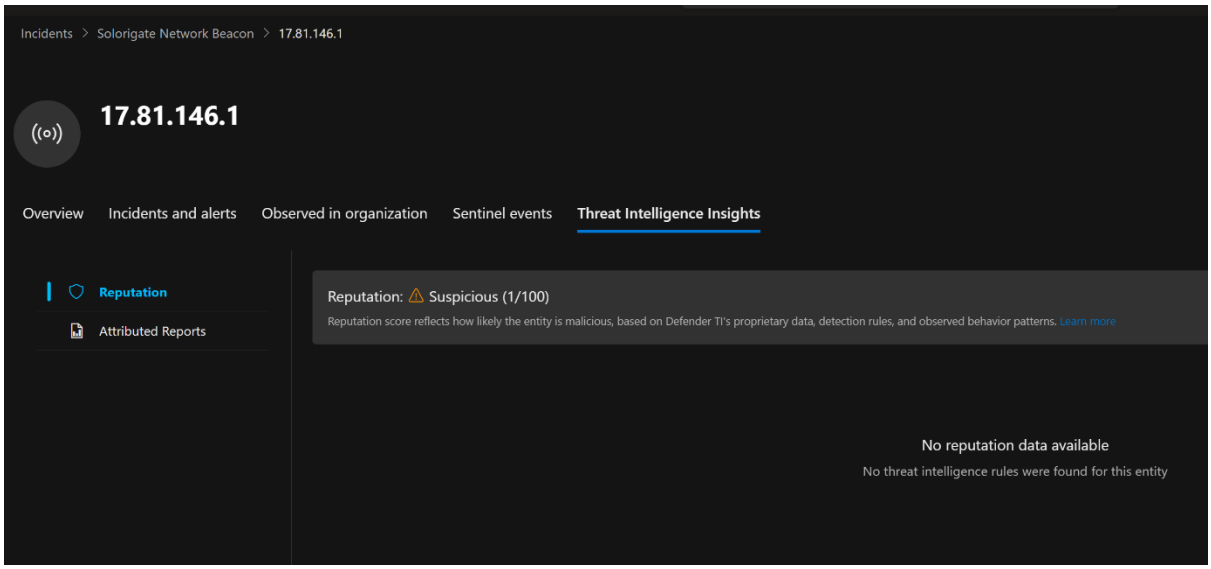
This strengthens analysis quality.

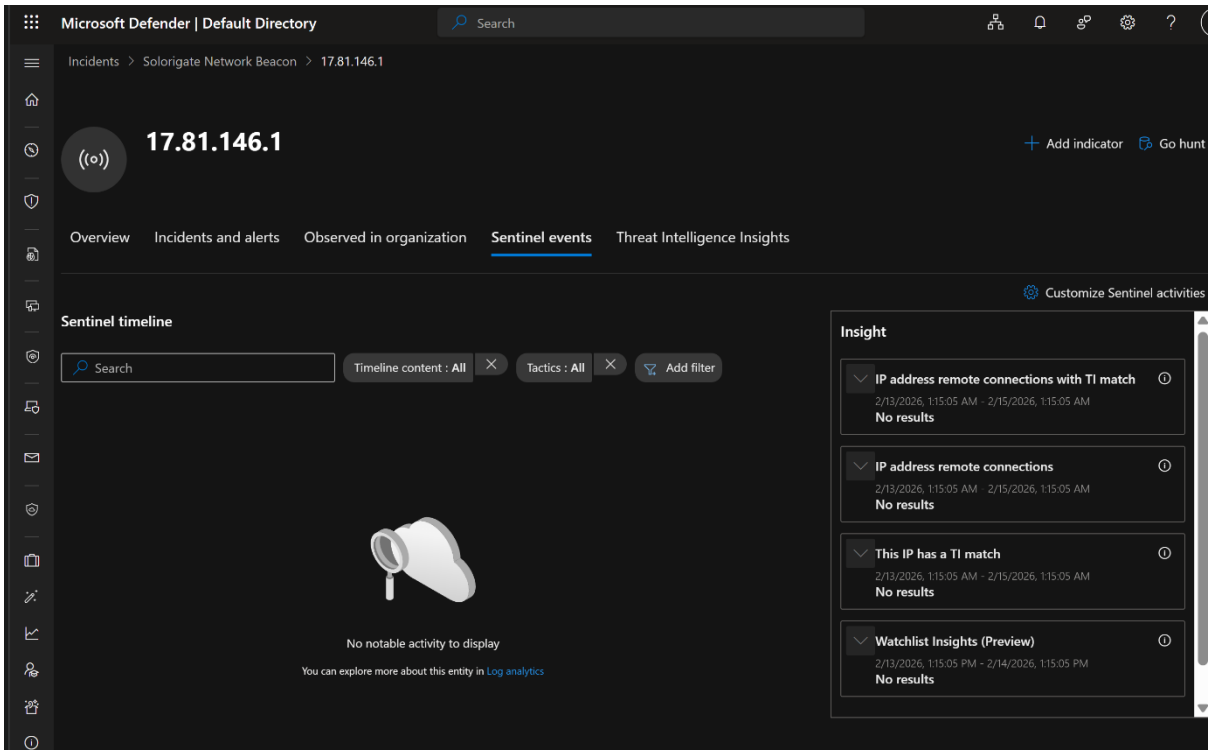
GUI Flow

Select **Solorigate Network Beacon** alert → Incident graph → Click IP **17.81.146.1** → **IP details** → **Open IP address page** to view detection summary, alert count, reputation, first seen/last seen, and related activity.






Incidents > Solorigate Network Beacon > 17.81.146.1
17.81.146.1
Overview
Incidents and alerts
Observed in organization
Sentinel events
Threat Intelligence Insights
Reputation
Attributed Reports
Reputation: Suspicious (1/100)
Reputation score reflects how likely the entity is malicious, based on Defender TI's proprietary data, detection rules, and observed behavior patterns. Learn more
No reputation data available
No threat intelligence rules were found for this entity


Microsoft Defender | Default Directory
Search
Incidents > Solorigate Network Beacon > 17.81.146.1
17.81.146.1
Add indicator
Go hunt
Overview
Incidents and alerts
Observed in organization
Sentinel events
Threat Intelligence Insights
Customize Sentinel activities
Sentinel timeline
Search
Timeline content : All
Tactics : All
Add filter
No notable activity to display
You can explore more about this entity in Log analytics
Insight
IP address remote connections with TI match
2/13/2026, 1:15:05 AM - 2/15/2026, 1:15:05 AM
No results
IP address remote connections
2/13/2026, 1:15:05 AM - 2/15/2026, 1:15:05 AM
No results
This IP has a TI match
2/13/2026, 1:15:05 AM - 2/15/2026, 1:15:05 AM
No results
Watchlist Insights (Preview)
2/13/2026, 1:15:05 PM - 2/14/2026, 1:15:05 PM
No results

7. Document Analyst Actions

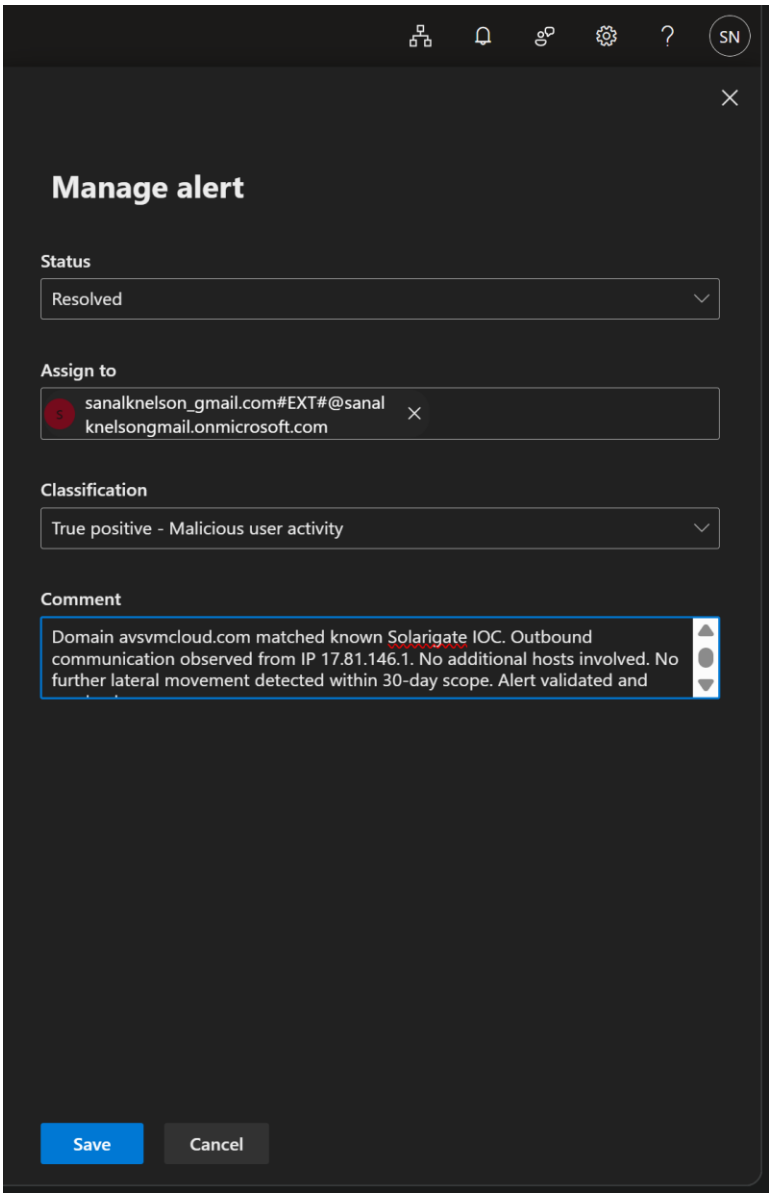
Finalize Analyst Action (Resolve the Alert Properly)

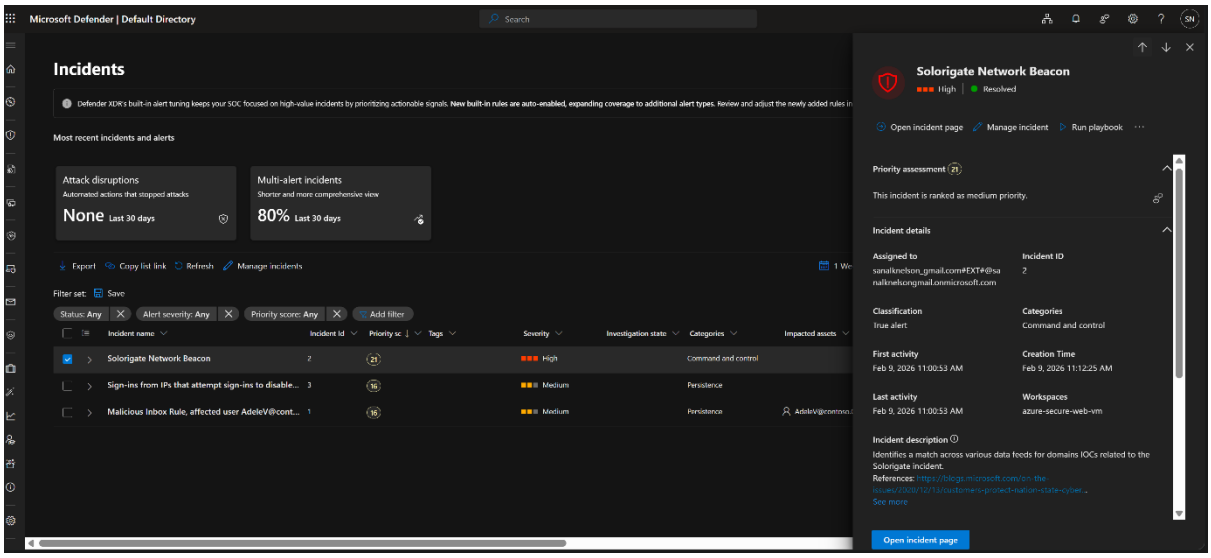
After completing the investigation and validating the evidence, we must formally close the alert from the same" Manage Alert" menu.

We should:

- Change the **Status** to **Resolved**
- Set **Classification** to **True positive – Malicious user activity**
- Add a detailed investigation comment *(In the screenshot)* explaining findings

This step confirms that investigation is complete and properly documented.





(After the resolution if we go back to "Incidents" page in Defender, if we click the alert it will show as resolved, Assigned to, Classification etc)

Outcome

By the end of this phase, we have:

- Identified and opened the **Solorigate Network Beacon** incident
- Taken ownership of the incident and moved it to **Active**
- Understood that multiple alerts were grouped under one incident
- Opened the detailed alert page and used **Manage alert** correctly
- Reviewed the **analytics rule** that triggered the detection
- Investigated key entities (domain avsvmcloud.com and IP 17.81.146.1)
- Used the Incident Graph to understand entity relationships
- Verified detection logic against raw evidence
- Expanded analysis scope to ensure no broader compromise
- Properly classified the alert as **True positive – Malicious user activity**
- Changed status to **Resolved**
- Documented investigation findings in analyst comments

At this stage, we have demonstrated:

- Real SOC triage workflow
- Alert-to-incident handling discipline
- Entity-based investigation using Defender XDR
- Proper closure and documentation standards