

# 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 (Solarigate)

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

The screenshot shows the Microsoft Defender Portal's 'Incidents' page. At the top, there are two cards: 'Attack disruptions' (None last 30 days) and 'Multi-alert incidents' (80% last 30 days). Below these are buttons for 'Export', 'Copy list link', and 'Refresh'. A filter bar includes 'Status: Any', 'Alert severity: Any', 'Priority score: Any', and an 'Add filter' button. The main area displays a table of incidents with columns for Incident name, Incident Id, Priority score, Tags, Severity, Investigation state, Categories, and Impacted assets. Three specific incidents are listed:

Incident name	Incident Id	Priority score	Tags	Severity	Investigation state	Categories	Impacted assets
Solarigate Network Beacon	2	(21)		High		Command and control	
Sign-ins from IPs that attempt sign-ins to disable...	3	(16)		Medium		Persistence	
Malicious Inbox Rule, affected user AdeleV@contoso...	1	(16)		Medium		Persistence	AdeleV@contoso.OnMicrosoft.com

The screenshot shows the Microsoft Defender interface. On the left, there's a sidebar with various icons. The main area has a title bar 'Microsoft Defender | Default Directory' and a search bar. Below the search bar is a 'Detection & Categories' section showing 'Active alerts' (5/5) and 'Categories' (1). It lists the 'First activity' (Feb 9, 2026 11:00:53 AM) and 'Last activity' (Feb 9, 2026 11:00:53 AM). A 'Creation time' section shows 'Feb 9, 2026 11:12:25 AM'. The 'Alerts' section lists five entries for 'Soligate Network Beacon' from Feb 9, 2026, at 11:00 AM, all marked as 'New'. Each alert entry includes a red circular icon with a dot, the date and time, the alert name, and a 'More' button. To the right of the alerts is an 'Incident graph' with nodes for 'Communication' and 'Association'. One node is labeled 'Soligate Network Beacon'. Below the graph is a section titled 'What happened' which includes an 'ANALYTICS RULE' section with a 'Rule name' of 'Soligate Network Beacon' and a 'View rule in Sentinel' link. There's also an 'Analytics rule details' section with a 'Rule description' that links to external resources. The right side of the screen displays the 'Soligate Network Beacon' incident details. It shows an 'INVESTIGATE' button, a status bar with 'High' (red), 'Unknown' (yellow), and 'New' (green), and an 'INSIGHT' section with the text 'Quickly classify this alert' and a 'Classify alert' button. Under 'Alert state', it shows 'Classification: Not Set', 'Assigned to: sanalnelson@gmail.com#EXT#@sanalne...longmail.onmicrosoft.com', and a 'Set Classification' button. The 'Alert details' section shows 'Alert ID: on0047517-ceeb-4-21-b137-6d3e3d71a2', 'Category: Command and control', and 'MITRE ATT&CK Techniques: Scheduled detection'. Detection source is listed as 'Microsoft Sentinel'.

## 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

    ? 

X

## Manage incident

Incident name

Severity

Incident tags

    ? 

Incident updated successfully 1:24 PM

**Priority assessment 21**

This incident is ranked as medium priority.

**Incident details**

<b>Assigned to</b>	<b>Incident ID</b>
sanalknelson_gmail.com#EXT#@sanalknelson@gmail.onmicrosoft.com	2
<b>Classification</b>	<b>Categories</b>
Not set	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.

The screenshot shows the Microsoft Defender for Cloud interface for an incident titled "ID 2: Solorigate Network Beacon".

**Incident Details:**

- Severity: High
- Type: Active
- Source: sanalnelson.gmail.com#EXT#@sanalnelson@gmail.onmicrosoft.com
- Status: Unclassified
- Last update time: Feb 14, 2026 1:24 PM

**Attack story:** Alerts (5), Activities (6), Assets (0), Investigations (0), Evidence and Response (2), Summary.

**Detection & Categories:**

- Active alerts: 5/5
- Categories: 1
- First activity: Feb 9, 2026 11:00:53 AM
- Last activity: Feb 9, 2026 11:00:53 AM
- Creation time: Feb 9, 2026 11:12:25 AM

**Alerts:**

- Feb 9, 2026 11:00 AM • New Solorigate Network Beacon
- Feb 9, 2026 11:00 AM • New Solorigate Network Beacon
- Feb 9, 2026 11:00 AM • New Solorigate Network Beacon
- Feb 9, 2026 11:00 AM • New Solorigate Network Beacon

**Priority assessment:** This incident is ranked as medium priority.

**Incident details:**

- Assigned to: sanalnelson.gmail.com#EXT#@sanalnelson@gmail.onmicrosoft.com
- Incident ID: 2
- Classification: Not set
- Categories: Command and control
- First activity: Feb 9, 2026 11:00:53 AM
- Last activity: Feb 9, 2026 11:00:53 AM
- Creation Time: Feb 9, 2026 11:12:25 AM
- Workspaces: azure-secure-web-vm

**Incident description:** (o) 17.81.146.1

Microsoft Defender | Default Directory

Incidents > Solorigate Network Beacon

## ID 2: Solorigate Network Beacon

High | Active | Unassigned | Unclassified | Last update time: Feb 9, 2026 11:32 AM

(1) 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 inaccuracy

Filter set:

Status: New, In progress

Tags	Severity	Investigation state	Status	Category	Impacted assets	Correlation reason
	High	New	New	Command and control	Same Analytic Rule...	S
	High	New	New	Command and control	Same Analytic Rule...	S
	High	New	New	Command and control	Same Analytic Rule...	S
	High	New	New	Command and control	Same Analytic Rule...	S
	High	New	New	Command and control	Same Analytic Rule...	S

Microsoft Defender | Default Directory

Incidents > Solorigate Network Beacon

## ID 2: Solorigate Network Beacon

High | Active | sanalknelson@gmail.com#EXT#@sanalknelsongmail.onmicrosoft.com | Unclassified | Last update time: Feb 14, 2026 1:24 PM

(1) 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

Filter set:

Origin: This incident

Activity started	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

Incidents > Solorigate Network Beacon

## ID 2: Solorigate Network Beacon

High | Active | sanaliknelson@gmail.com#EXT#@sanaliknelson@gmail.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 (5) | **Assets (0)** | Investigations (0) | Evidence and Response (2) | Summary

All assets (0)	Devices (0)
<input type="checkbox"/> Users (0)	<input type="checkbox"/> Export
<input type="checkbox"/> Mailboxes (0)	Device name ▾
<input type="checkbox"/> Apps (0)	Domain ▾
<input type="checkbox"/> Cloud Resources (0)	Device ID ▾
	Risk level ↑ ▾
	Exposure level ↑ ▾
	OS platf

Incidents > Solorigate Network Beacon > 17.81.14.14

Part of incident: Solorigate Network Beacon [View incident](#)

### Analytics rule wizard - Edit existing Scheduled rule

Solorigate Network Beacon

What happened

Identifies a match across various data feeds for domain incident.  
References: <https://blogs.microsoft.com/on-the-issue/nation-state-cyberattacks/>, <https://www.fireeye.com/blog/threat-research/2020/solarwinds-supply-chain-compromises-with-stunburst>

**ANALYTICS RULE**

Analytics rule details

Rule name: Solorigate Network Beacon [View rule in Sentinel](#)

Rule description: Identifies a match across various data feeds for domain protect-nation-state-cyberattacks/. <https://www.fireeye.com/blog/threat-research/2020/solarwinds-supply-chain-compromises-with-stunburst>

Related events

Query results

Define the logic for your new analytics rule.

**Rule query**

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
let domains = dynamic(["incomeupdate.com", "zupertech.com", "databasegalore.com", "panhardware.com", "avsvmcloud.com"]);
union isfuzzytrue(
    ComputerName|ComputerUser|ComputerIP|Message|RequestURL|DestinationHostName|Destinat...
).parse(DNSName) *
where DNSName in- (domains) or DestinationHostName has_any (domains) or RequestURL has_any(domains)
| extend AccountCustomEntity = SourceUserID, HostCustomEntity = DeviceName, TCPCustomEntity = SourceIP
```

[View query results >](#)

**Alert enhancement**

**Entity mapping**

Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

Account

FullName | AccountCustomEntity

Add identifier

< Previous | Next : Incident settings > | Cancel

(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.

The screenshot shows the Microsoft Defender Evidence and Response section for incident ID 2: Solorigate Network Beacon. It displays two DNS entries:

First seen	Entity	Entity type	Verdict	Remediation status
Feb 9, 2026 11:00 AM	avsvmcloud.com	DNS	Suspicious	
Feb 9, 2026 11:00 AM	17.81.146.1	IP Address	Suspicious	

The screenshot shows the Microsoft Defender Evidence and Response section for incident ID 2: Solorigate Network Beacon. It displays the DNS details for 'avsvmcloud.com':

First seen	Entity	Entity type	Verdict	Remediation status
Feb 9, 2026 11:00 AM	avsvmcloud.com	DNS	Suspicious	
Feb 9, 2026 11:00 AM	17.81.146.1	IP Address	Suspicious	

## 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.

The screenshot shows the Microsoft Defender Advanced hunting interface. At the top, there is a search bar and various navigation icons. Below the search bar, the title "Advanced hunting" is displayed. A code editor window contains a PowerShell-like search query:

```
1 let ip = "17.81.146.1";
2 search in (IdentityLogonEvents,IdentityQueryEvents,IdentityDirectoryEvents,EmailEvents,UrlClickEvents,DeviceNetworkEvents,DeviceFileEvents,Di
3 Timestamp between (ago(1d) .. now())
4 and (/ / Events initiated by this IP
5 LocalIP == ip
6 or FileOriginIP == ip
7 or RequestSourceIP == ip
8 or SenderIPv4 == ip
9 or SenderIPv6 == ip
10 or IPAddress == ip
11 // Events affecting this IP
12 or RemoteIP == ip
13 or DestinationIPAddress == ip
14 )
15 | take 100
```

Below the query, there are several filtering options and a search bar. The bottom right corner features a button labeled "Open in advanced hunting".

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

## 5. Pivot to Raw Logs

The screenshot shows the Microsoft Defender Detection & Categories interface. On the left, a sidebar displays "Active alerts" (5/5), "First activity" (Feb 9, 2026 11:00:53 AM), and "Creation time" (Feb 9, 2026 11:12:25 AM). The main pane shows a list of alerts under the "Alerts" section, all of which are categorized as "Solorigate Network Beacon". Each alert entry includes a timestamp (Feb 9, 2026 11:00 AM), a status (Resolved or New), and a description. A red arrow points from the bottom of the alert list towards the bottom of the screen. The bottom of the screen shows a "Query results" table with columns: TimeGenerated, TenantId, DeviceVendor, DeviceProduct, DeviceVersion, DeviceEventClassId, and Activity. The table shows one item with a timestamp of Feb 9, 2026 11:00:53.

The screenshot shows a Microsoft Defender log entry for a DNS lookup event. The log table has columns: TimeGenerated, TenantId, DeviceVendor, DeviceProduct, DeviceVersion, DeviceEventClassID, and Activity. A dropdown menu is open for the first row, showing the date Feb 9, 2026 11:00:53. The log details are as follows:

Field	Value
TimeGenerated	Feb 9, 2026 11:00:53 AM
EventCount	1
EventType_string	lookup
Type	Cisco_Umbrella_dns_CL
DNSName	avsvmcloud.com
IPCustomEntity	17.81.146.1
QueryType_int	1
EventStartTime	Sep 13, 2019 1:30:00 AM
EventProduct	Umbrella
EventVendor	Cisco Systems
EventSchemaVersion	0.1.1
Dvc	Unknown
EventResult	Success
EventResultDetails	NOERROR
SrcIpAddr	17.81.146.1
EventSubType	response
DnsQuery	avsvmcloud.com
SrcNatIpAddr	15.230.137.45
DvcAction	Allowed

**Inspect record**

- SrcNatIpAddr: 15.230.137.45
- DvcAction: Allowed
- EventEndTime: 2019-09-12T20:00:00.625Z
- DnsQueryType: 1
- DnsQueryTypeName: A
- PolicyIdentity: HOSTNAME
- DnsResponseCodeName: NOERROR
- Domain: avsvmcloud.com
- IpAddr: 17.81.146.1
- Query: avsvmcloud.com
- QueryTypeName: A

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 Solarigate 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 Solarigate).
- 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.

**Detection & Categories**

Active alerts	Categories
5/5	1

**First activity**      **Last activity**  
Feb 9, 2026 11:00:53 AM      Feb 9, 2026 11:00:53 AM

**Creation time**  
Feb 9, 2026 11:12:25 AM

**Alerts**

- Feb 9, 2026 11:00 AM • New **Solorigate Network Beacon**
  - Category: Command and control
  - MITRE ATT&CK Techniques: Not Set
  - Detection source: Scheduled detection
  - Service source: Microsoft Sentinel
- Feb 9, 2026 11:00 AM • New **Solorigate Network Beacon**
- Feb 9, 2026 11:00 AM • New **Solorigate Network Beacon**

**Incident graph**    Layout    Group similar nodes

**17.81.146.1**

**IP details**

- Pin related alerts
- Hide related alerts
- Go hunt
- Actions

**What happened**

Identifies a match across various data feeds for domains IOCs related to the Solorigate incident.

References: <https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/>, <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html?1>

**ANALYTICS RULE**

**Incident graph**    Layout    Group similar nodes

**17.81.146.1**

**What happened**

Identifies a match across various data feeds for domains IOCs related to the Solorigate Incident.

References: <https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/>, <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html?1>

**Analytics rule details**

**Rule name:** Solorigate Network Beacon  
[View rule in Sentinel](#)

**Rule description:** Identifies a match across various data feeds for domains IOCs related to the Solorigate incident. References: <https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/>, <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html?1>

**Postal code:** 511700

**Detection:** 5 active alerts in 1 incidents

**IP observed in organization devices:**

**Entity Reputation:** Suspicious (1/100)

**Log activity:**

First seen	Last seen
2/9/2026, 11:12:14 AM	2/9/2026, 11:32:12 AM

**Data Sources:** SecurityAlert

**Logged hosts:**

Host name	First seen	Last seen
Hosts were not found		

**Open IP address page**

Incidents > Solorigate Network Beacon > 17.81.146.1

# 17.81.146.1

(o)

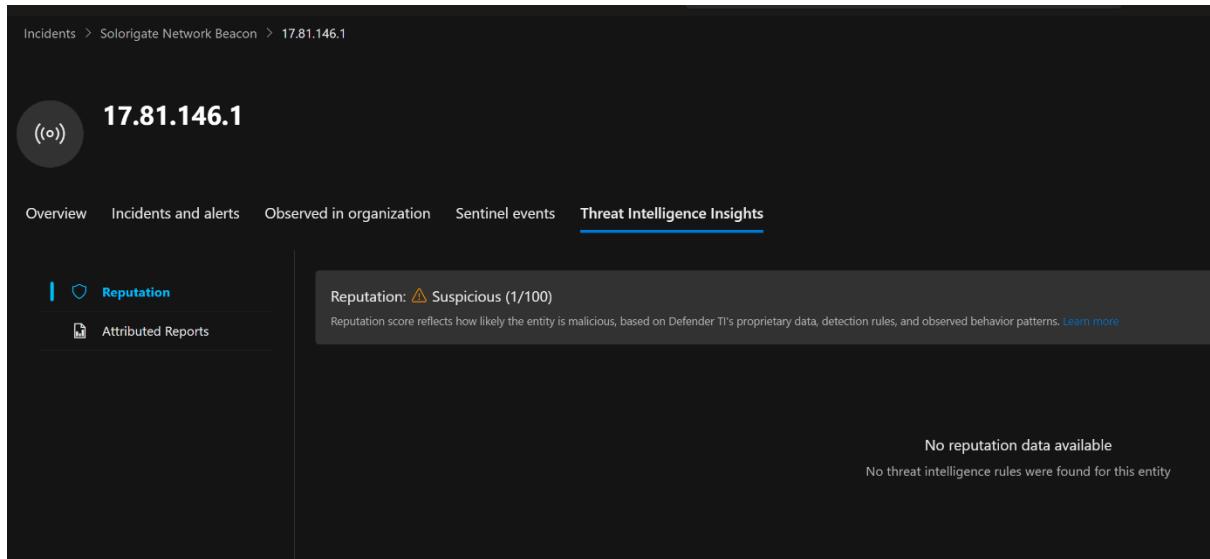
Overview Incidents and alerts Observed in organization Sentinel events Threat Intelligence Insights

| 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

Incidents > Solorigate Network Beacon > 17.81.146.1

# 17.81.146.1

(o)

+ 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

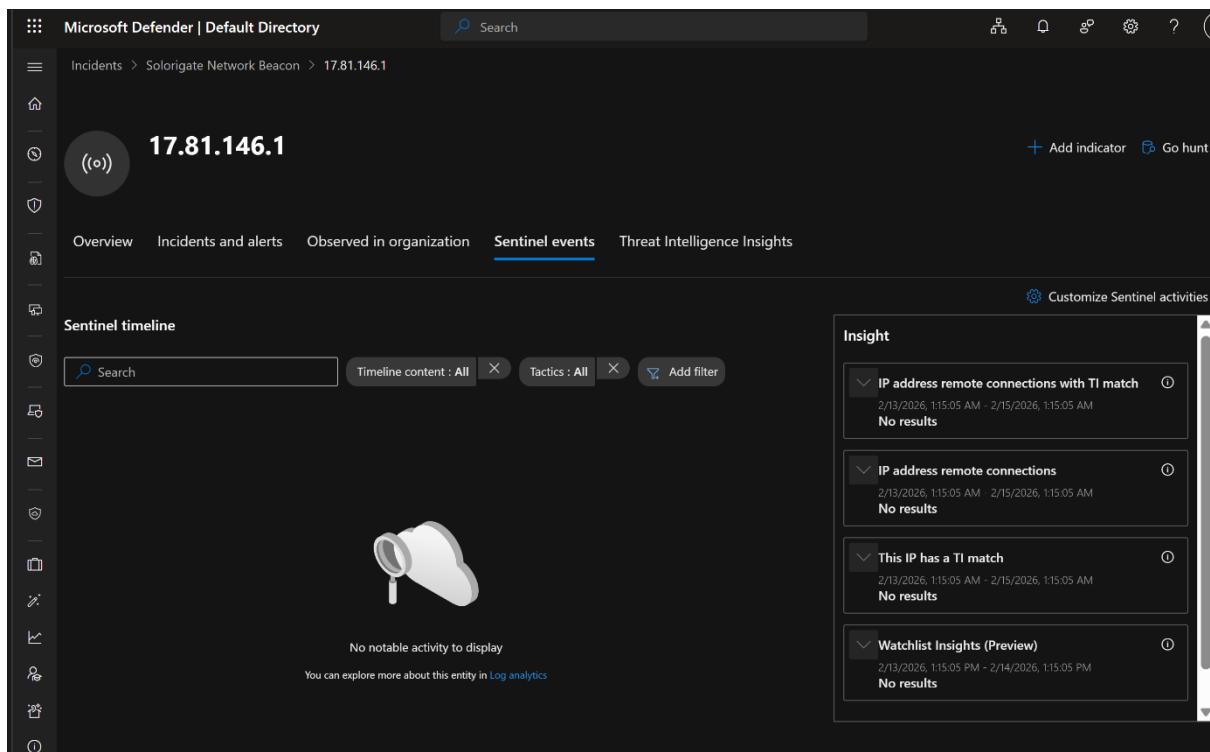
No notable activity to display

You can explore more about this entity in [Log analytics](#)

Cloud icon with magnifying glass

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

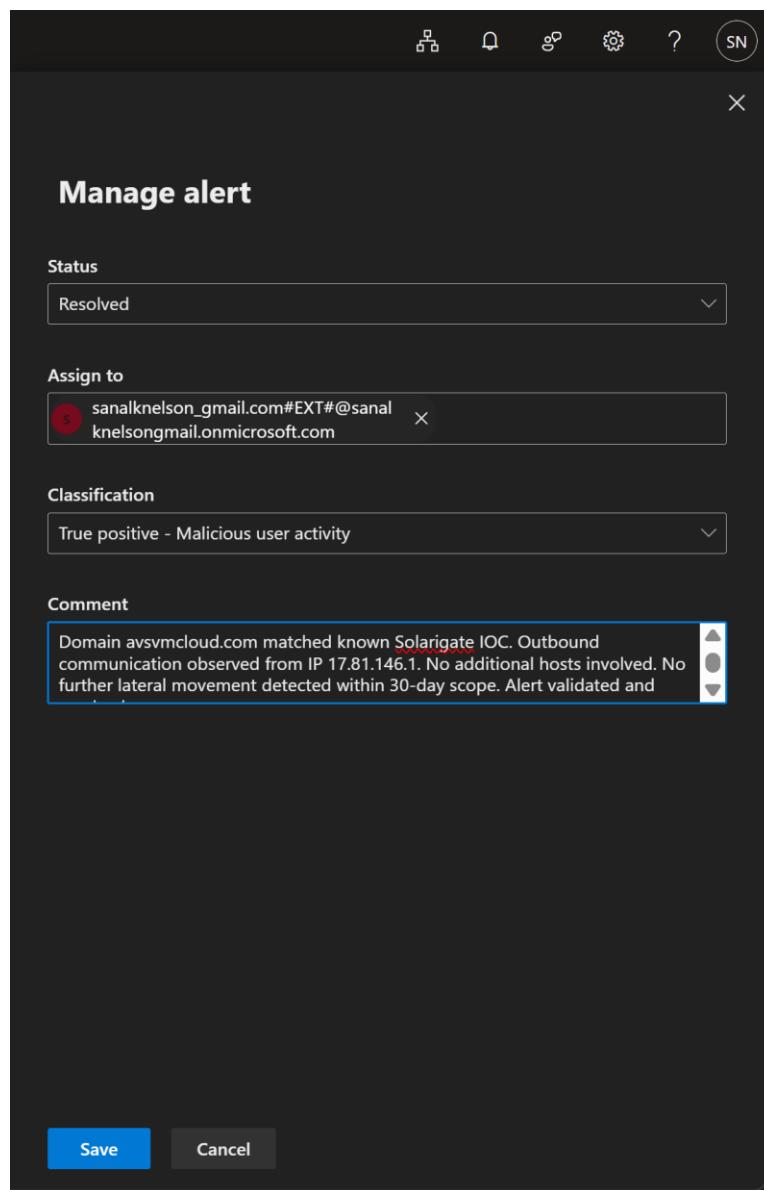
### Finalize Analyst Action (Resolve the Alert Properly)

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.



The screenshot shows the Microsoft Defender XDR interface. On the left, the 'Incidents' page displays a list of alerts. One alert, 'Solorigate Network Beacon', is selected and shown in a detailed view on the right. The detailed view includes sections for 'Priority assessment' (medium priority), 'Incident details' (assigned to saralinekong\_gmail.com#EXT#@sa, incident ID 2), 'Classification' (true alert), 'Categories' (Command and control), 'First activity' (Feb 9, 2026 11:00:53 AM), 'Creation Time' (Feb 9, 2026 11:12:25 AM), 'Last activity' (Feb 9, 2026 11:00:53 AM), 'Workspaces' (azuresecure-web-vm), and 'Incident description' (Identifies a match across various data feeds for domains IOCs related to the Solorigate incident). There are also 'References' and 'See more' links.

*(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