Lab Manual- Incident Management Azure Sentinel

Prepared for:

Date: 18th Nov 2021

Prepared by:

Document Name: Lab Manual

Document Number AZLabn993

Contributor:

Contents

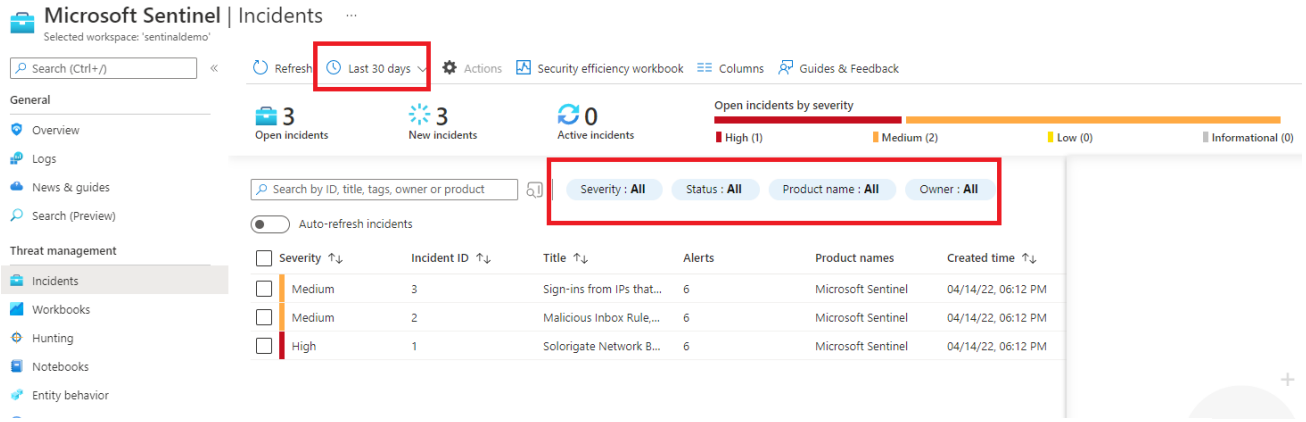
1. Introduction

Microsoft Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Defender for Cloud Apps, security alerts from Microsoft Defender for Cloud, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format (CEF), Syslog or REST-API to connect your data sources with Microsoft Sentinel

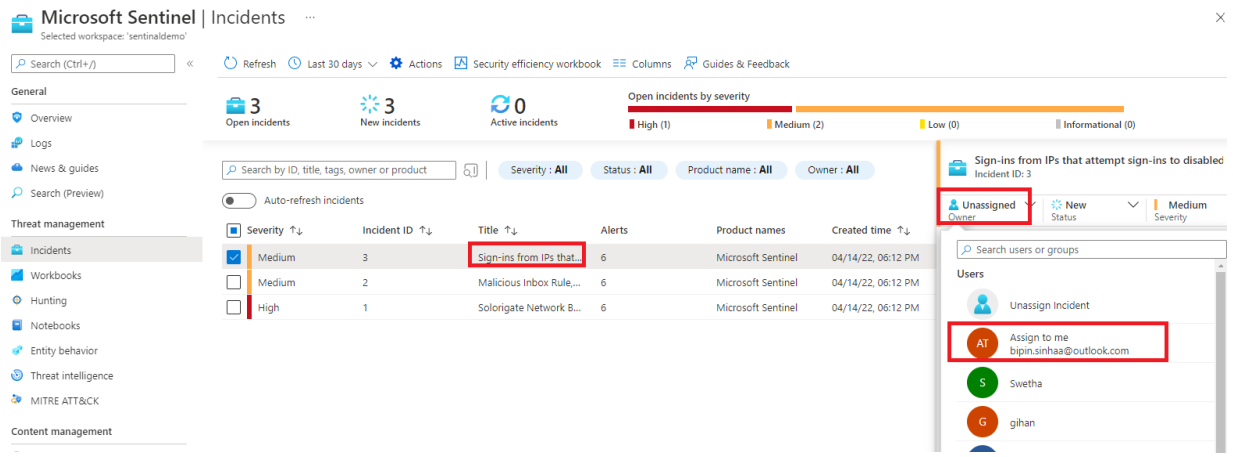
In this Lab , guides you through the SOC Analyst experience using Microsoft Sentinel's incident management capabilities.

2. Review Microsoft Sentinel incident tools and capabilities

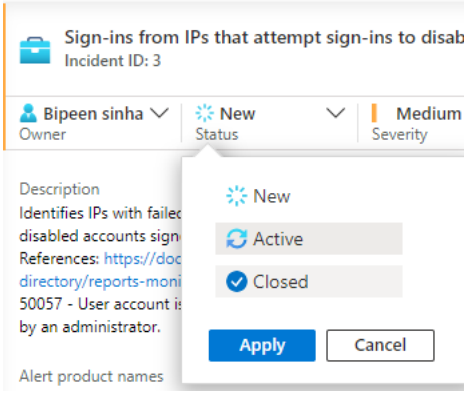
1. In the left navigation menu click on ***Incidents*** to open the incidents page. This page will show by default all the open incidents in the last **24hr**.
2. When we want to change the **time window**, present only incident from specific severity or to see also closed incident, we can use the filters bar:



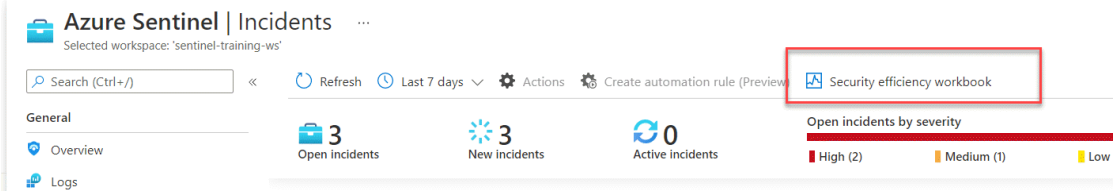
3. On the incident page select the ***Sign-ins from IPs that attempt sign-ins to disabled accounts*** incident. In the right pane you can see the incident preview with the high level information about the incident.
4. As you are the **SME SOC analyst** that deal and **investigate tickets**, you need to take ownership on this incident. On the right pane, change the unassigned to ***Assign to me***



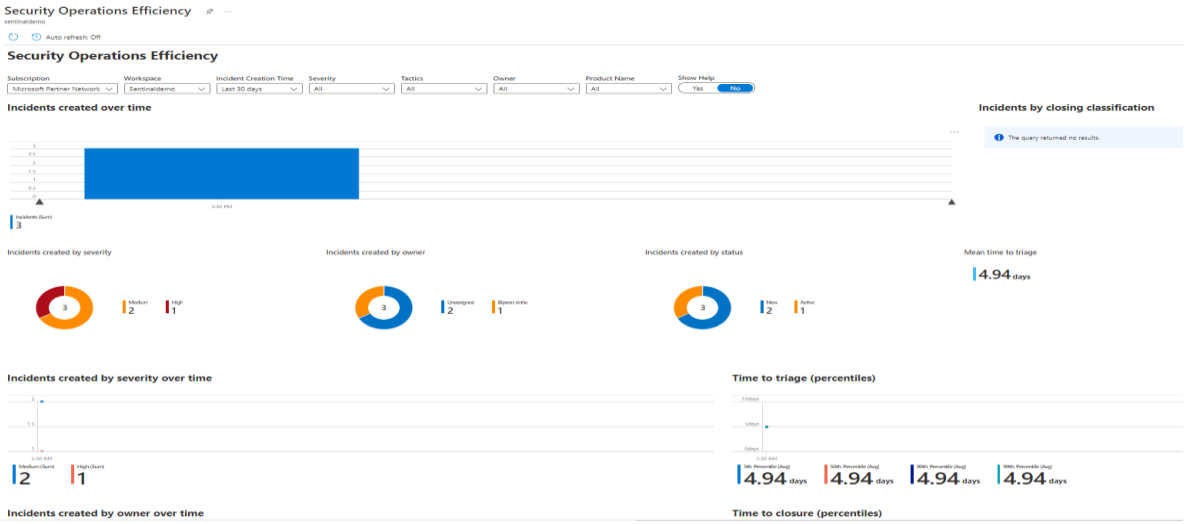
5. Also change the status from ***New*** to ***Active***.



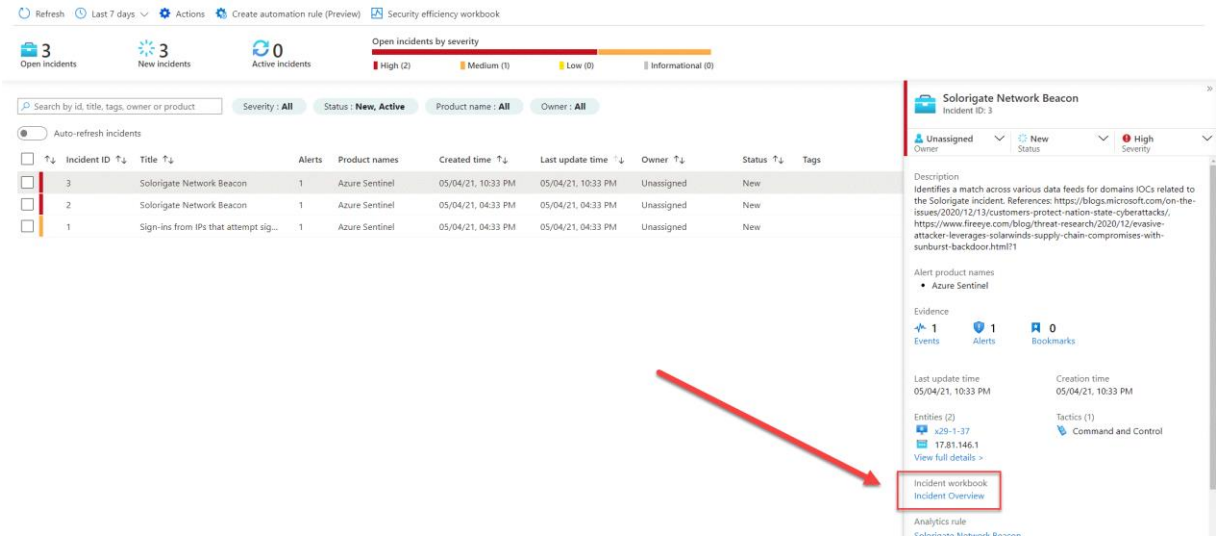
6. Another way to consume incidents and also get high level view on the general SOC health is through the ***Security efficiency workbook***.



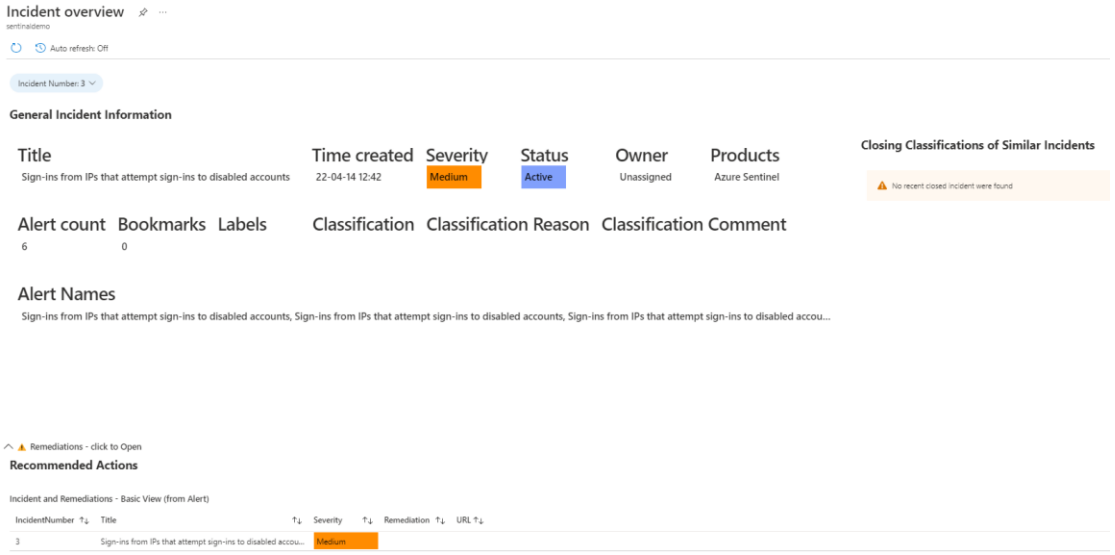
7. Review the dashboard.



8. Through the incident itself, that will open the same workbook on a different tab, and present the information and lifecycle for the given incident.



9. Review the dashboard.



3. Exercise 2: Handling Incident "Sign-ins from IPs that attempt sign-ins to disabled accounts"

1. Open Azure Sentinel incident page.

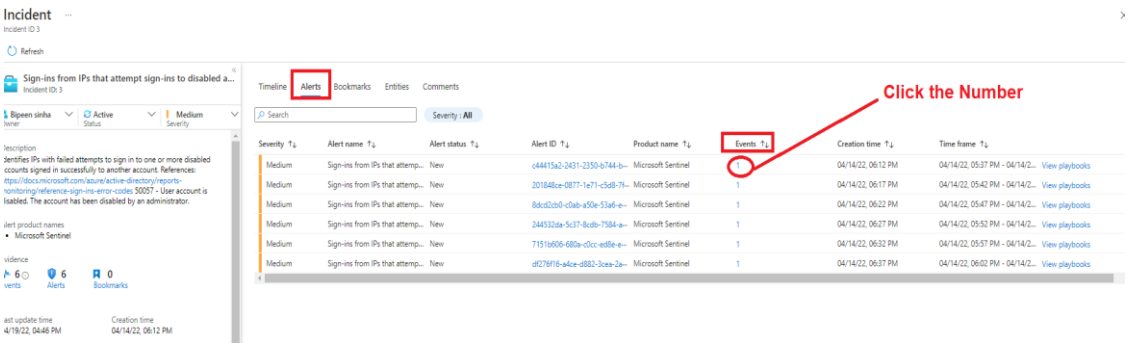
2. Locate the incident **"Sign-ins from IPs that attempt sign-ins to disabled accounts"**

3. Press on the incident and look on the right pane for the incident preview, please notice that in this pane we are surfacing the incident entities that belong to this incident.

4. Take ownership on the incident and change its status to **Active**

5. Navigate to incident full details by pressing **View full details** and execute playbook to bring Geo IP data (user will notice tags being added).

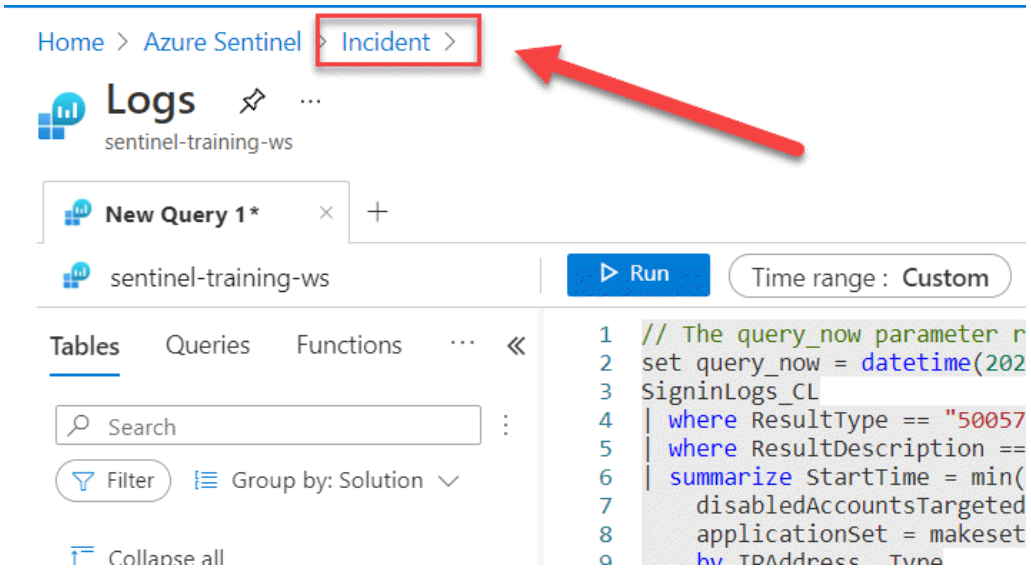
6. Navigate to the **Alerts** tab and press the number of **Events**. This action will redirect you to Raw logs that will present the alert evidence to support the investigation



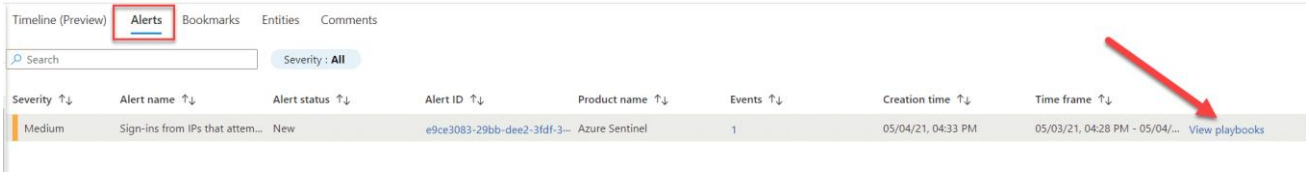
7. In raw log search, expend the received event and review the column and data we received, this properties will help us to decide if this incident is correlated to other events.

8. To get more context for this IP, we want to add GEO IP enrichment. In a real life SOC this operation will run automatically, but for this lab we want you to run it manually.

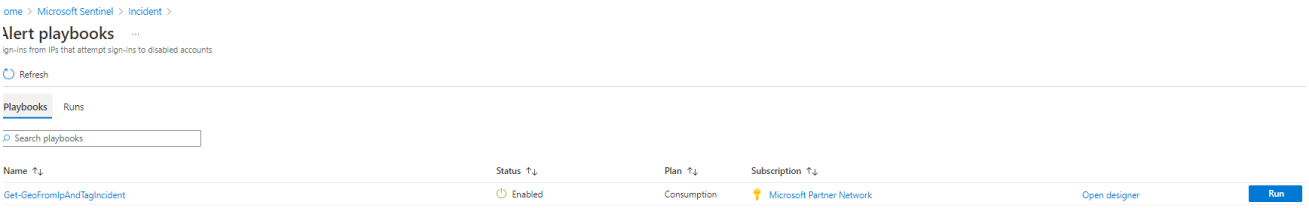
- Navigate back to the incident full page to the alert tab and scroll to the right



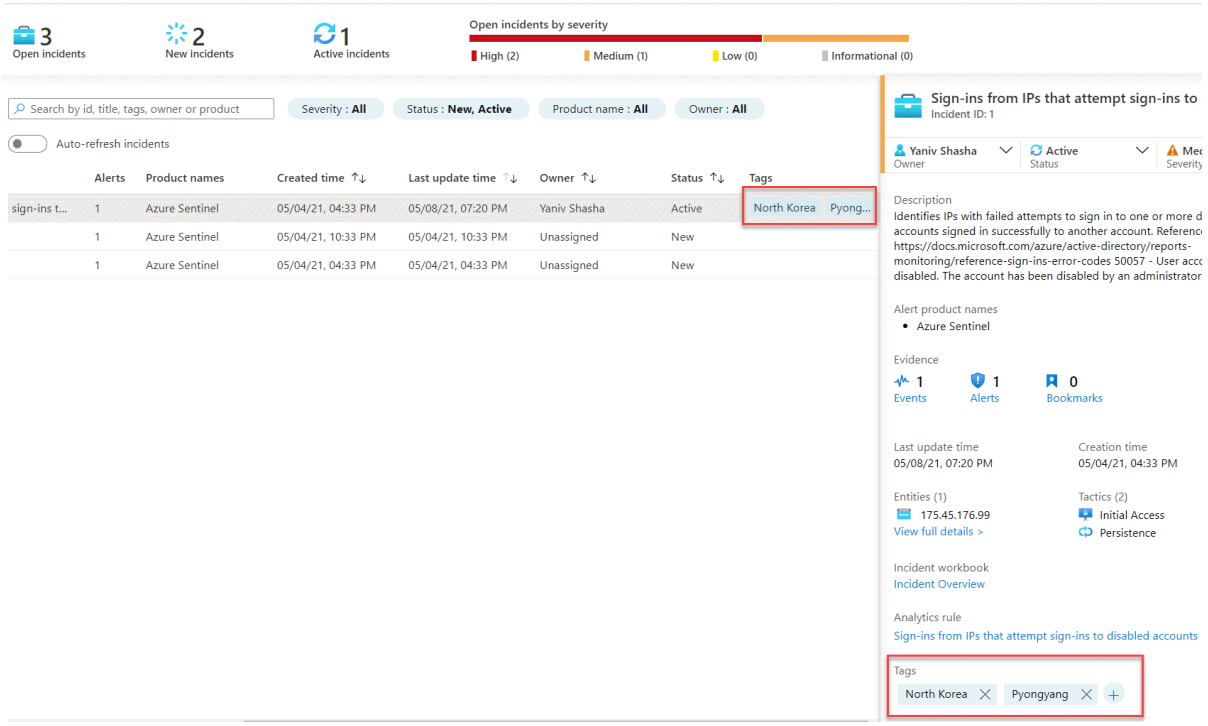
9. To view the relevant automation that will assist us with the enrichment operation, Press **view playbook**



9. Locate the playbook **Get-GeoFromIpAndTagIncident** and press **Run**. If the playbook is configured correctly, it should finish in a couple of seconds.

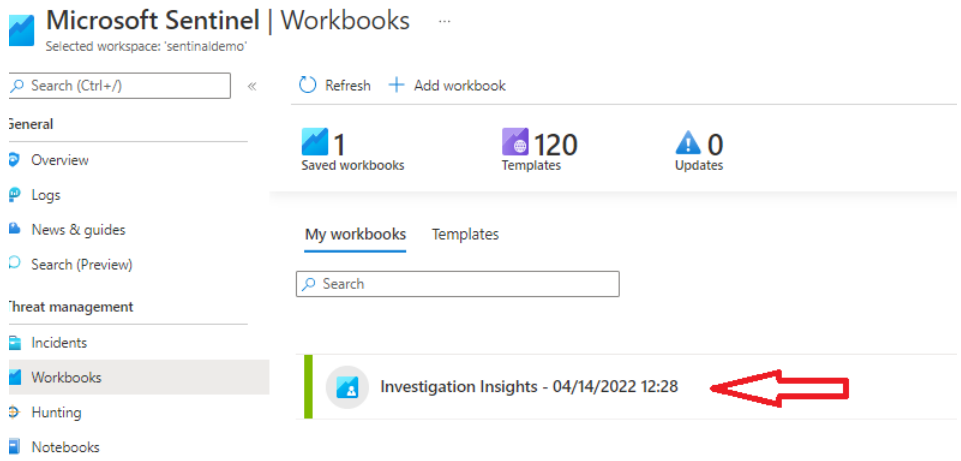


10. Navigate back to the main incident page and notice to new tags that added to the incident.



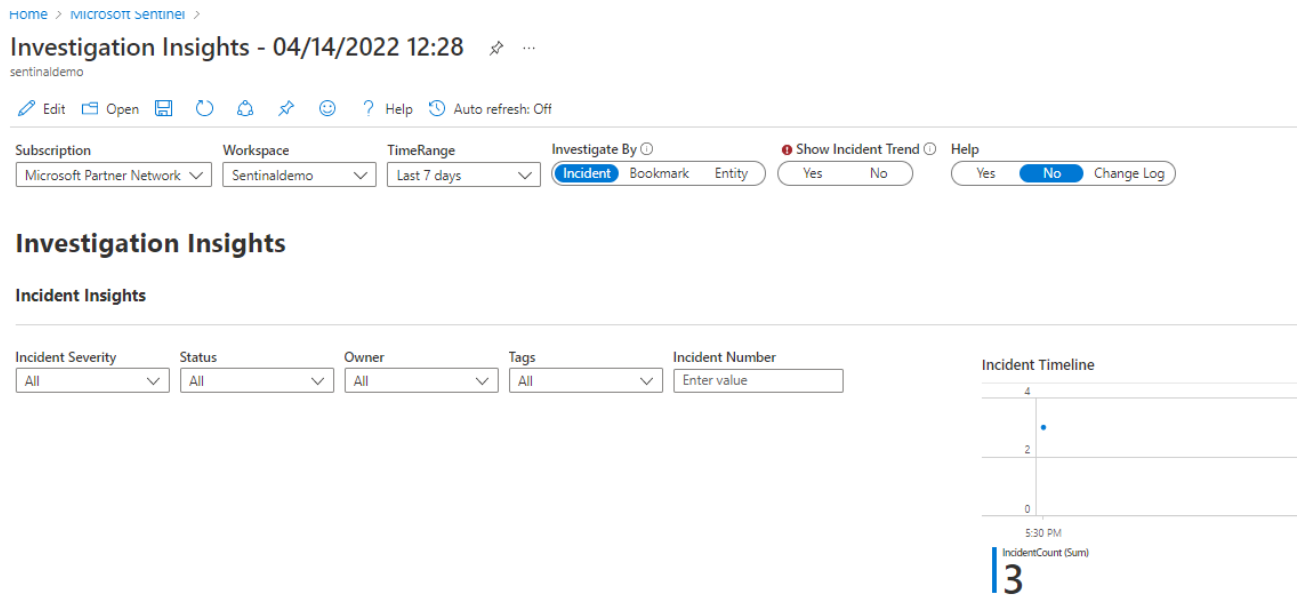
11. As this enrichment information increases your concern, you want to check other traces of this IP in your network. For this investigation you want to use the investigation workbook.

12. in the left navigation press **Workbooks** and select **My Workbooks**



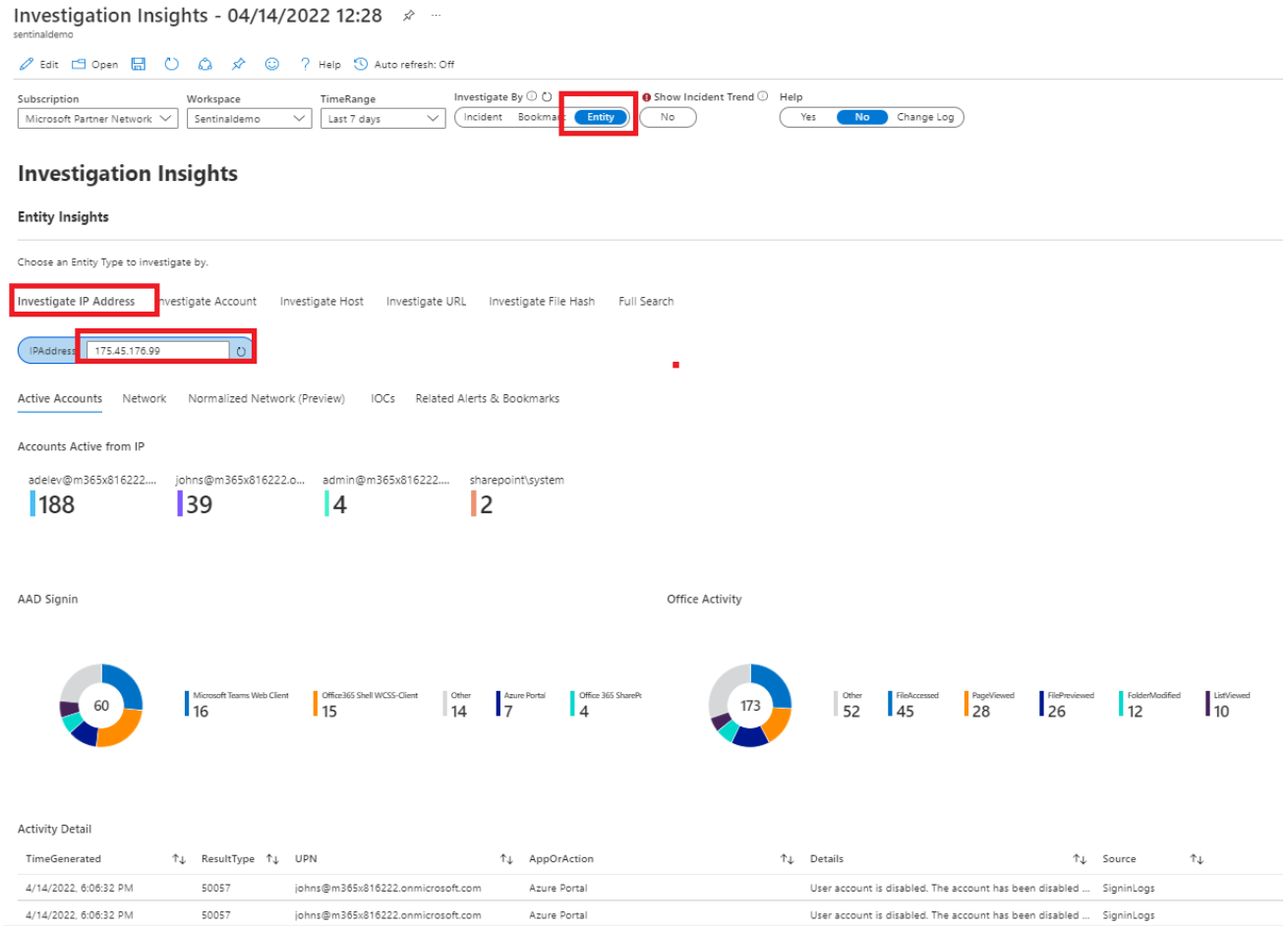
13. To open the **Investigation Insights - sentinel-training-ws** saved Workbook, in the right page press **View saved workbook**

14. Validate that in the properties selector, your workspace is set on **sentineldemo** and the subscription is the subscription that hosts your Microsoft Sentinel Lab.



15. As the subject of the investigation is the suspicious IP from North Korea. we want to see all the activity done by this IP so in the properties selector, switch on the **investigate by** to Entity.

16. in the **Investigate IP Address** Tab, add the suspicious IP.

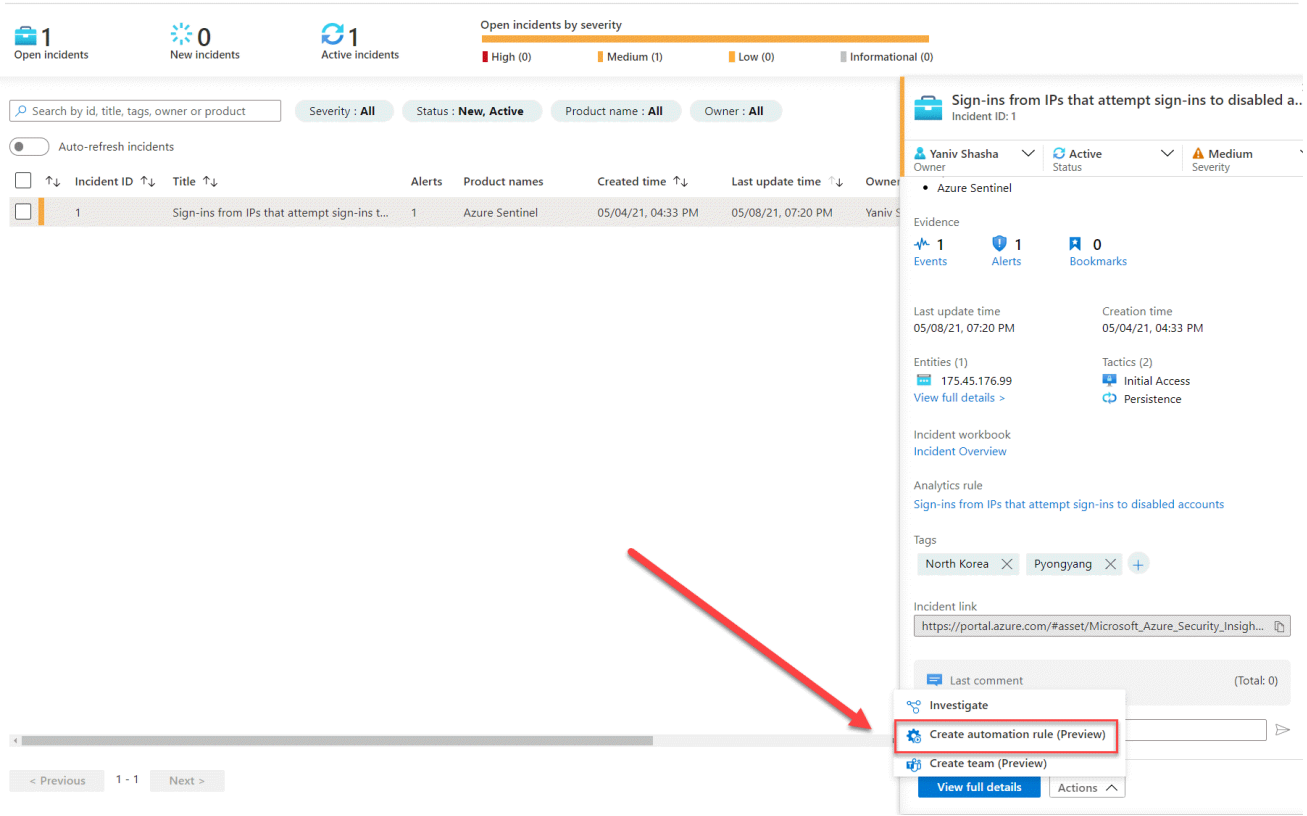


17. Under the activity Detail we see many successful logins from this IP with the user Adele, and also some failed logins to disabled account from last day/hours

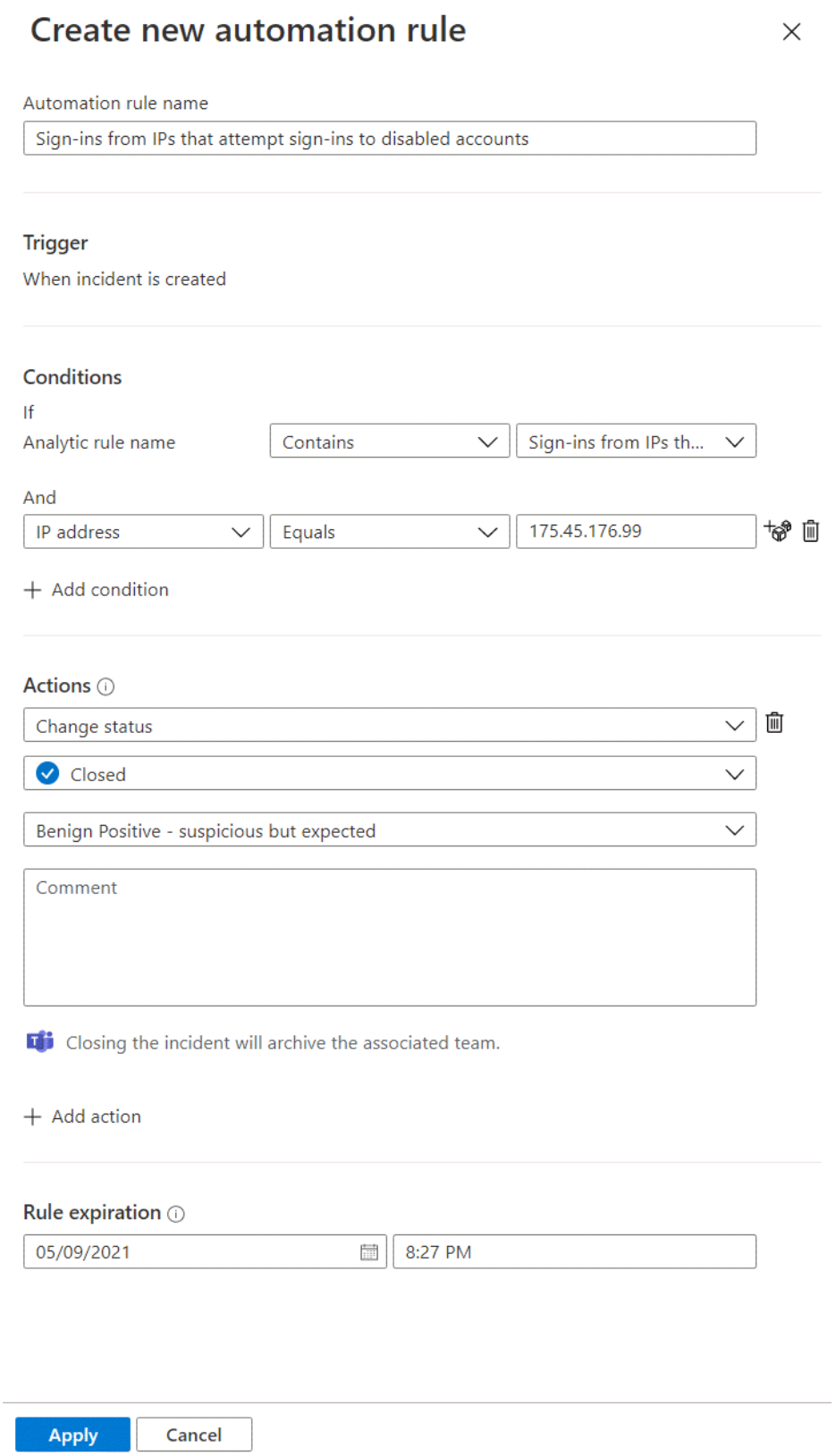
18. We copy the User adelev@m365x816222.onmicrosoft.com and validate it in our internal HR system, from the information we collected its seems that Adele is part of the security Red team, and this suspicious is part of the exercise.

19. As the red team exercise discovered by us, the SOC manager ask us to add this IP to the whitelisting IP's, that we will not trigger incident on it any more.

20. On the main incident page, select the relevant incident and press **Actions - > Create automation Rule**



21. In the new screen, we will see all the incident identifiers (the IP, and the specific Analytics rule), as the Red Team exercise will finish in 48 hr., adapt the rule expiration till the end of the drill, and press **Apply**.



22. As this incident consider as benign, we go back to the main incident page, and close the incident with the right classification.

Sign-ins from IPs that attempt sign-ins to disabled a...
Incident ID: 1

Yaniv Shasha
Owner

Active
Status

Medium
Severity

New

Active

Closed

Benign Positive - suspicious but expected

Red Team exercise user adelev@m365x816222.onmicrosoft.com is part of the team, confirm

Apply

Cancel

or more disabled
. References:
reports-
- User account is
ministrator.

3 PM

Entities (1)

175.45.176.99

View full details >

Tactics (2)

Initial Access

Persistence

Incident workbook

Incident Overview

Analytics rule

Sign-ins from IPs that attempt sign-ins to disabled accounts

Tags

North Korea

Pyongyang

Incident link

View full details

Investigate

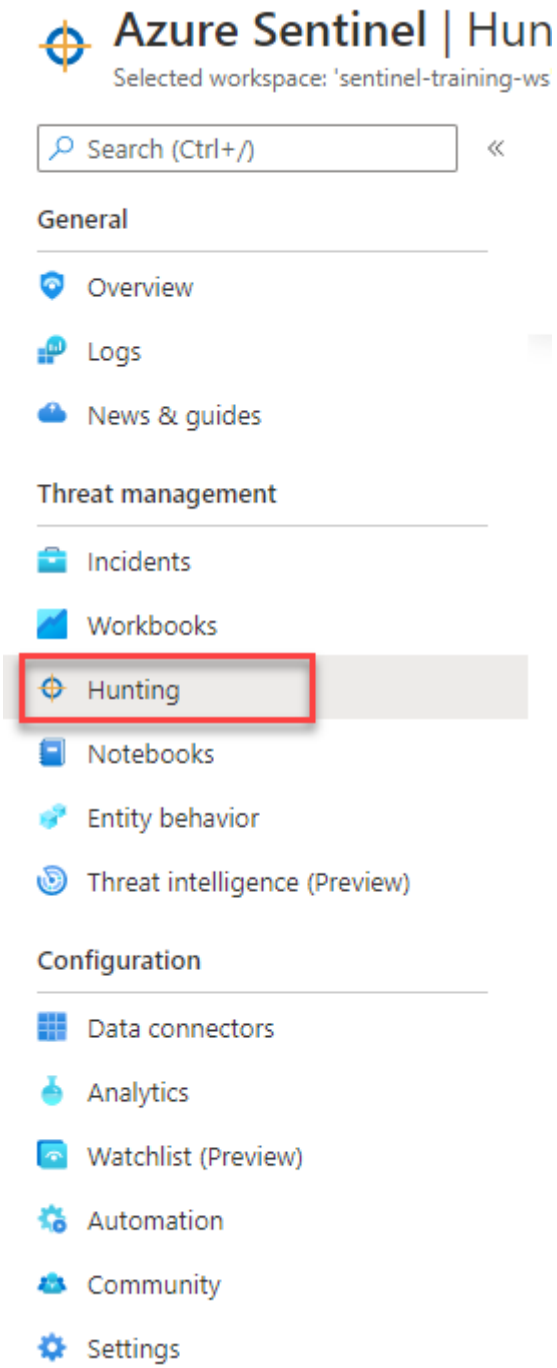
4. Exercise 4: Hunting for more evidence

1. As a next step, you would like to identify the hosts that might have been compromised. As part of your research, you find the following [guidance from Microsoft](https://techcommunity.microsoft.com/t5/azure-sentinel/solarwinds-post-compromise-hunting-with-azure-sentinel/ba-p/1995095).

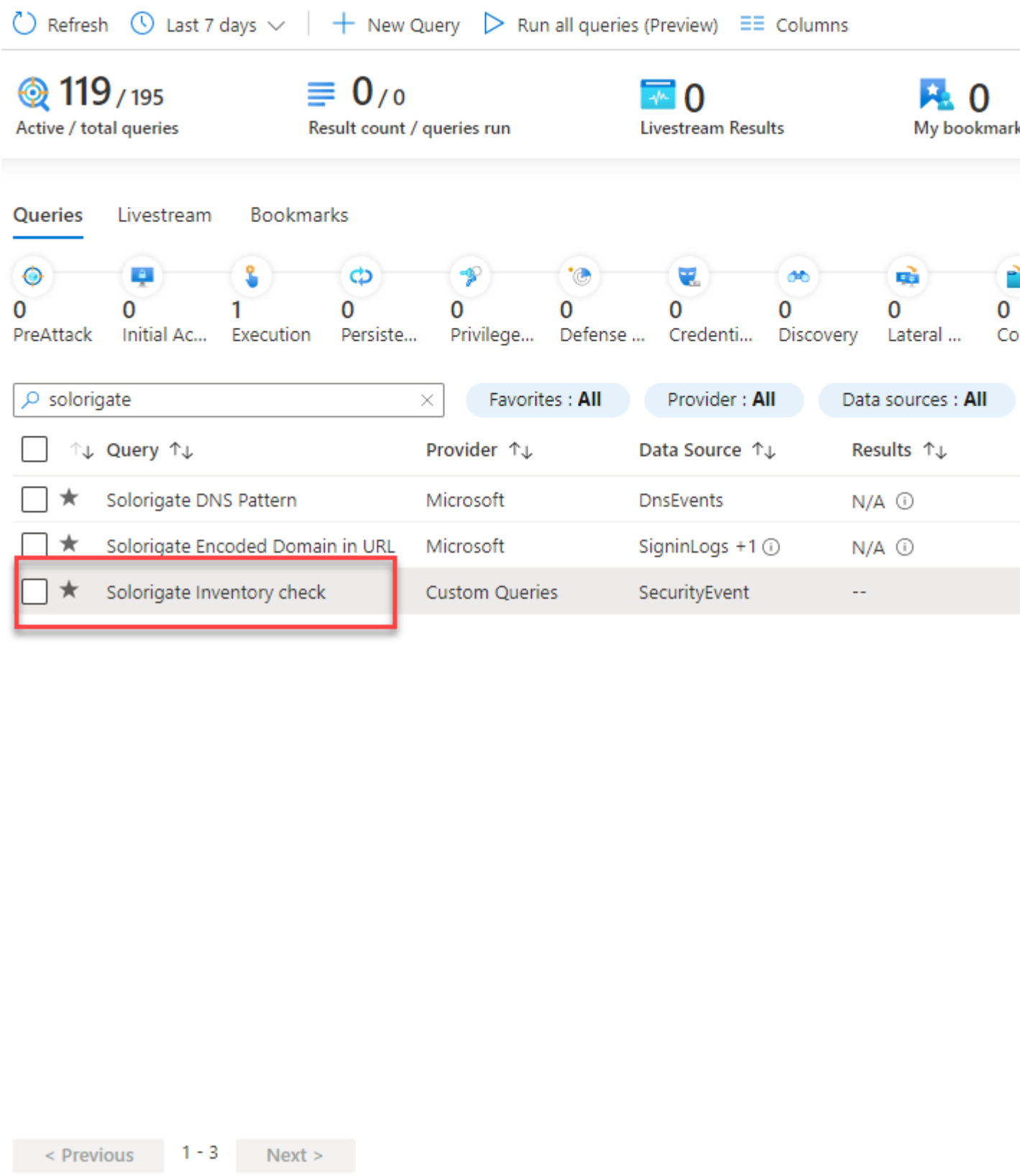
   https://techcommunity.microsoft.com/t5/azure-sentinel/solarwinds-post-compromise-hunting-with-azure-sentinel/ba-p/1995095

2. In this article, you can find a query that will do a SolarWinds inventory check query. We will use this query to find any other affected hosts.

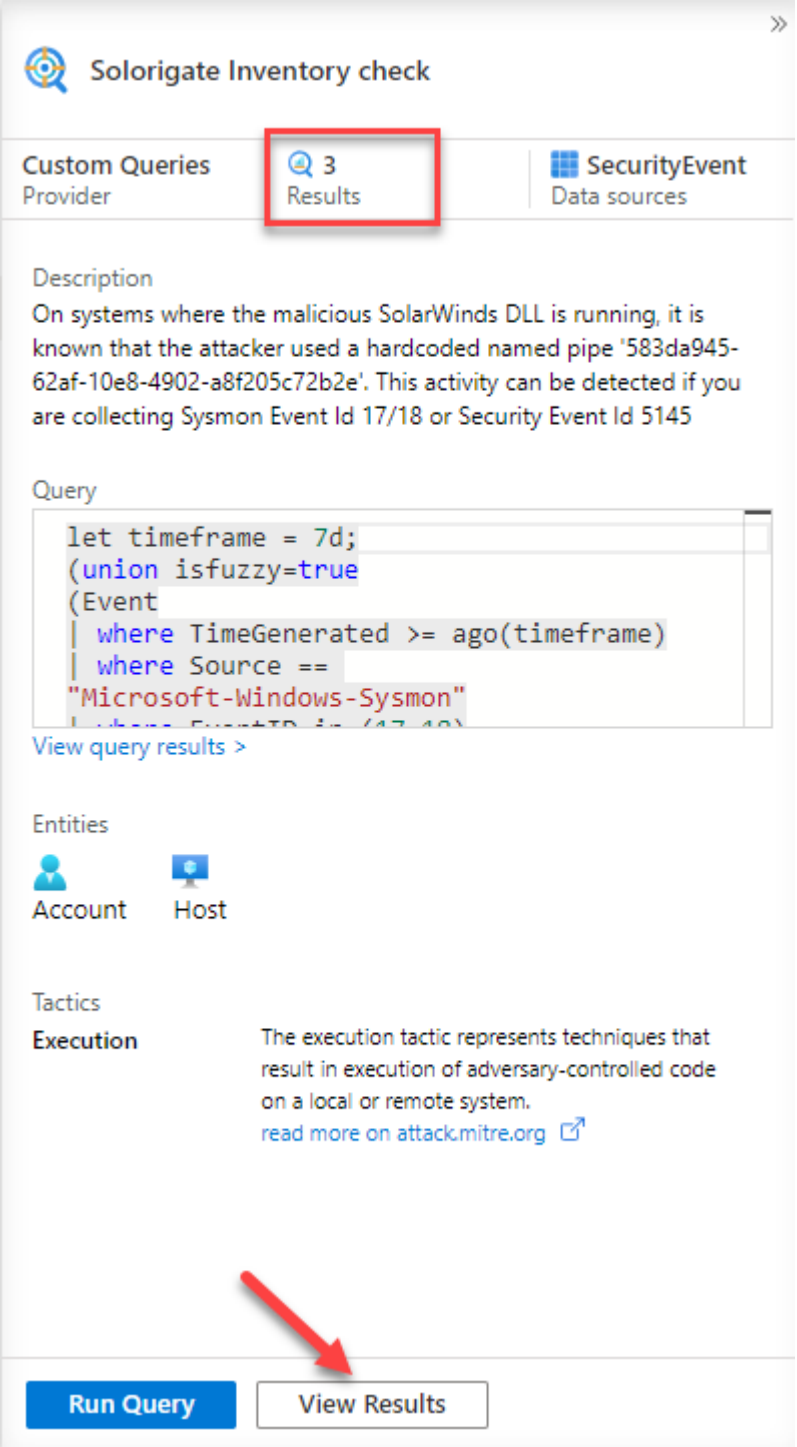
3. Switch to *Hunting* in the Microsoft Sentinel menu.



3. In the search box, type "solorigate". Select *Solorigate Inventory check* query and click on *Run Query*.



4. You should see a total of three results. Click on *View Results*



5. As you can see, besides **ClienPC**, there's two additional computers where the malicious DLL and named pipe has been found. Bookmark all three records, selecting them and then click on *Add bookmark*.

Run | Time range : Set in query | Save | Share | New alert rule | Expor

```
let timeframe = 7d;
(union isfuzzy=true
    (Event
     | where TimeGenerated >= ago(timeframe)
     | where Source == "Microsoft-Windows-Sysmon"
     | where EventID in (17, 18)
     | extend EvData = parse_xml(EventData)
     | extend EventDetail = EvData.DataItem.EventData.Data
     | extend NamedPipe = EventDetail.[5].["#text"]
     | extend ProcessDetail = EventDetail.[6].["#text"]
     | where NamedPipe contains '583da945-62af-10e8-4902-a8f205c72b2e'
```

Results | Chart | Columns | Add bookmark | Display time (UTC+00:00)

Completed

TimeGenerated [UTC]	NamedPipe	ProcessDetail	Account	timestamp [
5/11/2021, 8:45:20.947 PM				5/11/2021, 8
5/11/2021, 8:45:20.947 PM				5/11/2021, 8
5/11/2021, 8:45:20.947 PM				5/11/2021, 8

6. In the window that appears click on *Create* to create the bookmarks. As you can see entity mapping to already done for you.

Add multiple bookmarks

Hunting bookmarks enable Azure Sentinel users to save, tag, annotate, share and investigate results from a Log Analytics query.
You can view and manage Hunting Bookmarks in Azure Sentinel - Hunting. Click here to learn more.

Bookmark Name
Solorigate Inventory check - fc1ac8289b8a

Query Information
Account
Account_s - CONTOSO\ADMINPC$

Host
Computer - AdminPc.Contoso.Azure

IP
Choose column

URL
Choose column

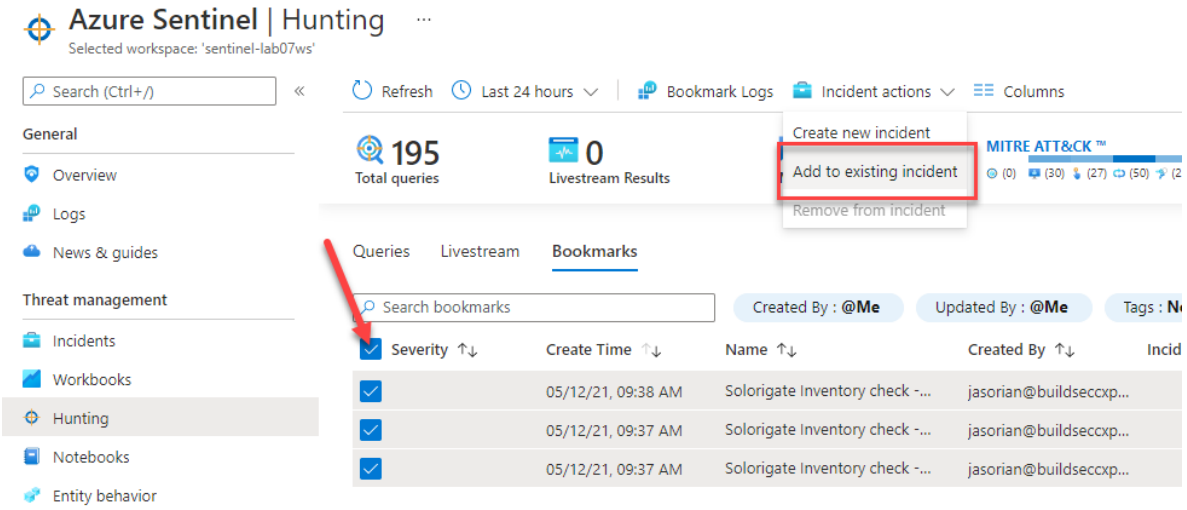
Timestamp
timestamp - 2021-05-04T13:33:16.356Z

Tags
+

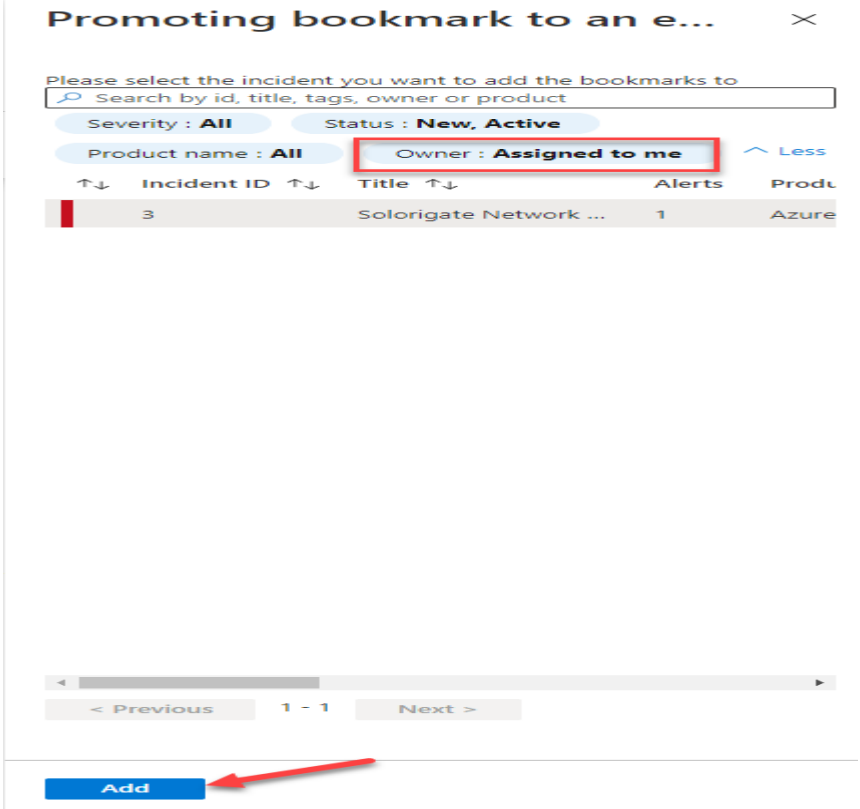
Notes

Create

7. Wait until the operation finishes and close the log search using the ✕ at the top right corner. This will land you in the Bookmarks tab inside Hunting menu, where you should see your two new bookmarks created. Select both of them and click on *Incident actions* at the top and then *Add to existing incident*.



8. From the list, pick the Solorigate incident that is assigned to you, and click *Add*.



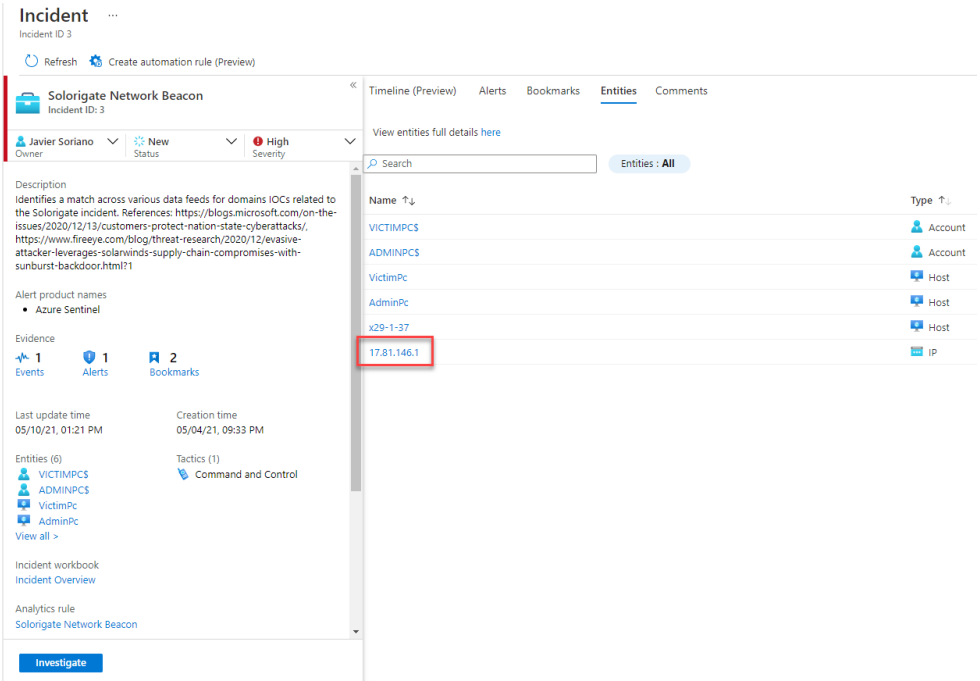
9. At this point you can ask the Operations team to isolate the hosts affected by this incident.

5. Exercise 5: Add IOC to Threat Intelligence

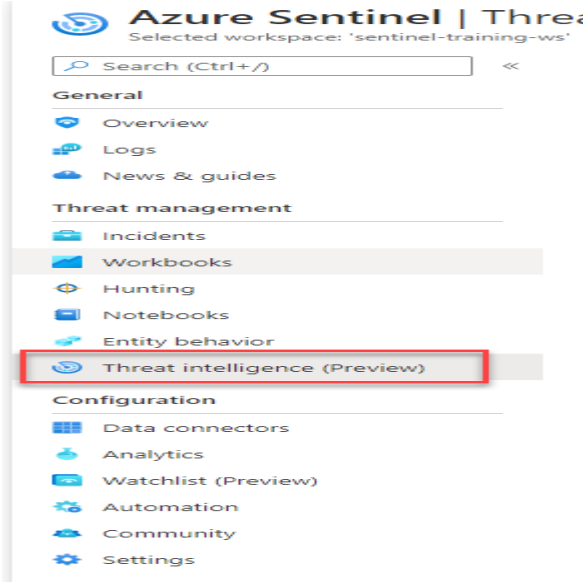
Now, we will add the IP address related to the incident to our list of IOCs, so we can capture any new occurrences of this IOC in our logs.

1. Go back to *Incidents* view.

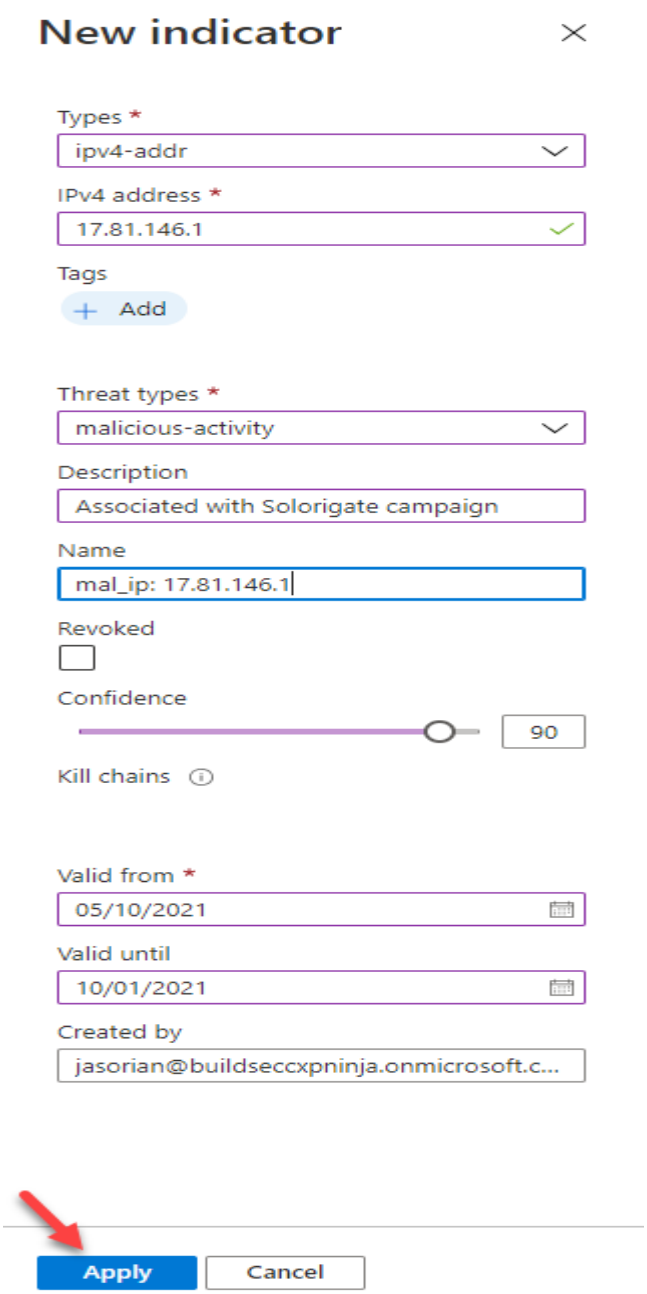
2. Select the Solorigate incident and copy the IP address entity involved. Notice that you have now more computer entities available (the ones coming from the bookmarks).



3. Go to the *Threat Intelligence* menu in Microsoft Sentinel and click *Add new* at the top.



4. Enter the following details in the *New indicator* dialog, with *Valid from* being today's date and *Valid until* being two months after. Then click *Apply*.

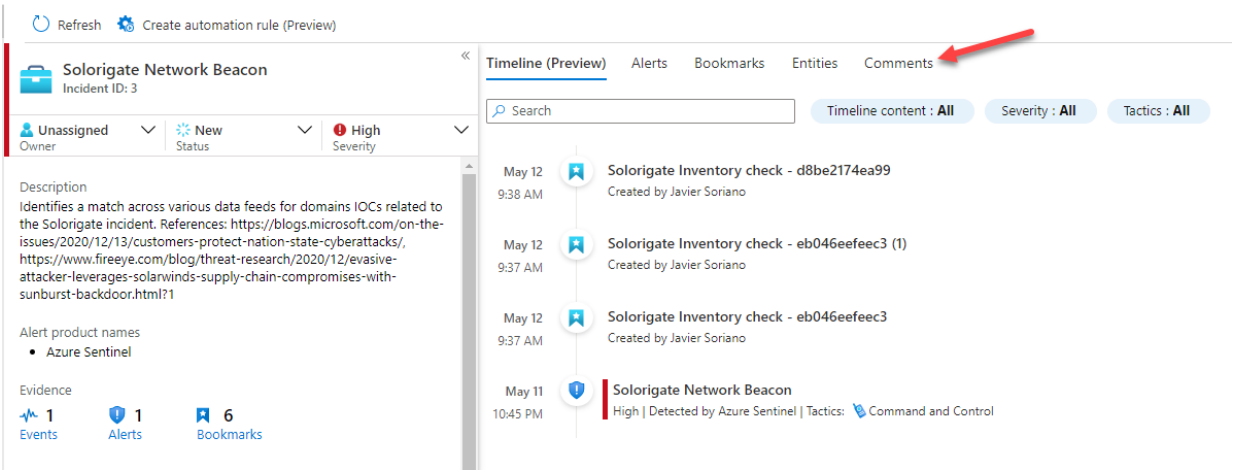


6. Exercise 6: Handover incident

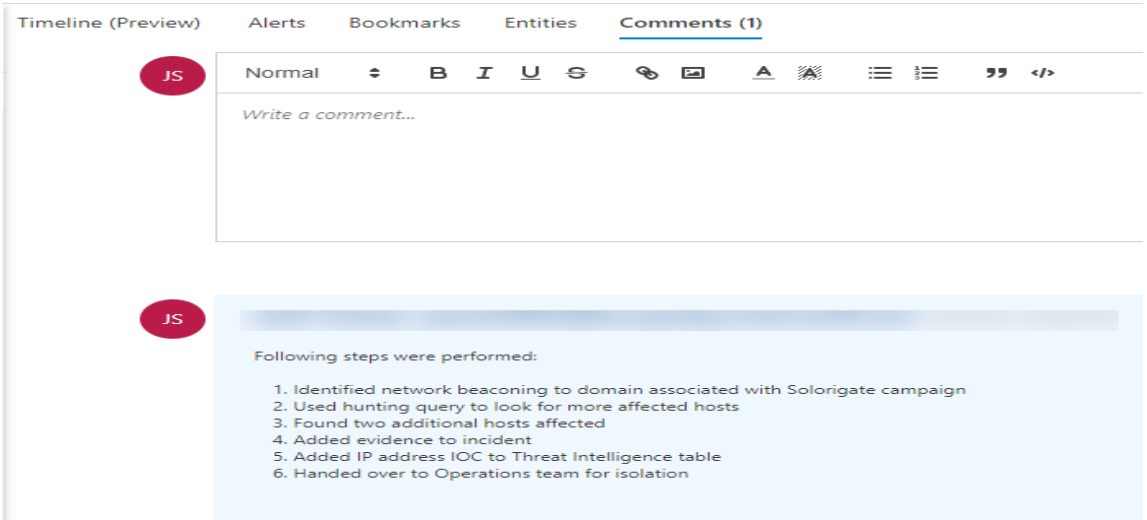
We will now prepare the incident for handover to forensics team.

1. Go to *Incidents* and select the Solorigate incident assigned to you. Click on *View full details*.

2. Move to the *Comments* tab.



3. Enter information about all the steps performed. As an example:



4. At this point you would hand over the incident to forensics team.