



# Lab Manual- Incident Management Azure Sentinel

---

**Prepared for:**

**Date:** 18<sup>th</sup> Nov 2021

**Prepared by:**

Document Name: Lab Manual

**Document Number** AZLabn993

**Contributor:**

## Contents

1. Introduction.....	3
2. Review Microsoft Sentinel incident tools and capabilities.....	3
3. Exercise 2: Handling Incident "Sign-ins from IPs that attempt sign-ins to disabled accounts" .....	5
4. Exercise 4: Hunting for more evidence .....	13
5. Exercise 5: Add IOC to Threat Intelligence .....	17
6. Exercise 6: Handover incident .....	19

## 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:

Microsoft Sentinel | Incidents

Selected workspace: 'sentinaldemo'

Search (Ctrl+/) Refresh Last 30 days Actions Security efficiency workbook Columns Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior

Open incidents: 3, New incidents: 3, Active incidents: 0

Open incidents by severity: High (1), Medium (2), Low (0), Informational (0)

Search by ID, title, tags, owner or product

Severity: All, Status: All, Product name: All, Owner: All

Auto-refresh incidents

Severity	Incident ID	Title	Alerts	Product names	Created time
Medium	3	Sign-ins from IPs that...	6	Microsoft Sentinel	04/14/22, 06:12 PM
Medium	2	Malicious Inbox Rule...	6	Microsoft Sentinel	04/14/22, 06:12 PM
High	1	Solorigate Network B...	6	Microsoft Sentinel	04/14/22, 06:12 PM

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**

Microsoft Sentinel | Incidents

Selected workspace: 'sentinaldemo'

Search (Ctrl+/) Refresh Last 30 days Actions Security efficiency workbook Columns Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK
- Content management

Open incidents: 3, New incidents: 3, Active incidents: 0

Open incidents by severity: High (1), Medium (2), Low (0), Informational (0)

Search by ID, title, tags, owner or product

Severity: All, Status: All, Product name: All, Owner: All

Auto-refresh incidents

Severity	Incident ID	Title	Alerts	Product names	Created time
Medium	3	Sign-ins from IPs that...	6	Microsoft Sentinel	04/14/22, 06:12 PM
Medium	2	Malicious Inbox Rule...	6	Microsoft Sentinel	04/14/22, 06:12 PM
High	1	Solorigate Network B...	6	Microsoft Sentinel	04/14/22, 06:12 PM

Sign-ins from IPs that attempt sign-ins to disabled accounts  
Incident ID: 3

Unassigned Owner

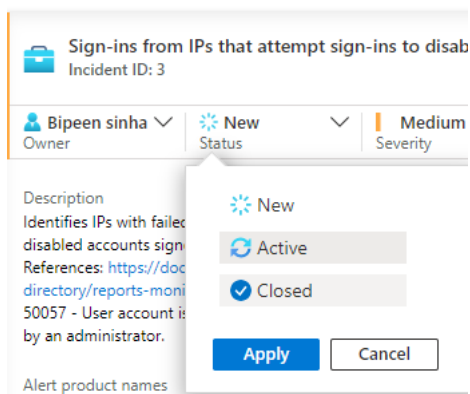
Assign to me  
bipin.sinhaa@outlook.com

Search users or groups

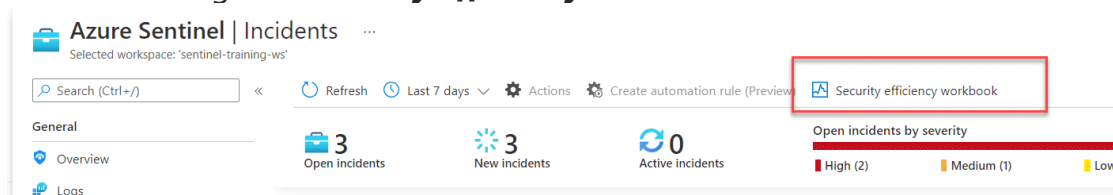
Users

- Unassign Incident
- Assign to me  
bipin.sinhaa@outlook.com
- Swetha
- gihan

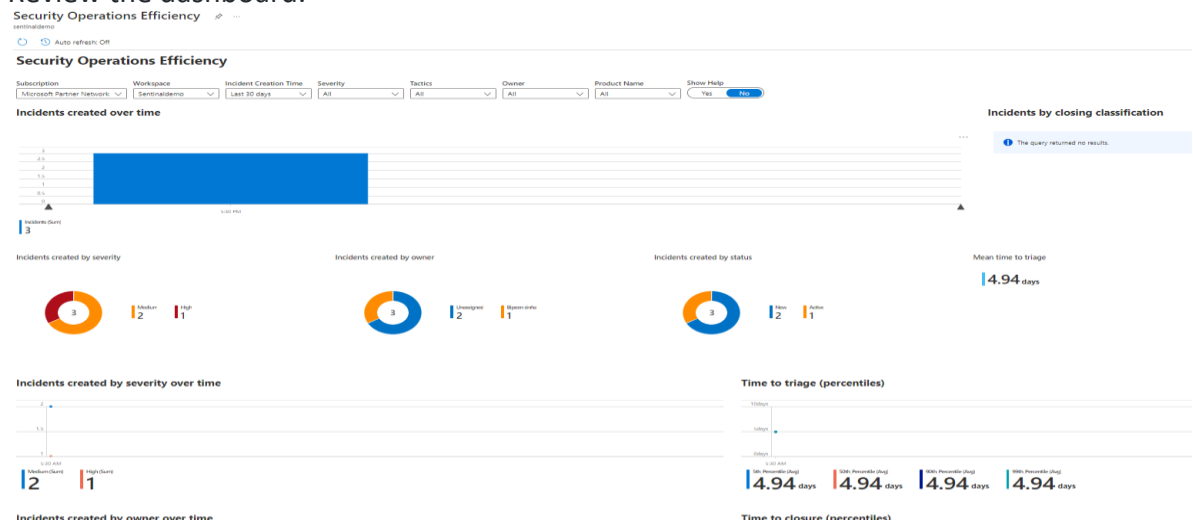
5. Also change the status from **New** to **Active**.



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.

The screenshot shows the Azure Sentinel interface. At the top, there are navigation links: Refresh, Last 7 days, Actions, Create automation rule (Preview), and Security efficiency workbook. Below this, a summary bar shows 3 Open Incidents, 3 New Incidents, and 0 Active Incidents. A bar chart displays 'Open incidents by severity' with 2 High, 1 Medium, 0 Low, and 0 Informational incidents. A search bar and filters for Severity, Status, Product name, and Owner are present. A table lists incidents, with the first one being 'Solorigate Network Beacon' (Incident ID: 3). The right-hand pane shows details for this incident, including a description, alert product names (Azure Sentinel), evidence (1 event, 1 alert, 0 bookmarks), last update time, creation time, entities (2), and tactics (1). A red arrow points to the 'Incident overview' link in the right-hand pane.

## 9. Review the dashboard.

The screenshot shows the 'Incident overview' page for the incident 'Sign-ins from IPs that attempt sign-ins to disabled accounts'. The page includes a section for 'General Incident Information' with fields for Title, Time created, Severity (Medium), Status (Active), Owner (Unassigned), and Products (Azure Sentinel). Below this is a table for 'Alert count', 'Bookmarks', 'Labels', 'Classification', 'Classification Reason', and 'Classification Comment'. The 'Alert Names' section lists the incident title. At the bottom, there is a 'Recommended Actions' section with a table showing the incident number, title, severity, and remediation URL.

## 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

Incident ID 3

Refresh

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

Alerts

Severity: All

Click the Number

Severity	Alert name	Alert status	Alert ID	Product name	Events	Creation time	Time frame
Medium	Sign-ins from IPs that attempt...	New	c44815a2-2431-2350-6744-b...	Microsoft Sentinel	1	04/14/22, 06:12 PM	04/14/22, 05:37 PM - 04/14/22...
Medium	Sign-ins from IPs that attempt...	New	201848e-0877-1e71-c5d8-7b...	Microsoft Sentinel	1	04/14/22, 06:17 PM	04/14/22, 05:42 PM - 04/14/22...
Medium	Sign-ins from IPs that attempt...	New	8dc02c0d-c0ab-a50e-53a6-e...	Microsoft Sentinel	1	04/14/22, 06:22 PM	04/14/22, 05:47 PM - 04/14/22...
Medium	Sign-ins from IPs that attempt...	New	244332a-5c37-8c0b-7384-e...	Microsoft Sentinel	1	04/14/22, 06:27 PM	04/14/22, 05:52 PM - 04/14/22...
Medium	Sign-ins from IPs that attempt...	New	7151606-680a-c0cc-e85e-e...	Microsoft Sentinel	1	04/14/22, 06:32 PM	04/14/22, 05:57 PM - 04/14/22...
Medium	Sign-ins from IPs that attempt...	New	d278f16-e4ce-d882-3caa-2a...	Microsoft Sentinel	1	04/14/22, 06:37 PM	04/14/22, 06:02 PM - 04/14/22...

- In raw log search, expand 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.

Run Time range: Custom Save Share New alert rule Exp

```

1 // The query_now parameter represents the time (in UTC) at which the scheduled
2 set query_now = datetime(2021-05-04T13:28:39.0301182Z);
3 SigninLogs_CL
4 | where ResultType == "50057"
5 | where ResultDescription == "User account is disabled. The account has been di
6 | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), disal
7   disabledAccountsTargeted = dcount(UserPrincipalName_s), applicationsTargeted
8   applicationSet = makeset(AppDisplayName_s)
9   by IPAddress, Type
10 | order by disabledAccountLoginAttempts desc
11 | join kind= leftouter (

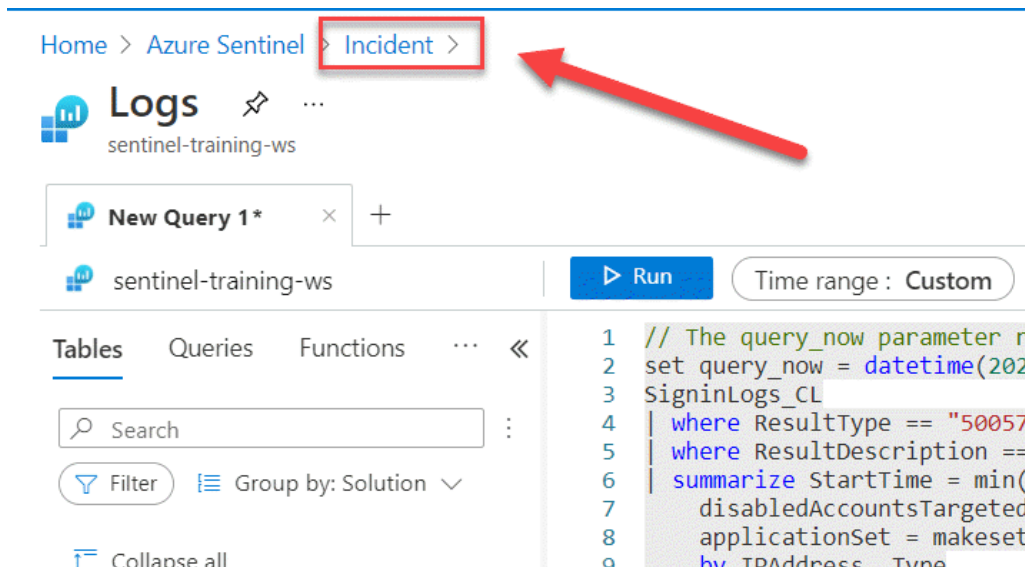
```

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

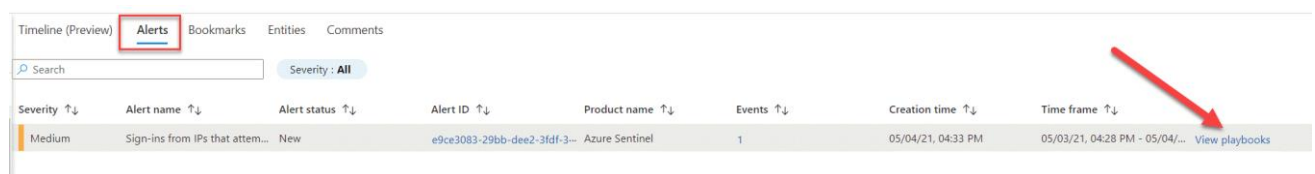
Completed. Showing results from the custom time range.

timestamp [UTC]	IPCustomEntity	StartTime [UTC]	EndTime [UTC]
5/4/2021, 1:27:11.545Z	175.45.176.99	5/4/2021, 1:27:11.545Z	5/4/2021, 1:27:11.545Z
...			
StartTime [UTC]		2021-05-04T13:27:11.545Z	
EndTime [UTC]		2021-05-04T13:27:11.545Z	
IPAddress	175.45.176.99		
disabledAccountLoginAttempts	4		
disabledAccountsTargeted	1		
disabledAccountSet	["johns@m365x816222.onmicrosoft.com"]		
	0 johns@m365x816222.onmicrosoft.com		
applicationSet	["Azure Portal"]		
successfulAccountSigninCount	1		
successfulAccountSigninSet	["adelev@m365x816222.onmicrosoft.com"]		
Type	SigninLogs_CL		
timestamp [UTC]		2021-05-04T13:27:11.545Z	
IPCustomEntity	175.45.176.99		

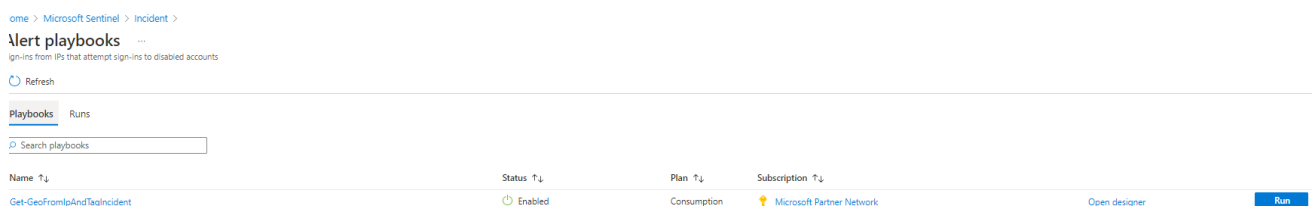
8. To get more context for this IP, we want to add GEO IP enrichment. In a real life SOC this operation will run automatically, but for this lab we want you to run it manually.
- Navigate back to the incident full page to the alert tab and scroll to the right



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.

Open incidents by severity: High (2), Medium (1), Low (0), Informational (0)

Search by id, title, tags, owner or product

Severity: All, Status: New, Active, Product name: All, Owner: All

Auto-refresh incidents

Alerts	Product names	Created time ↑↓	Last update time ↑↓	Owner ↑↓	Status ↑↓	Tags
sign-ins t...	Azure Sentinel	05/04/21, 04:33 PM	05/08/21, 07:20 PM	Yaniv Shasha	Active	North Korea, Pyong...
1	Azure Sentinel	05/04/21, 10:33 PM	05/04/21, 10:33 PM	Unassigned	New	
1	Azure Sentinel	05/04/21, 04:33 PM	05/04/21, 04:33 PM	Unassigned	New	

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

Owner: Yaniv Shasha, Status: Active, Severity: High

Description: Identifies IPs with failed attempts to sign in to one or more d accounts signed in successfully to another account. Refereno https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes 50057 - User acc disabled. The account has been disabled by an administrator

Alert product names: Azure Sentinel

Evidence: 1 Events, 1 Alerts, 0 Bookmarks

Last update time: 05/08/21, 07:20 PM, Creation time: 05/04/21, 04:33 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

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**

Microsoft Sentinel | Workbooks

Selected workspace: 'sentinaldemo'

Search (Ctrl+/) Refresh Add workbook

General: Overview, Logs, News & guides, Search (Preview)

Threat management: Incidents, Workbooks, Hunting, Notebooks

1 Saved workbooks, 120 Templates, 0 Updates

My workbooks, Templates

Search

Investigation Insights - 04/14/2022 12:28

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.



## Investigation Insights - 04/14/2022 12:28

sentinaldemo

[Edit](#) [Open](#) [Print](#) [Refresh](#) [Share](#) [Help](#) Auto refresh: Off

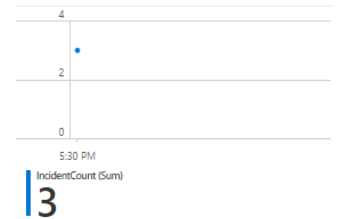
Subscription: Microsoft Partner Network Workspace: Sentinaldemo TimeRange: Last 7 days Investigate By: Incident Bookmark Entity Show Incident Trend: Yes No Help: Yes No Change Log

## Investigation Insights

## Incident Insights

Incident Severity: All Status: All Owner: All Tags: All Incident Number: Enter value

## Incident Timeline



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.

## Investigation Insights - 04/14/2022 12:28

sentinaldemo

[Edit](#) [Open](#) [Print](#) [Refresh](#) [Share](#) [Help](#) Auto refresh: Off

Subscription: Microsoft Partner Network Workspace: Sentinaldemo TimeRange: Last 7 days Investigate By: Incident Bookmark **Entity** Show Incident Trend: No Help: Yes No Change Log

## Investigation Insights

## Entity Insights

Choose an Entity Type to investigate by:

**Investigate IP Address** Investigate Account Investigate Host Investigate URL Investigate File Hash Full Search

IPAddress: 175.45.176.99

Active Accounts Network Normalized Network (Preview) IOCs Related Alerts & Bookmarks

## Accounts Active from IP

adelev@m365x816222... 188 johns@m365x816222.o... 39 admin@m365x816222... 4 sharepoint\system 2

## AAD Signin



Microsoft Teams Web Client 16 Office 365 Shell WCSS-Client 15 Other 14 Azure Portal 7 Office 365 SharePoint 4

## Office Activity



Other 52 FileAccessed 45 PageViewed 28 FilePreviewed 26 FolderModified 12 ListViewed 10

## Activity Detail

TimeGenerated	ResultType	UPN	AppOrAction	Details	Source
4/14/2022, 6:06:32 PM	50057	johns@m365x816222.onmicrosoft.com	Azure Portal	User account is disabled. The account has been disabled ...	SignInLogs
4/14/2022, 6:06:32 PM	50057	johns@m365x816222.onmicrosoft.com	Azure Portal	User account is disabled. The account has been disabled ...	SignInLogs

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](mailto:adelev@m365x816222.onmicrosoft.com) and validate it in our internal HR system, from the information we collected it 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**

The screenshot displays the Azure Sentinel incident management interface. At the top, there are filters for 'Open incidents by severity' (High, Medium, Low, Informational) and a search bar. The main table lists incidents, with the first incident selected. The right-hand pane shows details for the selected incident, including 'Sign-ins from IPs that attempt sign-ins to disabled a...' and 'Incident ID: 1'. The 'Actions' dropdown menu is open, and the 'Create automation rule (Preview)' option is highlighted with a red box and a red arrow.

Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner
1	Sign-ins from IPs that attempt sign-ins t...	1	Azure Sentinel	05/04/21, 04:33 PM	05/08/21, 07:20 PM	Yaniv S

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**.

## Create new automation rule



Automation rule name

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

### Trigger

When incident is created

### Conditions

If

Analytic rule name

Contains



Sign-ins from IPs th...



And

IP address



Equals



175.45.176.99



+ Add condition

### Actions <sup>①</sup>

Change status



Closed



Benign Positive - suspicious but expected



Comment

Closing the incident will archive the associated team.

+ Add action

### Rule expiration <sup>①</sup>

05/09/2021



8:27 PM

Apply

Cancel

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

### 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](#)

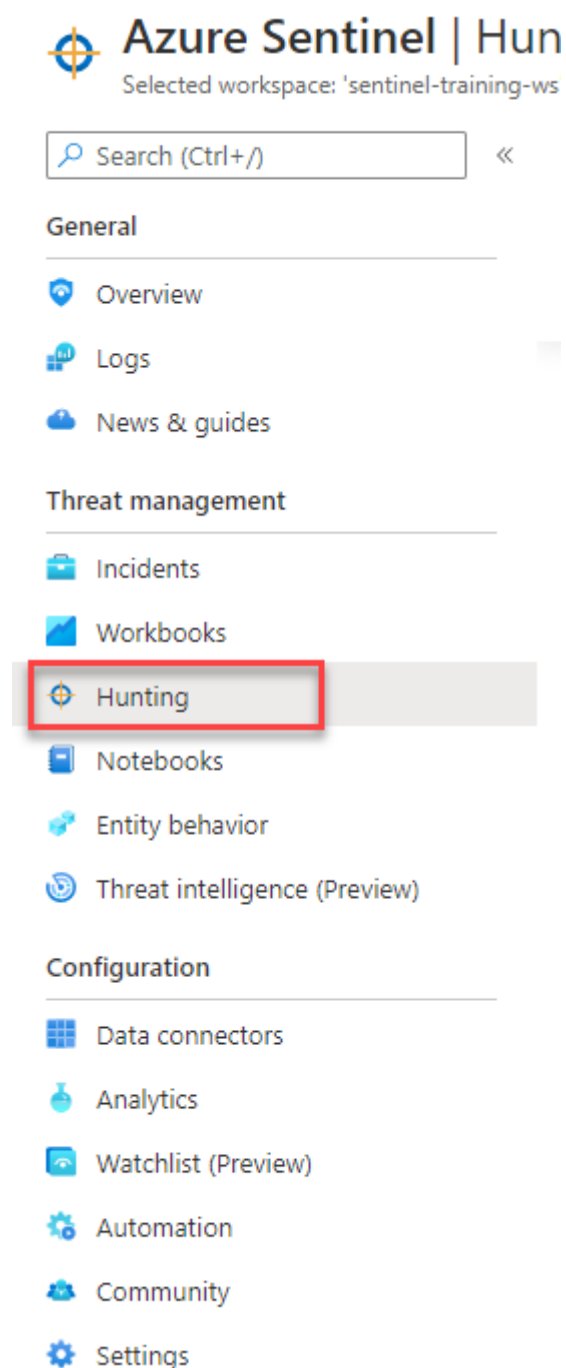
[Investigate](#)

## 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*.

Refresh Last 7 days | + New Query ▶ Run all queries (Preview) Columns

119 / 195 Active / total queries    0 / 0 Result count / queries run    0 Livestream Results    0 My bookmark

Queries Livestream Bookmarks


0 PreAttack    0 Initial Ac...    1 Execution    0 Persiste...    0 Privilege...    0 Defense ...    0 Credenti...    0 Discovery    0 Lateral ...    0 Co

solorigate x    Favorites : All    Provider : All    Data sources : All


<input type="checkbox"/> ↑↓ Query ↑↓	Provider ↑↓	Data Source ↑↓	Results ↑↓
<input type="checkbox"/> ★ Solorigate DNS Pattern	Microsoft	DnsEvents	N/A ⓘ
<input type="checkbox"/> ★ Solorigate Encoded Domain in URL	Microsoft	SigninLogs +1 ⓘ	N/A ⓘ
<input type="checkbox"/> ★ Solorigate Inventory check	Custom Queries	SecurityEvent	--


< Previous    1 - 3    Next >

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

 Solorigate Inventory check

Custom Queries  
Provider

 3  
Results

 SecurityEvent  
Data sources

Description


On systems where the malicious SolarWinds DLL is running, it is known that the attacker used a hardcoded named pipe '583da945-62af-10e8-4902-a8f205c72b2e'. This activity can be detected if you are collecting Sysmon Event Id 17/18 or Security Event Id 5145


Query

```
let timeframe = 7d;  
(union isfuzzy=true  
(Event  
| where TimeGenerated >= ago(timeframe)  
| where Source ==  
"Microsoft-Windows-Sysmon"  
| where EventId in (17, 18)
```

[View query results >](#)

Entities


 Account

 Host

Tactics

**Execution**

The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.

[read more on attack.mitre.org](#) 

Run Query

View Results

- 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

Export

```

1 let timeframe = 7d;
2 (union isfuzzy=true
3   (Event
4     | where TimeGenerated >= ago(timeframe)
5     | where Source == "Microsoft-Windows-Sysmon"
6     | where EventID in (17, 18)
7     | extend EvData = parse_xml(EventData)
8     | extend EventDetail = EvData.DataItem.EventData.Data
9     | extend NamedPipe = EventDetail.[5].["#text"]
10    | extend ProcessDetail = EventDetail.[6].["#text"]
11    | 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

- 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



- Wait until the operation finishes and close the log search using the **X** 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*.

Azure Sentinel | Hunting

Selected workspace: 'sentinel-lab07ws'

Search (Ctrl+/) Refresh Last 24 hours Bookmark Logs Incident actions Columns

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting**
- Notebooks
- Entity behavior

195 Total queries 0 Livestream Results

Create new incident Add to existing incident Remove from incident

MITRE ATT&CK™

Queries Livestream Bookmarks

Search bookmarks Created By : @Me Updated By : @Me Tags : N

Severity	Create Time	Name	Created By	Incid
✓	05/12/21, 09:38 AM	Solorigate Inventory check -...	jasorian@buildseccxp...	
✓	05/12/21, 09:37 AM	Solorigate Inventory check -...	jasorian@buildseccxp...	
✓	05/12/21, 09:37 AM	Solorigate Inventory check -...	jasorian@buildseccxp...	

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

Promoting bookmark to an e...

Please select the incident you want to add the bookmarks to

Search by id, title, tags, owner or product

Severity : All Status : New, Active

Product name : All Owner : Assigned to me

Incident ID	Title	Alerts	Prod
3	Solorigate Network ...	1	Azure

< Previous 1 - 1 Next >

Add

- 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.

- 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).

The screenshot shows the 'Incident' view in Microsoft Sentinel for an incident named 'Solorigate Network Beacon' (Incident ID: 3). The interface includes a left sidebar with incident details, a main content area with tabs for 'Timeline (Preview)', 'Alerts', 'Bookmarks', 'Entities', and 'Comments', and a right sidebar with a list of entities. The 'Entities' tab is active, showing a table of entities. The entity '17.81.146.1' is highlighted with a red box. The table has columns for 'Name' and 'Type'.

Name	Type
VICTIMPCS	Account
ADMINPCS	Account
VictimPc	Host
AdminPc	Host
x29-1-37	Host
17.81.146.1	IP

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

The screenshot shows the 'Azure Sentinel | Threat Intelligence' menu. The 'Threat intelligence (Preview)' option is highlighted with a red box. The menu includes sections for 'General', 'Threat management', and 'Configuration'.

- General
  - Overview
  - Logs
  - News & guides
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks
  - Entity behavior
  - Threat intelligence (Preview)
- Configuration
  - Data connectors
  - Analytics
  - Watchlist (Preview)
  - Automation
  - Community
  - Settings

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*.

## New indicator



Types \*

ipv4-addr



IPv4 address \*

17.81.146.1



Tags

+ Add

Threat types \*

malicious-activity



Description

Associated with Solorigate campaign

Name

mal\_ip: 17.81.146.1

Revoked

☐

Confidence

90

Kill chains ⓘ

Valid from \*

05/10/2021



Valid until

10/01/2021



Created by

jasorian@buildseccxpinja.onmicrosoft.c...



Apply

Cancel

## 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.

Refresh Create automation rule (Preview)

### Solorigate Network Beacon

Incident ID: 3

Unassigned Owner New Status High Severity

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>

Alert product names  
• Azure Sentinel

Evidence  
1 Events 1 Alerts 6 Bookmarks

Timeline (Preview) Alerts Bookmarks Entities Comments

Search Timeline content : All Severity : All Tactics : All

- May 12 9:38 AM Solorigate Inventory check - d8be2174ea99 Created by Javier Soriano
- May 12 9:37 AM Solorigate Inventory check - eb046eefec3 (1) Created by Javier Soriano
- May 12 9:37 AM Solorigate Inventory check - eb046eefec3 Created by Javier Soriano
- May 11 10:45 PM Solorigate Network Beacon High | Detected by Azure Sentinel | Tactics: Command and Control

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

Timeline (Preview) Alerts Bookmarks Entities Comments (1)

JS

Normal B I U S

Write a comment...

JS

Following steps were performed:

1. Identified network beaconing to domain associated with Solorigate campaign
2. Used hunting query to look for more affected hosts
3. Found two additional hosts affected
4. Added evidence to incident
5. Added IP address IOC to Threat Intelligence table
6. Handed over to Operations team for isolation

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