

Implementing Microsoft Sentinel for Real-Time Threat Monitoring and Incident Response

By Frederick Adigun

Documentation

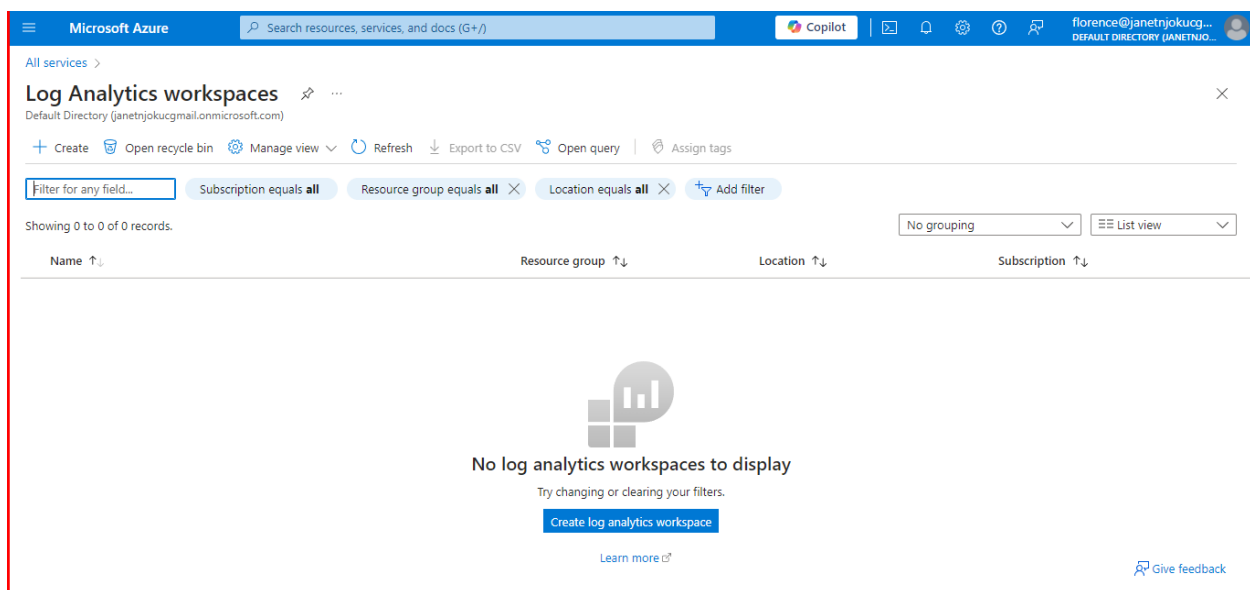
Steps

1. Setup Microsoft Sentinel.
2. Connect Microsoft Entra ID to Sentinel.
3. Configure analytic rules for your simulated attack scenario.
4. Automate Incident Response.

Step 1: Setup Microsoft Sentinel

Task 1: Create a Log Analytics Workspace in Azure

1. In the Azure Portal, search for and select “Log Analytics workspaces”.
2. Navigate to Log Analytics Workspaces
In the left-hand menu, click on “All services”.
In the “Categories” section, select “Monitor”.
Scroll down and click on “Log Analytics workspaces”.



3. Create a new Log Analytics Workspace:

Click on the “+ Create” button.

Fill in the required information:

- Subscription: Select the subscription you want to use.
- Resource Group: Select an existing resource group or create a new one.
- Name: Enter a unique name for the workspace.
- Region: Select the region closest to your resources.

Click on “Review + create”.

Review your settings and click on “Create” to deploy the workspace.

The screenshot shows the 'Create Log Analytics workspace' page in the Microsoft Azure portal. The page has a blue header with the Microsoft Azure logo and a search bar. Below the header, there's a breadcrumb trail: 'All services > Log Analytics workspaces >'. The main title is 'Create Log Analytics workspace'. Below the title, there's a brief description: 'With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.' The form is divided into two sections: 'Project details' and 'Instance details'. In the 'Project details' section, there are two dropdown menus: 'Subscription' (selected: Microsoft Azure Sponsorship) and 'Resource group' (selected: GROUP3-Get2cloudRG). Below the 'Resource group' dropdown is a link 'Create new'. In the 'Instance details' section, there are two dropdown menus: 'Name' (selected: Group3-Logs) and 'Region' (selected: East US). At the bottom of the form, there are three buttons: 'Review + Create' (highlighted in blue), '< Previous', and 'Next: Tags >'. The user's profile information is visible in the top right corner: 'florence@janetnjokucg...' and 'DEFAULT DIRECTORY (JANETNJOKUCG...)'.

Task 2: Enable Sentinel on the created Log Analytics Workspace

1. Navigate to Microsoft Sentinel:

In the Azure Portal, use the search bar at the top to search for “Microsoft Sentinel”.

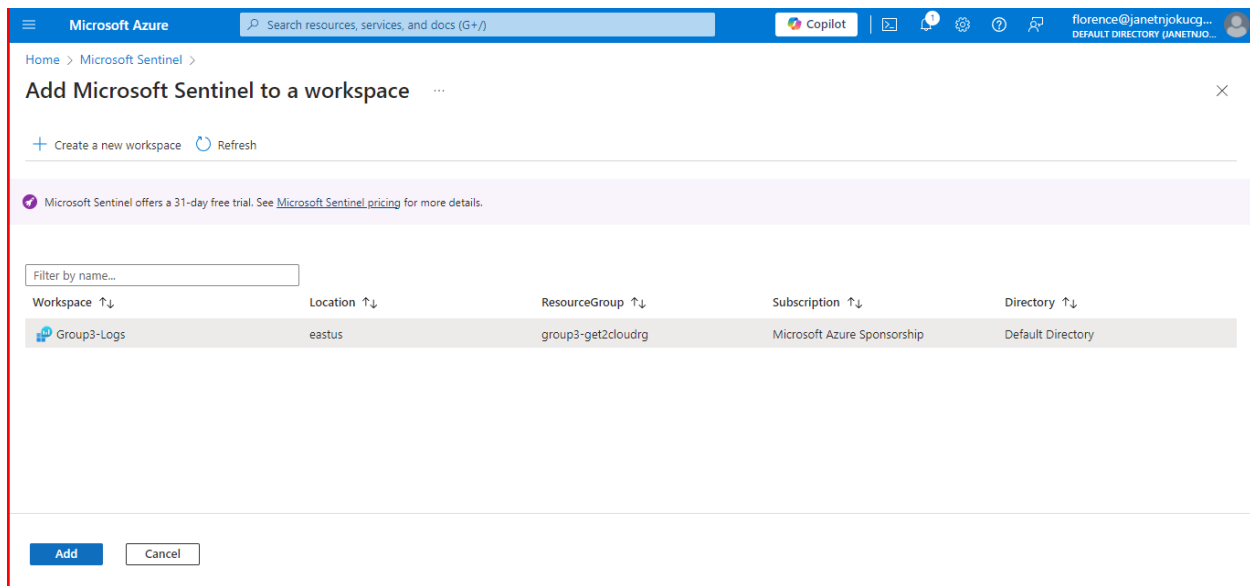
Click on “Microsoft Sentinel” from the search results.

2. Add Microsoft Sentinel:

On the Microsoft Sentinel page, click on the “+ Add” button.

Select the Log Analytics Workspace you created earlier from the list.

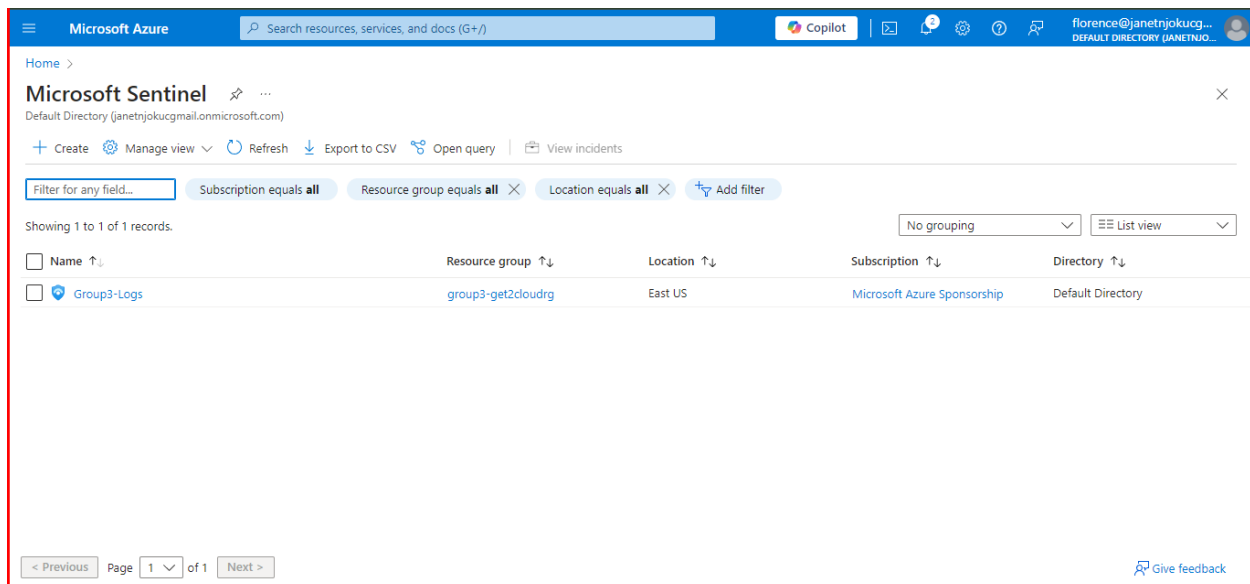
Click on “Add Microsoft Sentinel”.



3. Verify Sentinel Enablement:

Once the workspace is added, you should see it listed under the “Microsoft Sentinel” page.

Click on the workspace name to navigate to the Microsoft Sentinel dashboard.



Step 2: Connect Microsoft Entra ID to Sentinel

Task 1: Configure the Microsoft Entra ID Data Connector

1. Navigate to Microsoft Sentinel:

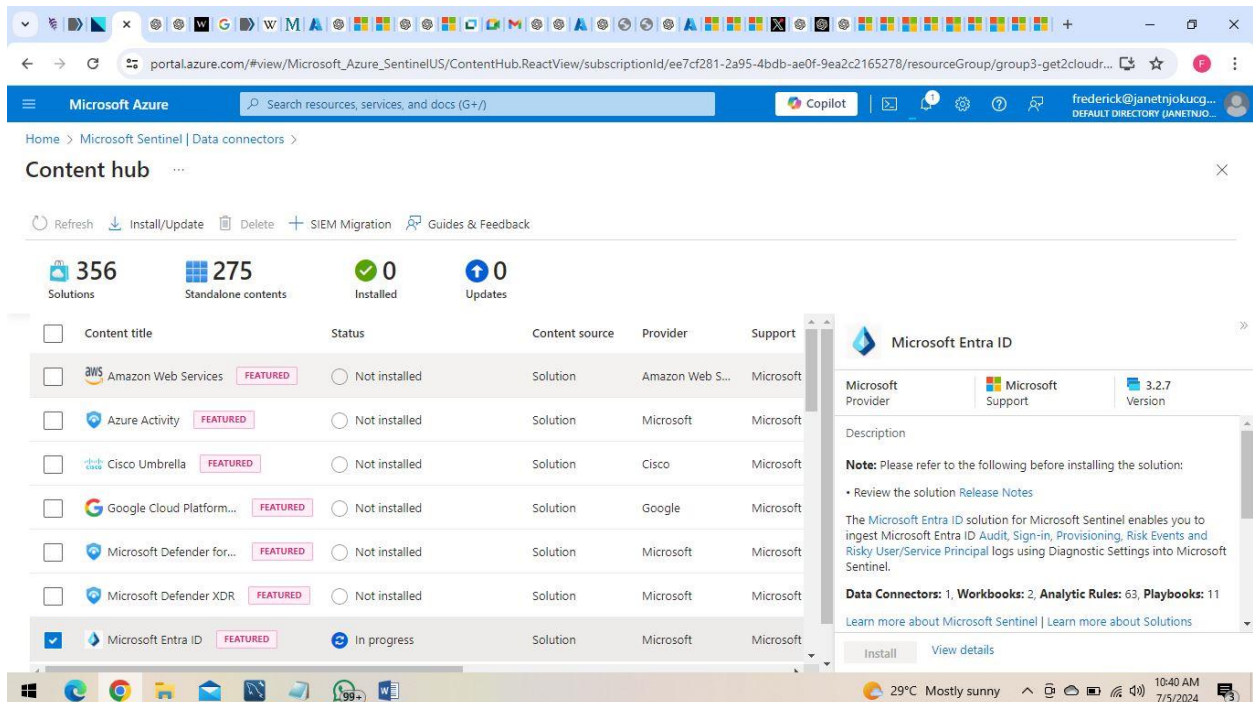
Open the Azure portal.

Search for Microsoft Sentinel and select your Sentinel workspace.

2. Add Data Connector:

In the Microsoft Sentinel workspace, go to Configuration > Data connectors.

Search for Microsoft Entra ID and select it.



The screenshot shows the Microsoft Azure portal interface for the Microsoft Sentinel Content hub. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile. The main content area displays the 'Content hub' with a list of data connectors. The connectors are organized into columns: Content title, Status, Content source, Provider, and Support. The Microsoft Entra ID connector is highlighted, showing its status as 'In progress' and a description of its functionality. The description includes a note about the solution and a link to the release notes.

Content title	Status	Content source	Provider	Support
Amazon Web Services	Not installed	Solution	Amazon Web S...	Microsoft
Azure Activity	Not installed	Solution	Microsoft	Microsoft
Cisco Umbrella	Not installed	Solution	Cisco	Microsoft
Google Cloud Platform...	Not installed	Solution	Google	Microsoft
Microsoft Defender for...	Not installed	Solution	Microsoft	Microsoft
Microsoft Defender XDR	Not installed	Solution	Microsoft	Microsoft
Microsoft Entra ID	In progress	Solution	Microsoft	Microsoft

Microsoft Entra ID

Microsoft Provider | Microsoft Support | 3.2.7 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The **Microsoft Entra ID** solution for Microsoft Sentinel enables you to ingest Microsoft Entra ID Audit, Sign-in, Provisioning, Risk Events and Risky User/Service Principal logs using Diagnostic Settings into Microsoft Sentinel.

Data Connectors: 1, **Workbooks:** 2, **Analytic Rules:** 63, **Playbooks:** 11

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

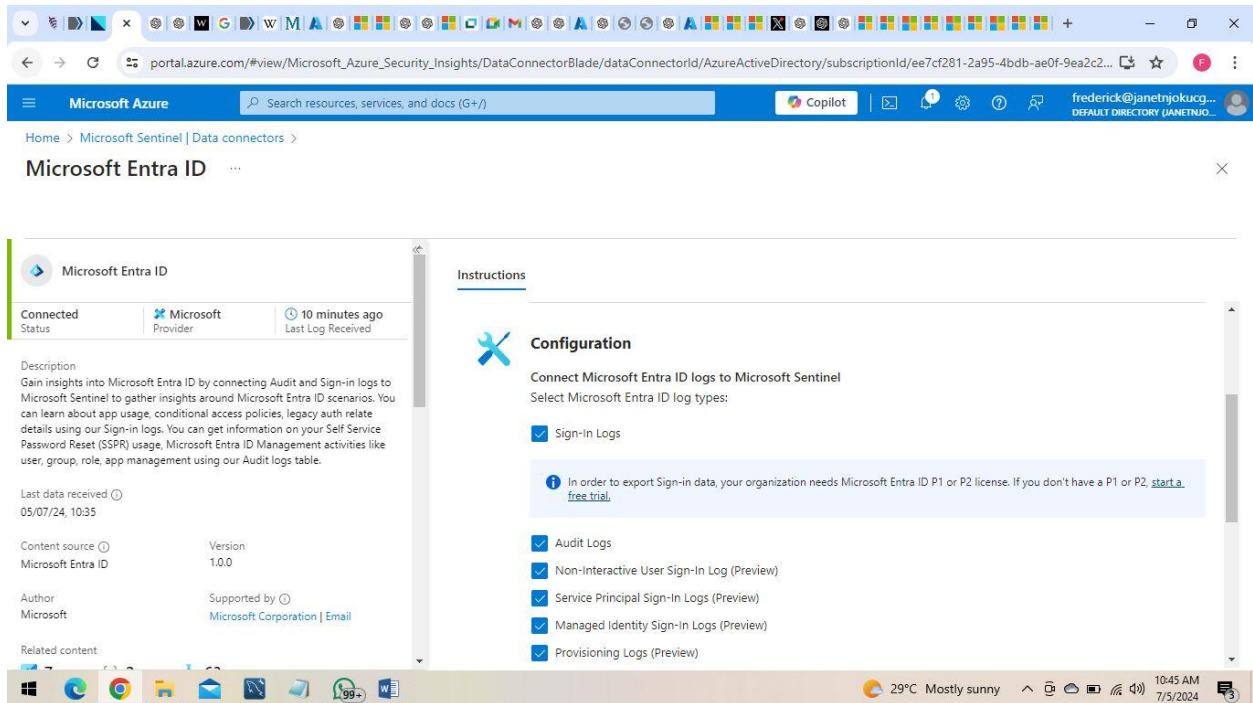
[Install](#) [View details](#)

3. Connect Microsoft Entra ID:

Click on the Open connector page.

You will see the Prerequisites section. Ensure you have the necessary permissions.

In the Configuration section, select the Sign-in logs and Audit logs checkboxes to enable these logs.



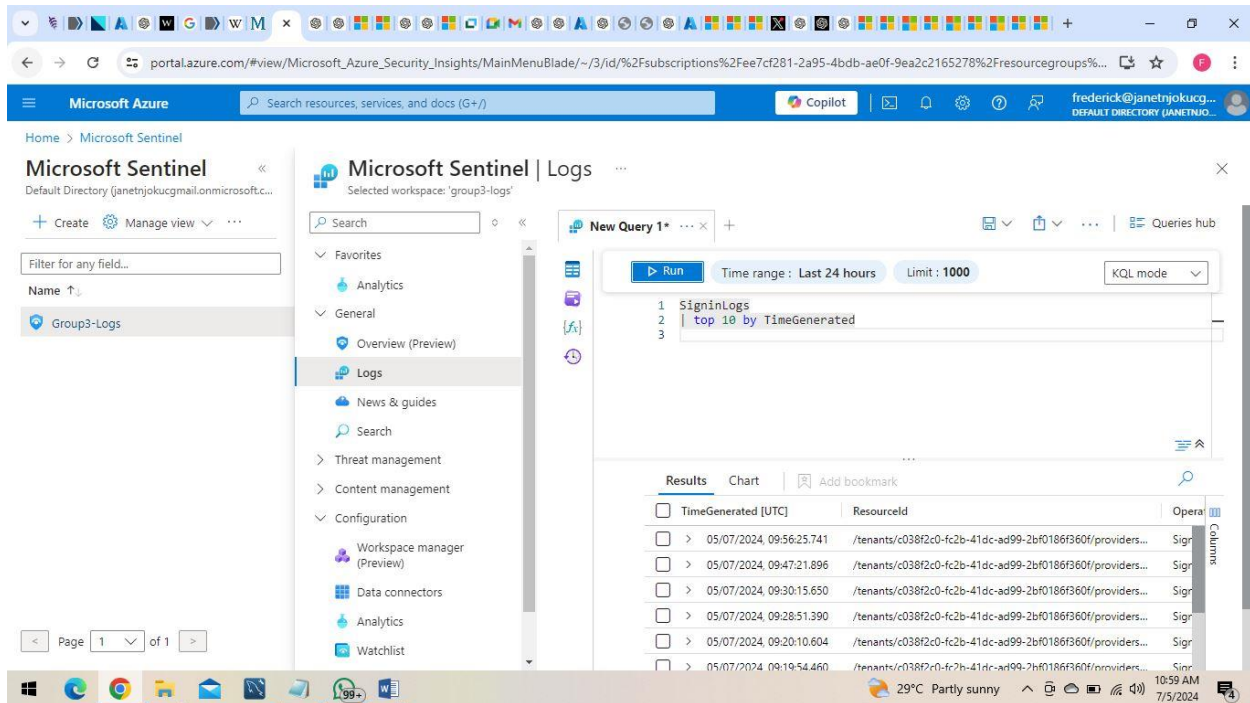
Click on Apply changes to save the configuration.

Task 2: Verify Connection and Ingestion

1. Go to Logs in Microsoft Sentinel:
In your Microsoft Sentinel workspace, go to Logs under the General section.
2. Run a Basic Query:
Use the following Kusto Query Language (KQL) query to check if sign-in logs are being ingested:

This query retrieves the top 10 most recent sign-in log entries

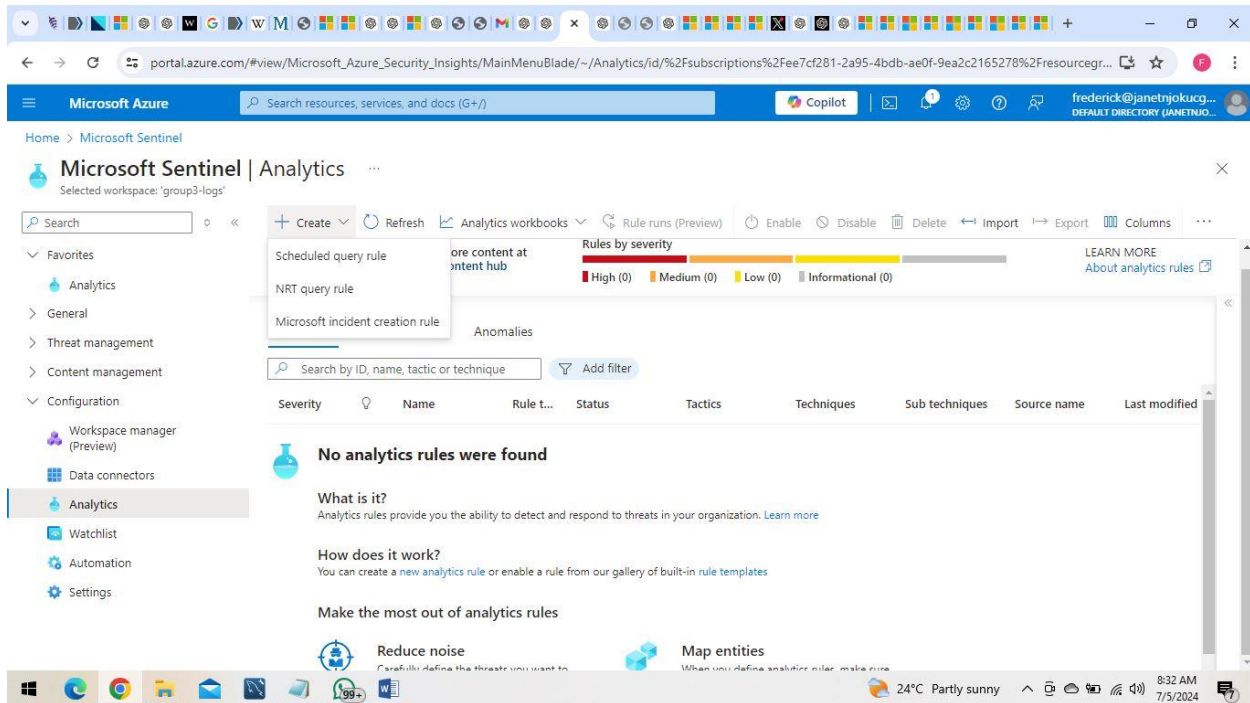
```
1 SigninLogs
2 | top 10 by TimeGenerated
3
```



Step 3: Configure analytic rules for your simulated attack scenario

Task 1: Configuring Analytic rule to detect a brute force attack scenario

1. Access Microsoft Sentinel:
 - Navigate to the Azure portal.
 - In the left-hand menu, select Microsoft Sentinel.
 - Choose the Sentinel workspace where you want to create the rule.
2. Go to Analytic Rules:
 - In the Sentinel workspace, select Configuration from the left-hand menu.
 - Click on Analytics.
3. Create a New Rule:
 - Click on + Create and choose Scheduled query rule.



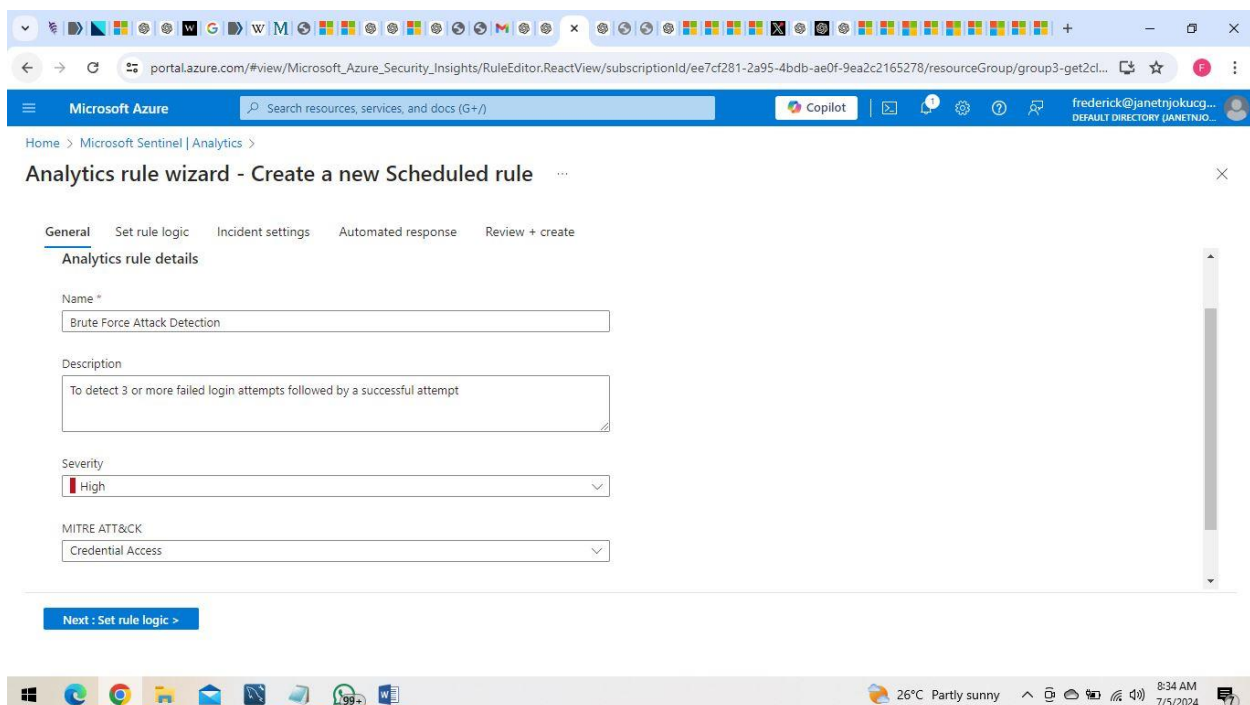
4. General Settings:

Name: Provide a name for your rule (Brute Force Attack Detection).

Description: Add a description to explain what the rule does.

Tactics: Select the MITRE ATT&CK tactics that this rule addresses (Credential access).

Severity: Choose the severity level (High).



5. Set the Rule Logic:

Rule Query: Enter or paste the Kusto Query Language (KQL) query that defines the logic for detecting the condition

```
let FailedLogins =  
SigninLogs  
| where ResultType != "0" // ResultType != 0 indicates a failed login  
| summarize FailedCount = count() by UserPrincipalName, bin(TimeGenerated, 10m)  
| where FailedCount >= 3;  
let SuccessfulLogins =  
SigninLogs  
| where ResultType == "0" // ResultType == 0 indicates a successful login  
| project UserPrincipalName, SuccessTime = TimeGenerated;  
FailedLogins  
| join kind=inner (SuccessfulLogins) on UserPrincipalName  
| where SuccessTime between (TimeGenerated .. TimeGenerated + 10m)  
| project UserPrincipalName, TimeGenerated, FailedCount, SuccessTime  
| order by TimeGenerated desc
```

Run Query: Click on the button to test your query and see the results.

Frequency: Set how often the query should run (30 mins) .

Lookup Period: Define the time range for data the query should analyze (5 hours)

6. Alert Settings:

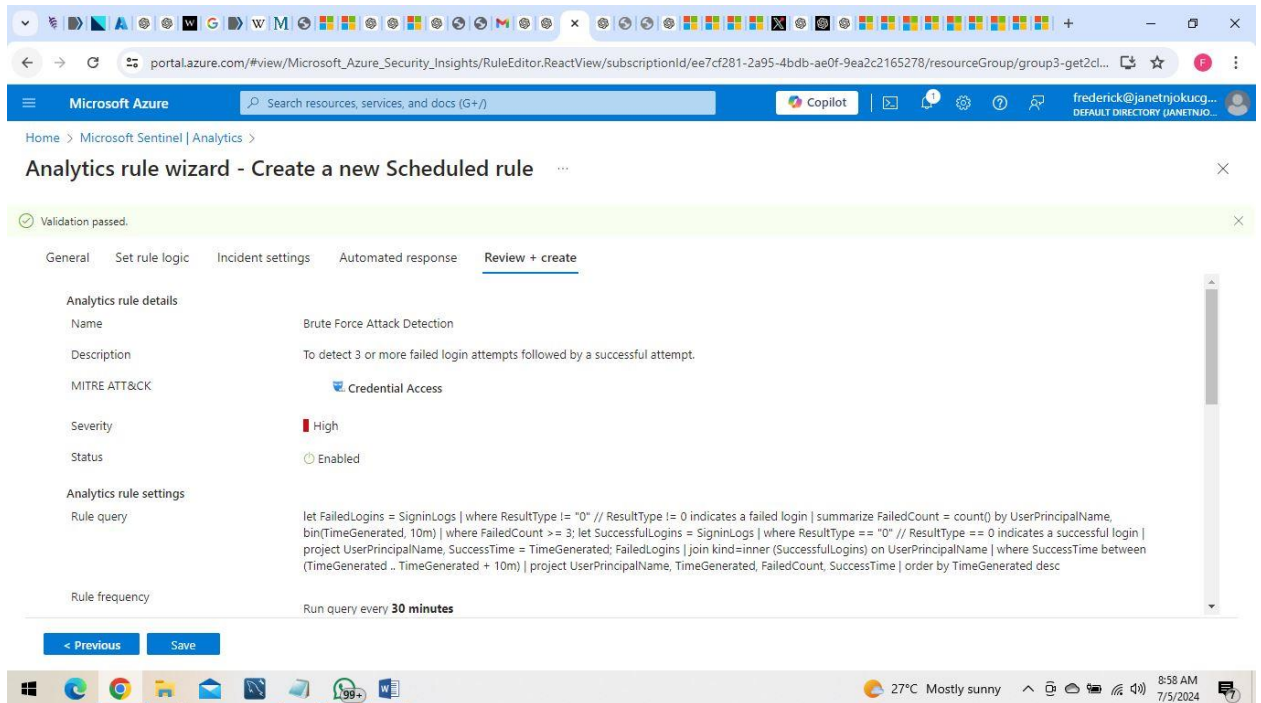
Event Grouping: Specify how events should be grouped together into a single incident (e.g., by IP address, account name, etc.).

Alert Threshold: Set the threshold that determines when an alert should be triggered (Greater than 0).

7. Incident Settings:

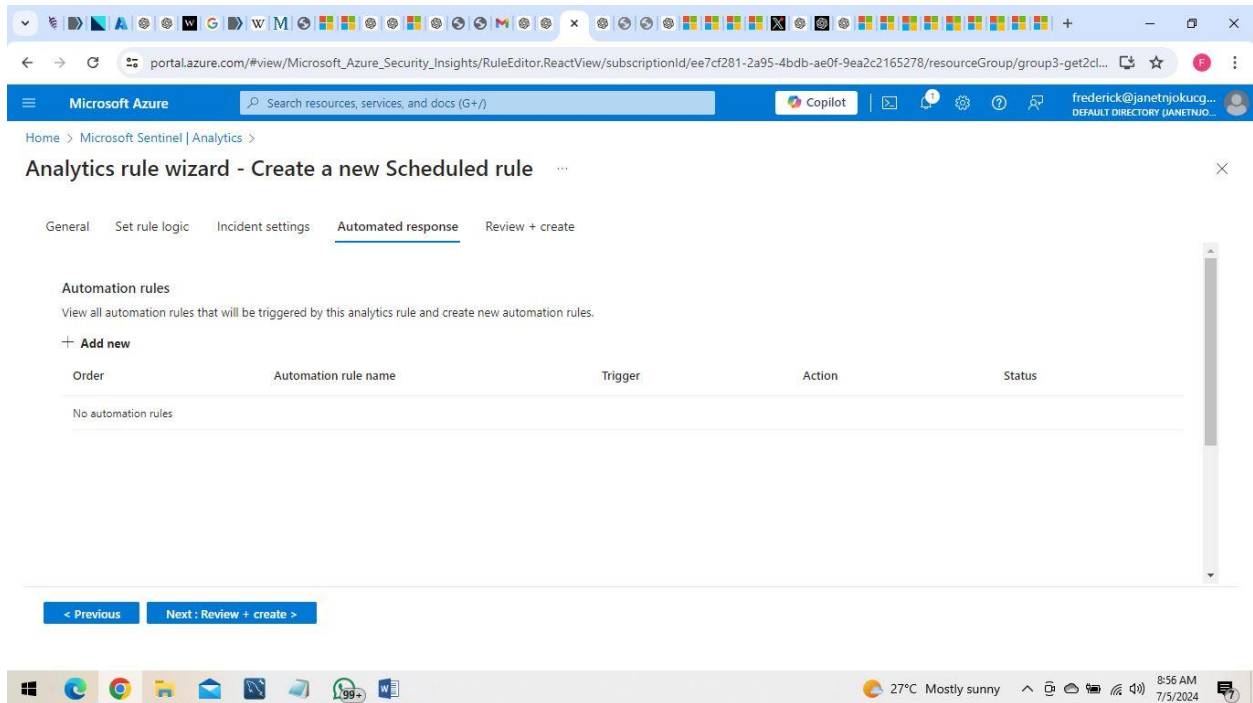
Create Incident: Enable this option if you want an incident to be created automatically when the rule triggers.

8. Review and create



Task 2. Configuring Analytic rule to detect multiple login into an account with different IP addresses within a time interval

1. Access Microsoft Sentinel:
 - Navigate to the Azure portal.
 - In the left-hand menu, select Microsoft Sentinel.
 - Choose the Sentinel workspace where you want to create the rule.
2. Go to Analytic Rules:
 - In the Sentinel workspace, select Configuration from the left-hand menu.
 - Click on Analytics.
3. Create a New Rule:
 - Click on + Create and choose Scheduled query rule.



4. General Settings:

Name: Provide a name for your rule (Multi login Group 3).

Description: Add a description to explain what the rule does.

Tactics: Select the MITRE ATT&CK tactics that this rule addresses (Credential access).

Severity: Choose the severity level (High).

5. Set the Rule Logic:

Rule Query: Enter or paste the Kusto Query Language (KQL) query that defines the logic for detecting the condition

```
let timeWindow = 10m; // Set the time window for detection
SigninLogs
| where ResultType == 0 // Filter for successful logins
| summarize IPCount = dcount(IPAddress), IPAddresses = make_set(IPAddress) by UserPrincipalName, bin(TimeGenerated, timeWindow)
| where IPCount > 1
| project UserPrincipalName, IPAddresses, TimeGenerated
```

Run Query: Click on the button to test your query and see the results.

Frequency: Set how often the query should run (30 mins).

Lookup Period: Define the time range for data the query should analyze (5 hours)

Alert Settings:

Event Grouping: Specify how events should be grouped together into a single incident (e.g., by IP address, account name, etc.).

Alert Threshold: Set the threshold that determines when an alert should be triggered (Greater than 0).

6. Incident Settings:

Create Incident: Enable this option if you want an incident to be created automatically when the rule triggers.

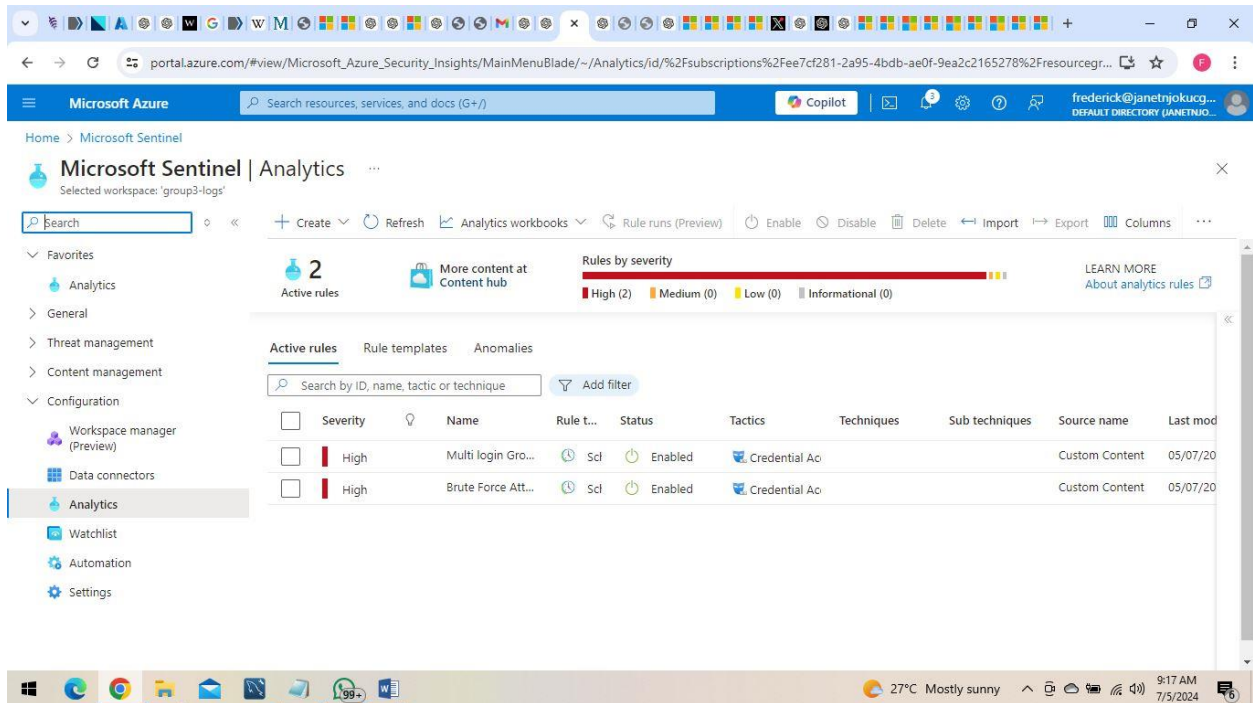
7. Review and create

The screenshot shows the Microsoft Azure portal interface for creating a new scheduled rule. The browser address bar shows the URL: `portal.azure.com/#view/Microsoft_Azure_Security_Insights/RuleEditor.ReactView/subscriptionId/ee7cf281-2a95-4bdb-ae0f-9ea2c2165278/resourceGroup/group3-get2cl...`. The page title is "Analytics rule wizard - Create a new Scheduled rule". A green banner at the top indicates "Validation passed".

The "Review + create" tab is active, showing the following details:

- Analytics rule details:**
 - Name: Multi login Group 3
 - Description: To detect multiple logins into an account within a 10 minute time frame from more than one IP address.
 - MITRE ATT&CK: Credential Access
 - Severity: High
 - Status: Enabled
- Analytics rule settings:**
 - Rule query: `let timeWindow = 10m; // Set the time window for detection SigninLogs | where ResultType == 0 // Filter for successful logins | summarize IPCount = dcount(IPAddress), IPAddresses = make_set(IPAddress) by UserPrincipalName, bin(TimeGenerated, timeWindow) | where IPCount > 1 | project UserPrincipalName, IPAddresses, TimeGenerated`
 - Rule frequency: Run query every 30 minutes

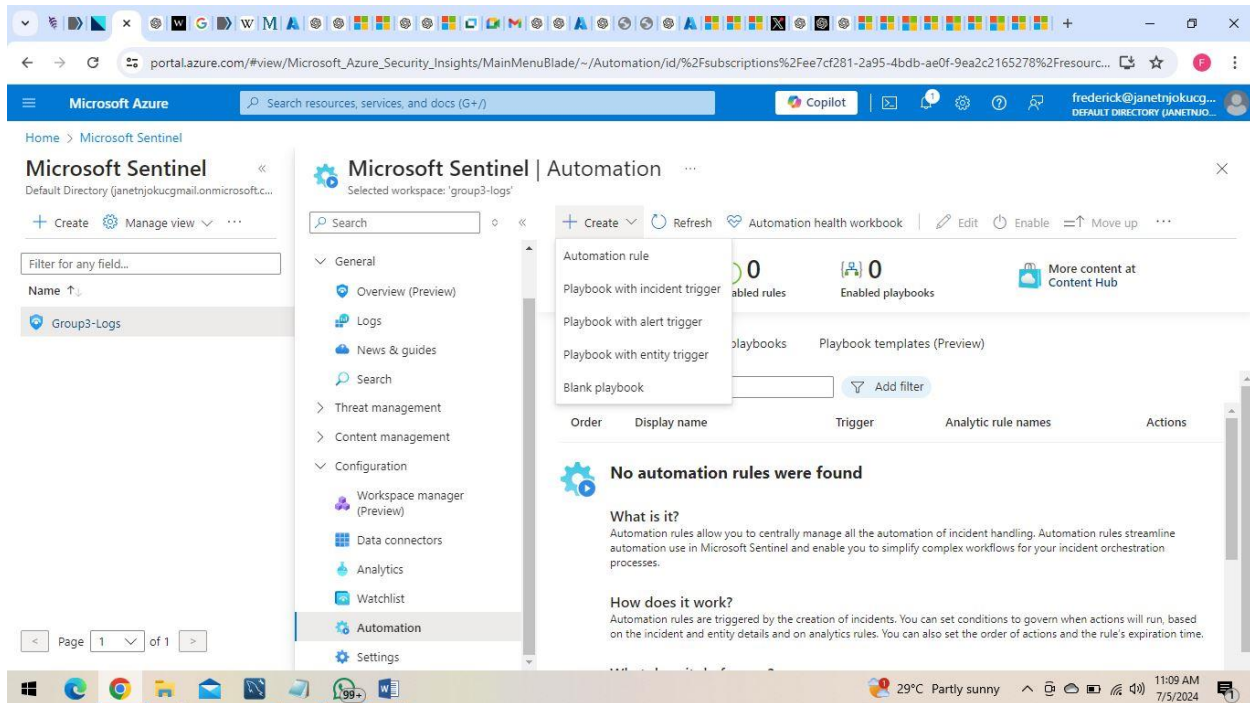
At the bottom, there are buttons for "< Previous" and "Save". The Windows taskbar at the bottom shows the time as 9:16 AM on 7/5/2024, with a weather forecast of 27°C Mostly sunny.



Step 4: Automate Incident Response

Task 1: Create an automation rule to automatically tag and assign incidents based on specific criteria.

1. Access Microsoft Sentinel:
 - Log in to the Azure portal.
 - Navigate to Microsoft Sentinel from the list of services.
2. Navigate to Automation:
 - In the Microsoft Sentinel workspace, go to the "Automation" section in the left-hand menu.
3. Create a New Automation Rule:
 - Click on "+ Add new rule" to create a new automation rule.



4. Define Rule Name and Description:

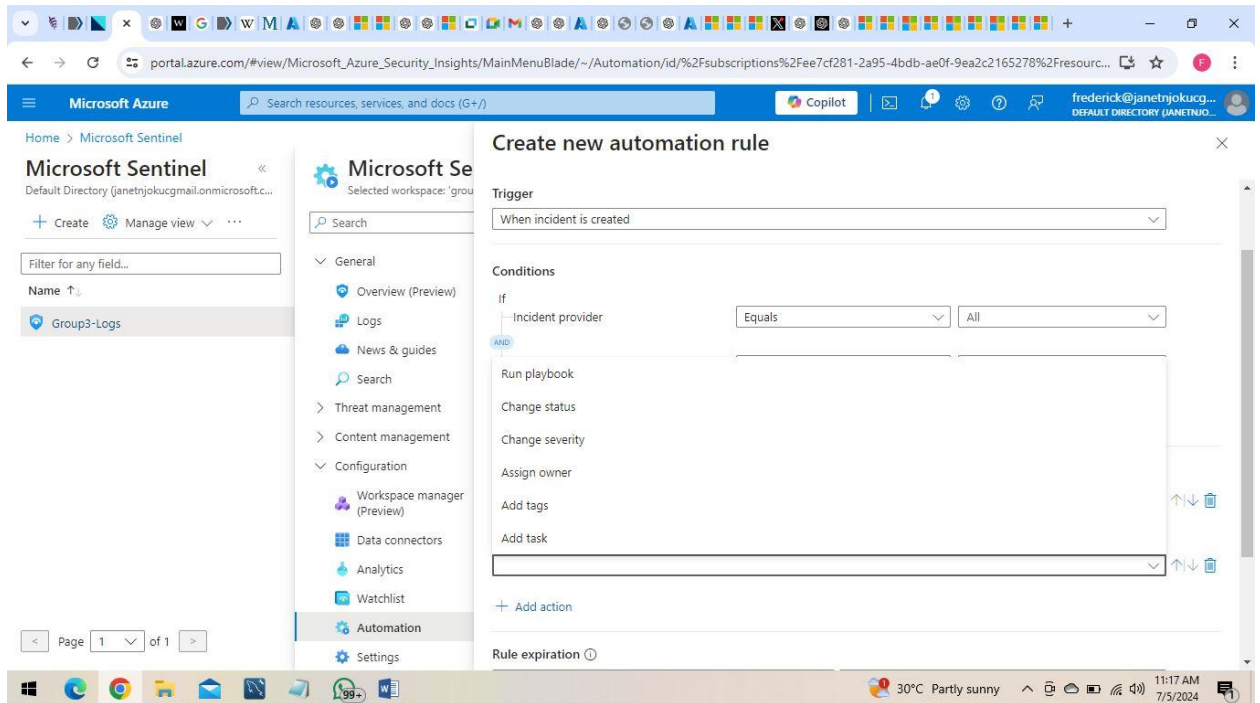
Provide a name (Group 3 automation rule) and description for the automation rule to identify its purpose.

5. Set Rule Logic:

Trigger: Specify the trigger condition. For example, you might want to trigger the rule when an incident is created or updated.

Criteria: Define the criteria for the rule based on various parameters such as severity, incident type, tags, entities, etc.

- Example: If you want to tag and assign incidents with a specific severity level, set the criteria to match incidents with that severity.



6. Add Actions:

Tag Incident: To automatically tag an incident, use the "Add a tag" action. Specify the tag you want to add.

Assign Incident: To assign the incident to a specific user or group (Get2cloud group 3), use the "Assign incident" action. Specify the assignee.

portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade~/Automation/id/%2Fsubscriptions%2Fee7cf281-2a95-4bdb-ae0f-9ea2c2165278%2Fresourc...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

frederick@janetnjokucg...
DEFAULT DIRECTORY (JANETNJOKUCG...)

Home > Microsoft Sentinel

Microsoft Sentinel
Default Directory (janetnjokucg@mail.onmicrosoft.c...)

+ Create Manage view ...

Filter for any field...

Name ↑

Group3-Logs

Page 1 of 1

Microsoft Sentinel
Selected workspace: 'grou...

Search

General

- Overview (Preview)
- Logs
- News & guides
- Search
- Threat management
- Content management
- Configuration
- Workspace manager (Preview)
- Data connectors
- Analytics
- Watchlist
- Automation
- Settings

Create new automation rule

AND

Analytic rule name

Contains

All

+ Add

Actions

And then

Run playbook

Change status

Change severity

Assign owner

Add tags

Add task

Apply Cancel

30°C Partly sunny 11:18 AM 7/5/2024

portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade~/Automation/id/%2Fsubscriptions%2Fee7cf281-2a95-4bdb-ae0f-9ea2c2165278%2Fresourc...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

frederick@janetnjokucg...
DEFAULT DIRECTORY (JANETNJOKUCG...)

Home > Microsoft Sentinel

Microsoft Sentinel
Default Directory (janetnjokucg@mail.onmicrosoft.c...)

+ Create Manage view ...

Filter for any field...

Name ↑

Group3-Logs

Page 1 of 1

Microsoft Sentinel
Selected workspace: 'grou...

Search

General

- Overview (Preview)
- Logs
- News & guides
- Search
- Threat management
- Content management
- Configuration
- Workspace manager (Preview)
- Data connectors
- Analytics
- Watchlist
- Automation
- Settings

Create new automation rule

AND

Analytic rule name

Contains

All

+ Add

Actions

And then

Add tags

Add tag

Suspicious login

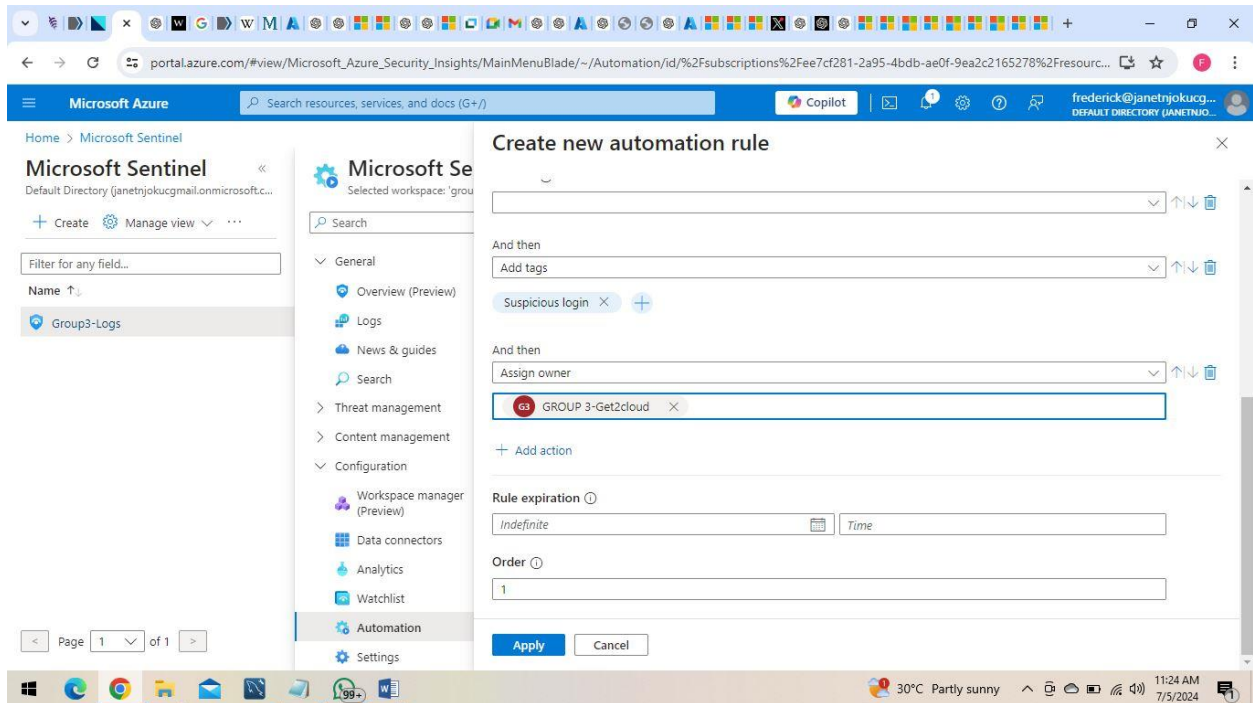
Apply Cancel

Time

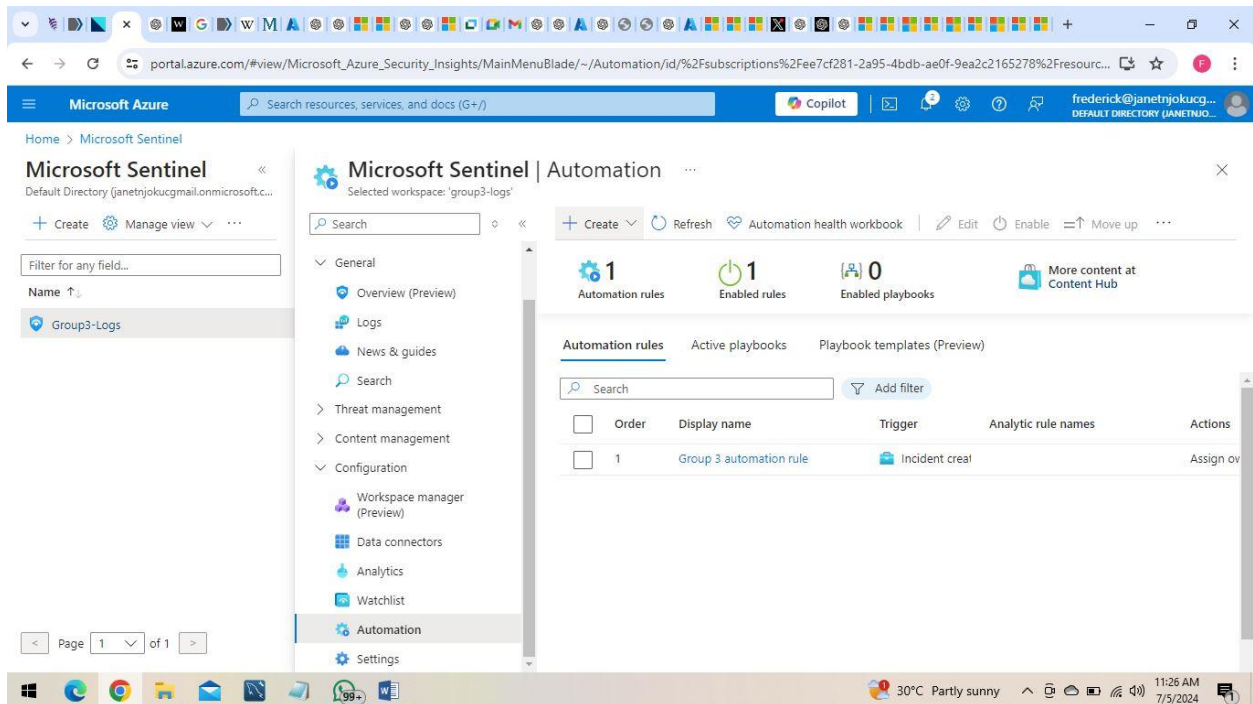
Order

1

30°C Partly sunny 11:20 AM 7/5/2024



7. Save the Automation Rule:
Review the settings and criteria.
Click "Save" to create the automation rule.



Task 2. Create a playbook to send email alerts to designated recipients when an incident is detected.

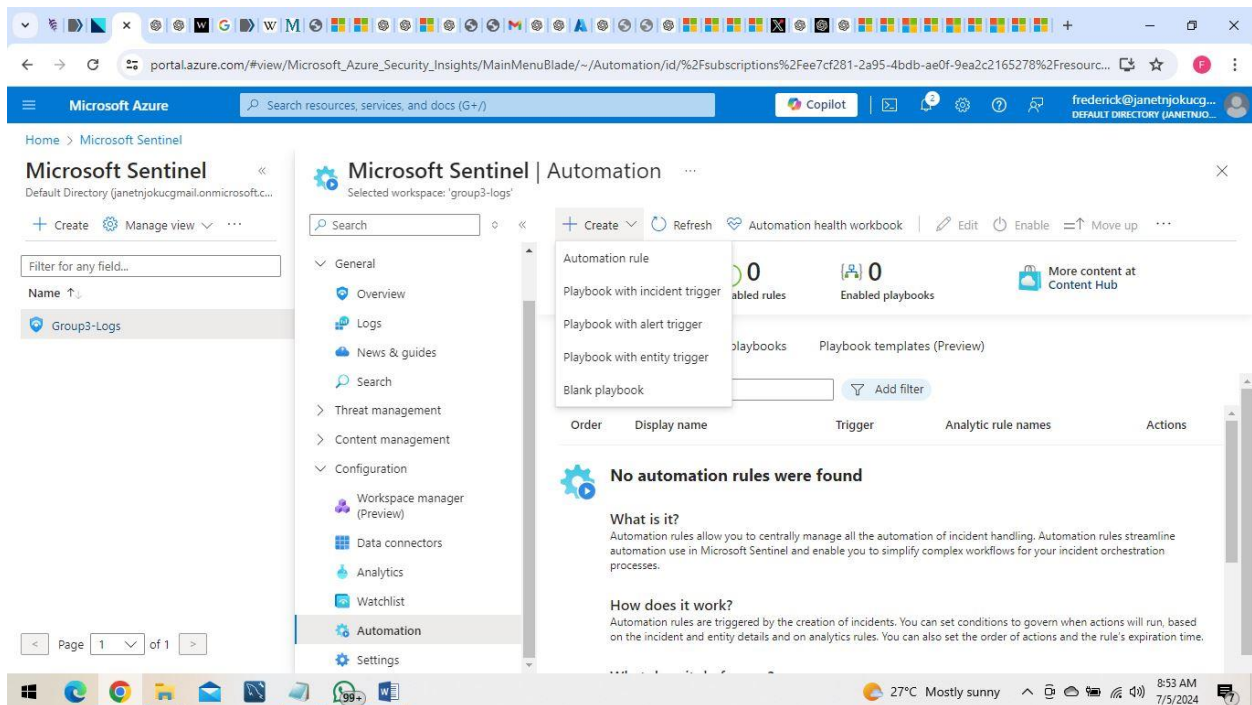
1. Create a Playbook (Group3playbook):

Navigate to Microsoft Sentinel > Automation > Playbooks > "+ Create".

Click on blank playbook. This takes you to a page where you create a Logic app.

Fill in the necessary details (Subscription, Resource Group, Logic App Name ,

Region) and click "Review + create" and then "Create"



2. Design the Logic App Workflow:

Once the Logic App is created, go to the Logic App Designer.

Microsoft Azure portal showing the "Create Logic App" wizard. The subscription is "Microsoft Azure Sponsorship" and the resource group is "GROUP3-Get2cloudRG". The instance details include "Logic App name" (Group3Playbook), "Region" (UK South), "Enable log analytics" (Yes), and "Log Analytics workspace" (Group3-Logs). The plan type is "Standard".

Subscription *

Resource Group *

Instance Details

Logic App name *

Region *

Enable log analytics * ☒ Yes ☐ No

Log Analytics workspace *

Plan

The plan type you choose dictates how your app scales, what features are enabled, and how it is priced. [Learn more](#)

Plan type * ☐ Standard: Best for enterprise-level, serverless applications, with event-based scaling and networking isolation.

[Review + create](#) [< Previous](#) [Next : Tags >](#)

Microsoft Azure portal showing the "Overview" page for the deployment "Microsoft.Web-LogicAppConsumption-Portal-0e85abe4-9f84". The deployment is complete, with a start time of 05/07/2024, 11:38:47. The deployment details include the subscription "Microsoft Azure Sponsorship" and the resource group "GROUP3-Get2cloudRG".

Deployment name: Microsoft.Web-LogicAppConsumption-Portal-0e85abe4-9f84

Subscription: Microsoft Azure Sponsorship

Resource group: GROUP3-Get2cloudRG

Start time: 05/07/2024, 11:38:47

Correlation ID: 2978a7fc-6af3-457c-9079-e54ea98

Deployment details

Next steps

Setup log analytics for your app. Recommended

[Go to resource](#)

Give feedback

[Tell us about your experience with deployment](#)

Cost Management

Get notified to stay within your budget and prevent unexpected charges on your bill.

[Set up cost alerts >](#)

Microsoft Defender for Cloud

Secure your apps and infrastructure

[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials

[Start learning today >](#)

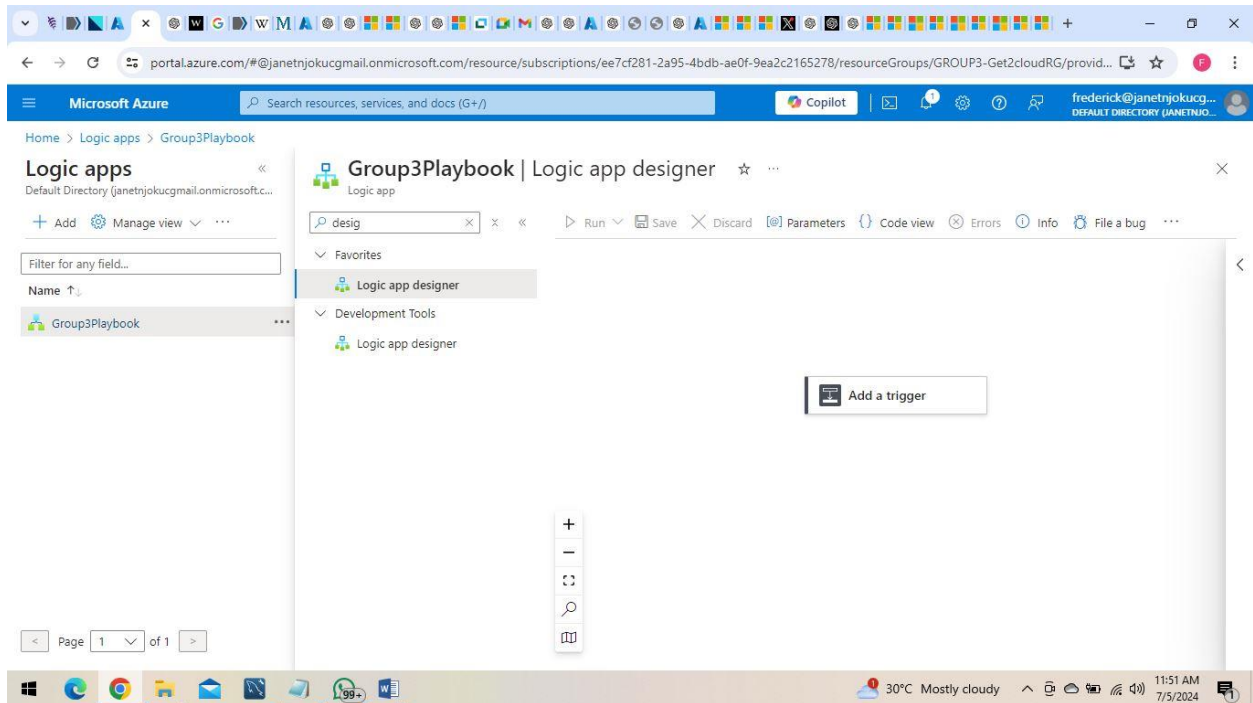
Work with an expert

Azure experts are service provider partners who can help manage your Azure environment.

3. Add a Trigger:

In the designer, click "Add a trigger".

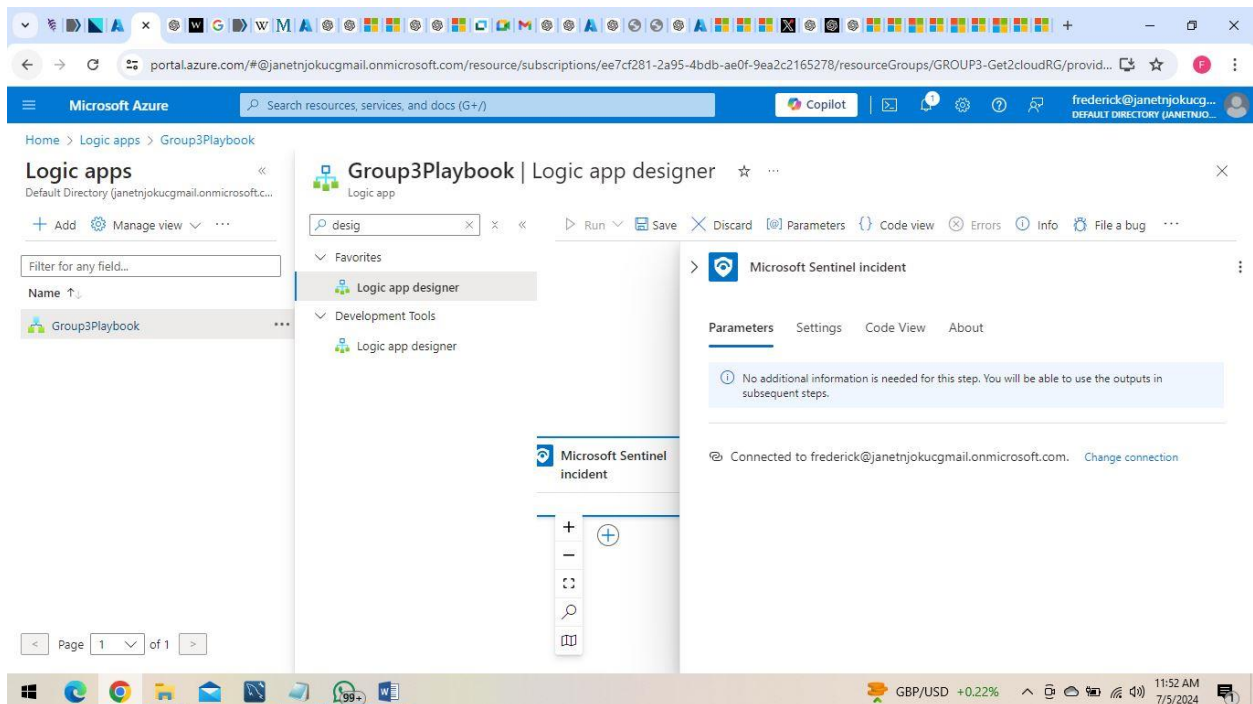
Search for "Microsoft Sentinel" and choose "Microsoft Sentinel incident trigger"



4. Configure the Trigger:

Select the appropriate Azure Sentinel instance.

Configure the trigger with the relevant criteria for the incidents you want to act upon

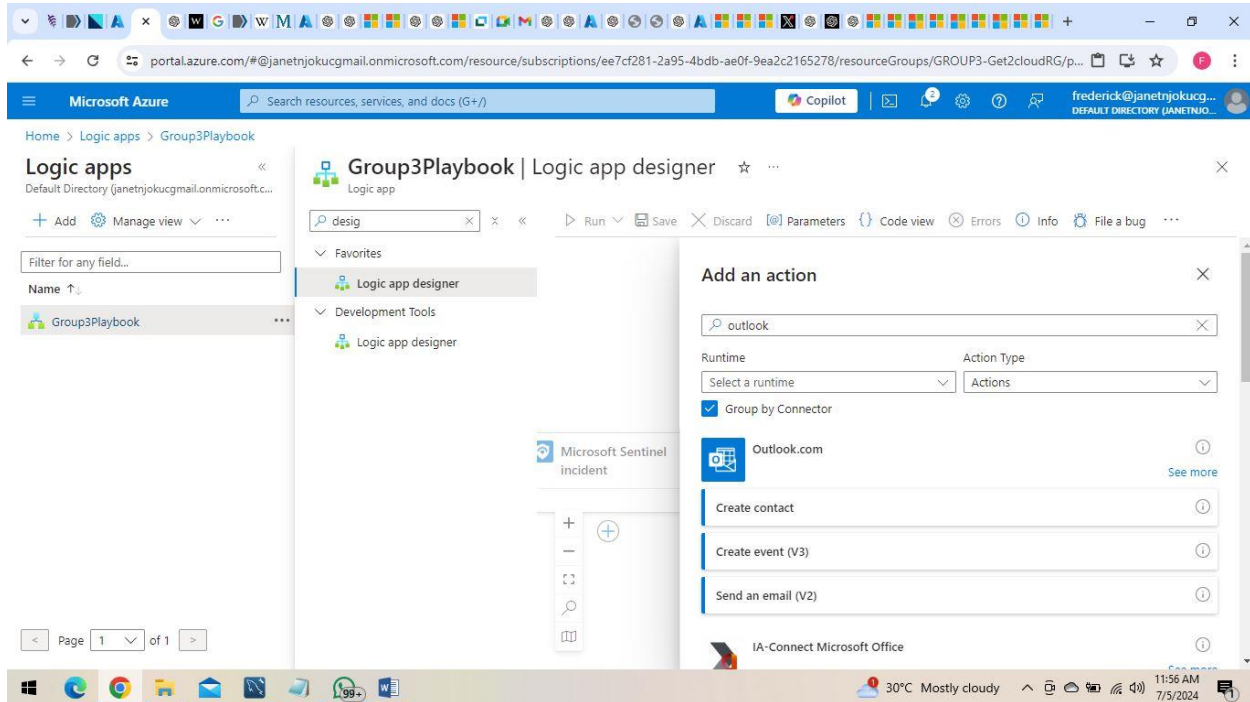


5. Add an Action for Email:

After the trigger, add a new step by clicking on "New step".

Search for and select an email connector (e.g., Office 365 Outlook, SMTP, SendGrid).

Choose the action "Send an email (V2)" for Office 365 Outlook or a similar action for other email services.



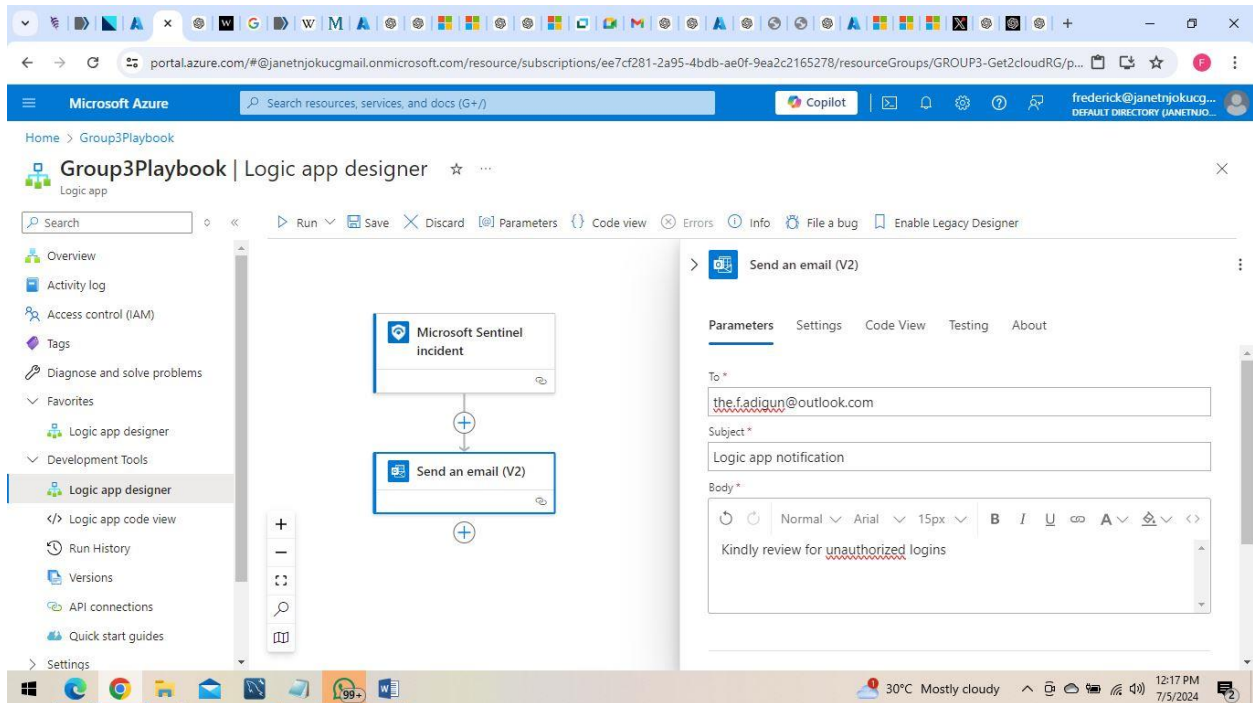
6. Configure the Email Action:

Fill in the necessary details such as:

To: Specify the email addresses of the recipients.

Subject: Provide a subject for the email, you can use dynamic content from the incident.

Body: Write the email body and use dynamic content to include details from the Sentinel incident.



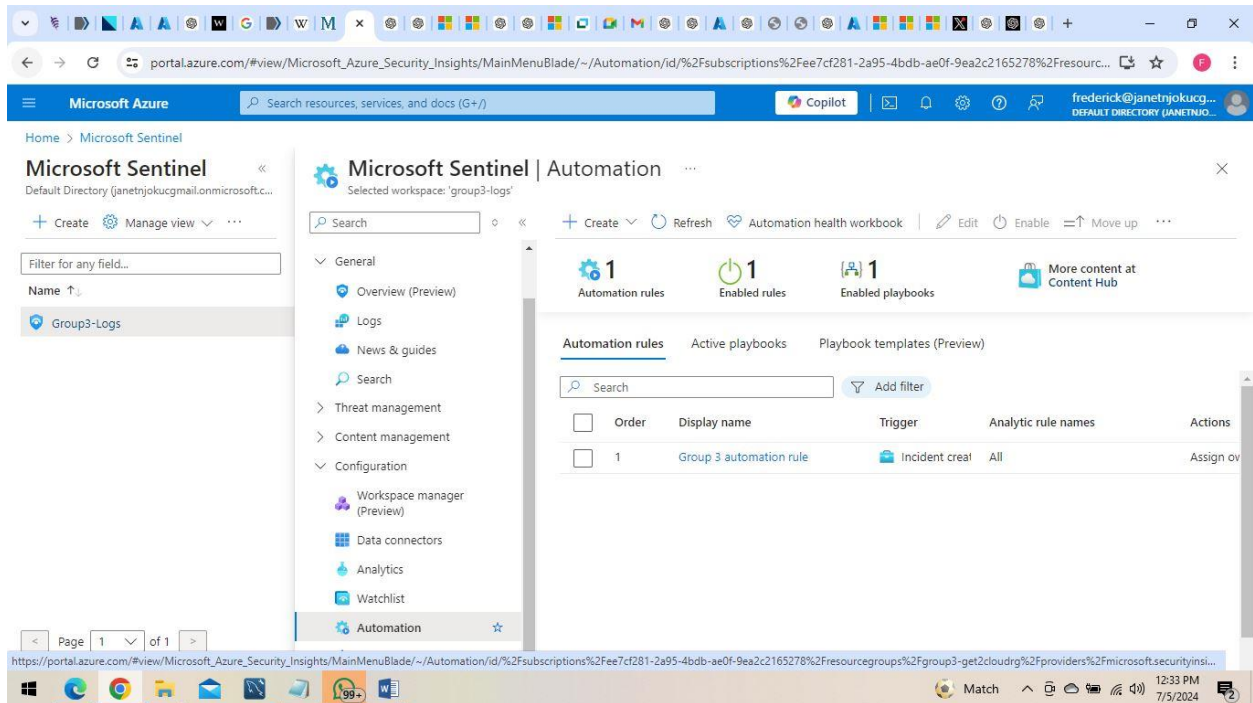
7. Save the Logic App: Click on "Save" to save your logic app

8. Link Playbook to Automation Rule:

In your automation rule earlier created (Group 3 automation rule), add an action to the rule and select "Run playbook" to run the Playbook you created (Group 3 Playbook).

Click on "apply" to effect the configuration

Go back to the Automation Tab to confirm the Playbook has been enabled.



9. Test the Workflow:

Create a test incident (e.g., Brute force attack) in Azure Sentinel to see if the Logic App triggers and sends an email as expected.

Check the run history in the Logic App to debug any issues if the email is not sent.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

fredenck@janetnjokucg...
DEFAULT DIRECTORY (JANETNJOKUCG...)

Home > Microsoft Sentinel

Microsoft Sentinel
Default Directory (janetnjokucg@mail.onmicrosoft.c...)

Create

Manage view

Filter for any field...

Name ↑

Group3-Logs

Logs

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Configuration

Microsoft Sentinel | Incidents

Selected workspace: 'group3-logs'

Create incident (Preview)

Refresh

Last 24 hours

Actions

Delete

30

Open incidents

30

New incidents

0

Active incidents

Open incidents by severity

High (30) Medium (0) Low (0) Informational (0)

Search by ID, title, tags, owner or product

Severity: All

Status: 2 selected

More (3)

Auto-refresh incidents

Severity ↑↓	Incident number ↑↓	Title ↑↓	Alerts	Incident provider n
High	210	Brute Force Attack ...	1	Azure Sentinel
High	209	Brute Force Attack ...	1	Azure Sentinel
High	208	Multi login Group 3	1	Azure Sentinel
High	207	Brute Force Attack ...	1	Azure Sentinel
High	206	Multi login Group 3	1	Azure Sentinel
High	205	Brute Force Attack ...	1	Azure Sentinel

< Previous 1 - 30 Next >

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

fredenck@janetnjokucg...
DEFAULT DIRECTORY (JANETNJOKUCG...)

Home > Microsoft Sentinel

Microsoft Sentinel
Default Directory (janetnjokucg@mail.onmicrosoft.c...)

Create

Manage view

Filter for any field...

Name ↑

Group3-Logs

Logs

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Configuration

Microsoft Sentinel | Incidents

Selected workspace: 'group3-logs'

Create incident (Preview)

Refresh

Last 24 hours

Actions

Delete

30

Open incidents

30

New incidents

0

Active incidents

Open incidents by severity

High (30) Medium (0) Low (0) Informational (0)

Search by ID, title, tags, owner or product

Severity: All

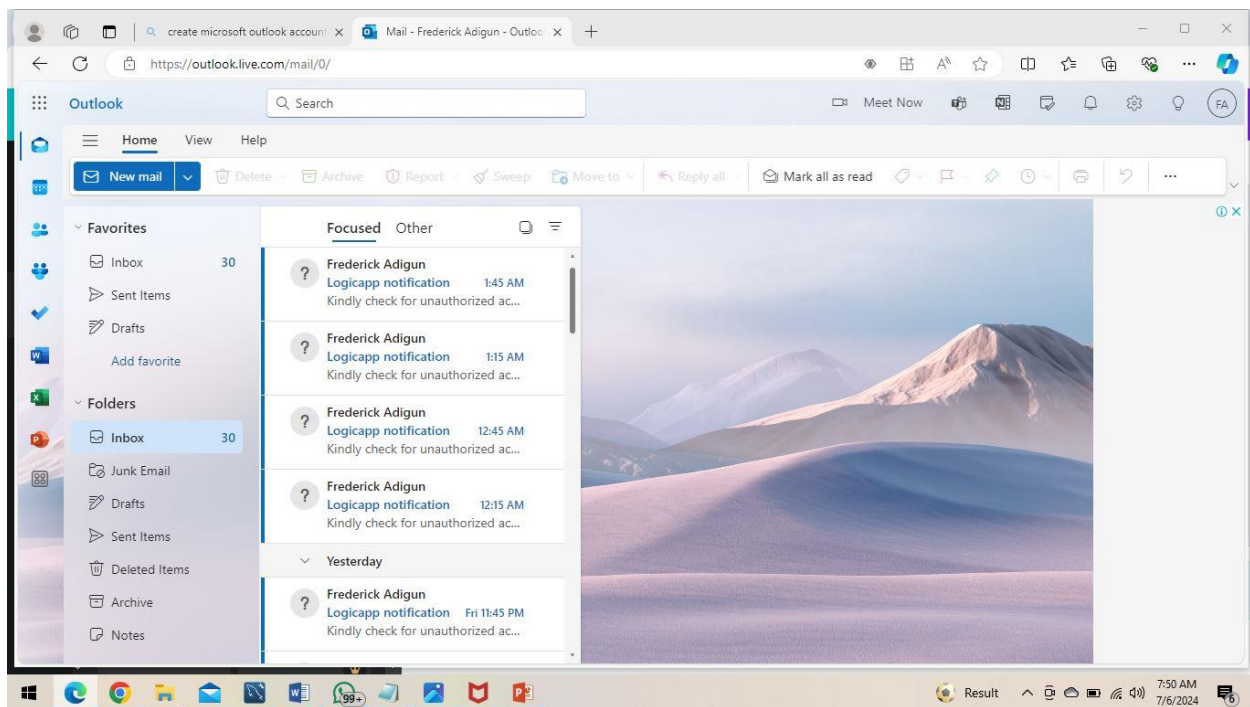
Status: 2 selected

More (3)

Auto-refresh incidents

ID time ↑↓	Last update time ↑↓	Owner ↑↓	Status ↑↓	Tags
24, 23:45	05/07/24, 23:45	GROUP 3-Get2cloud	New	Suspicious login
24, 21:30	05/07/24, 21:30	GROUP 3-Get2cloud	New	Suspicious login
24, 21:15	05/07/24, 21:15	GROUP 3-Get2cloud	New	Suspicious login
24, 21:00	05/07/24, 21:00	GROUP 3-Get2cloud	New	Suspicious login
24, 20:45	05/07/24, 20:45	GROUP 3-Get2cloud	New	Suspicious login

< Previous 1 - 30 Next >



Here are the detailed steps for implementing Microsoft Sentinel to enable real-time threat monitoring and incident response. I hope you find them useful.