


# INTRODUCTION

Security Information and Event Management (SIEM) solutions play a crucial role in monitoring and securing IT infrastructure.

This project focuses on deploying Microsoft Sentinel in Microsoft Azure to monitor successful login attempts on a Virtual Machine (VM).

By integrating the VM with Sentinel, security logs can be collected, analyzed, and monitored for real-time threat detection and investigation.



# PROJECT OBJECTIVES

- Deploy and configure Microsoft Sentinel as a SIEM solution.
- Set up an Azure Virtual Machine (VM) for monitoring.
- Create a Log Analytics workspace and integrate Sentinel.
- Define a data collection rule to track successful login events.
- Generate and analyze security alerts based on log activity.
- Enhance security visibility using Sentinel's monitoring tools.

# METHODOLOGY

## Step 1: Azure Account Registration

- Created an Azure account and accessed the Azure Portal.

## Step 2: Virtual Machine (VM) Deployment

- Configured a Windows VM in Azure.
- Set up appropriate networking and firewall rules.



# STEP 1 AND 2 SCREENSHOTS

Private

portal.azure.com

Search resources, services, and docs (G+)

Copilot

Home > Virtual machines >

Create a virtual machine

Help me create a low cost VMHelp me create a VM optimized for high availabilityHelp me choose the right VM size for my workload

Create new

Instance details

Virtual machine name \* ⓘogscriptkiddie✓

Region \* ⓘ(Canada) Canada Central✓

Availability options ⓘAvailability zone✓

Zone options ⓘ

Self-selected zone

Choose up to 3 availability zones, one VM per zone

Azure-selected zone (Preview)

Let Azure assign the best zone for your needs

Availability zone \* ⓘZone 1✓

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘTrusted launch virtual machines✓

[Configure security features](#)

Trusted launch virtual machine is required when using 1P Gallery images.

Image \* ⓘ

Windows 11 Pro, version 24H2 - x64 Gen2

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ

Arm64

x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ☐

Size \* ⓘStandard\_D2s\_v3 - 2 vcpus, 8 GiB memory (US\$81.03/month)✓

[See all sizes](#)

Enable Hibernation ⓘ☐

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more](#)

Administrator account

< Previous

Next : Disks >

Review + create

Estimated monthly costs ⓘ

Costs indicated here are estimates only. Pricing may vary depending on your Microsoft agreement, date of purchase, subscription type, usage costs, licensing and currency exchange rates. Total costs may include other resource costs, licensing and subscription implications. This feature may have limited or restricted functionality, but is made available on a preview basis for evaluation and feedback.

[Give feedback about your estimate experience](#)

Basics

Virtual machineUS\$81.03

ImageUS\$0.00

Windows 11 Pro, version 24H2

Windows BYOL applied ⓘ

SizeUS\$81.03

Standard\_D2s\_v3

Disks

Networking

Management

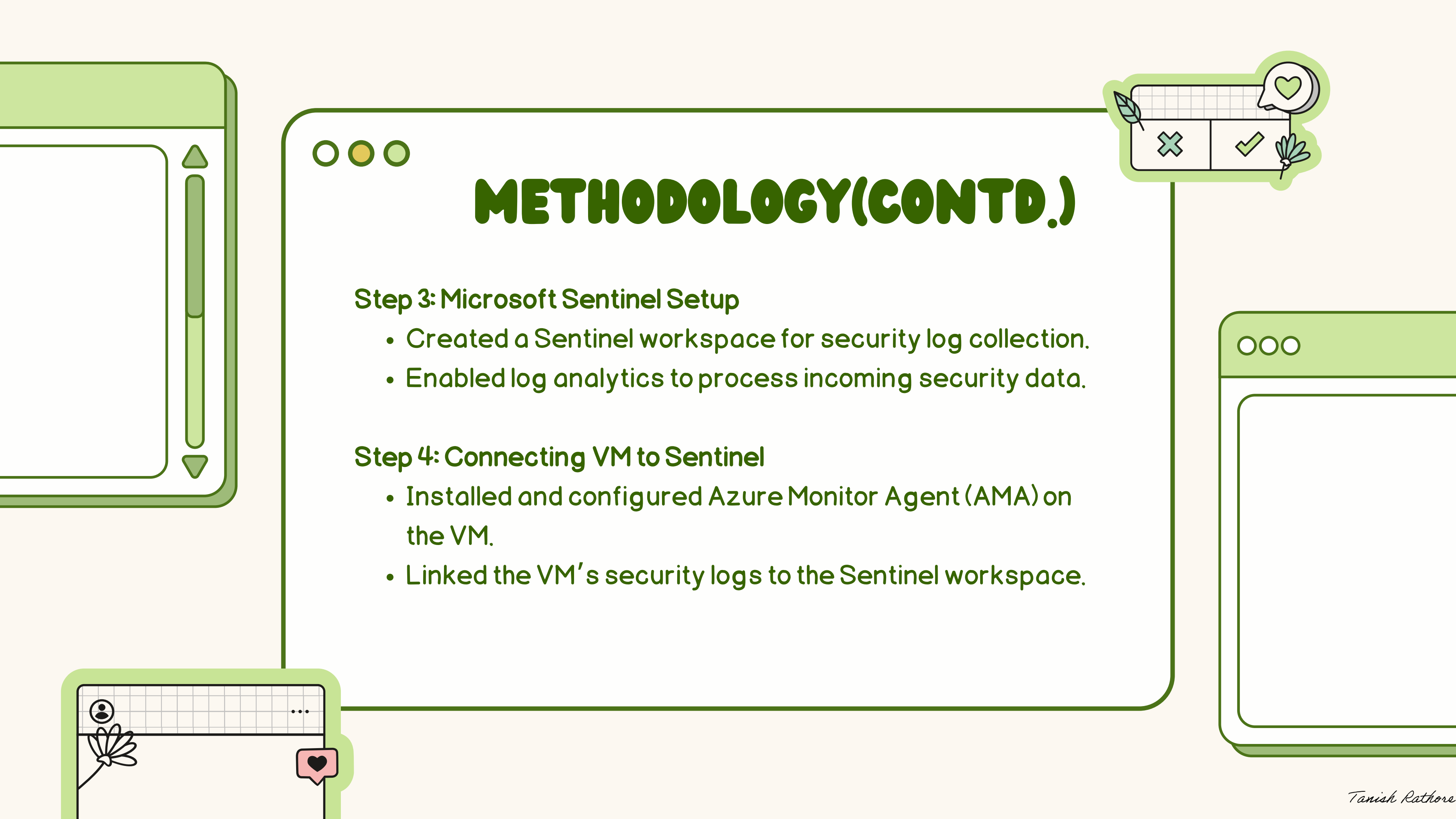
Monitoring

Advanced

Estimated monthly cost

US\$100.74

[Give feedback](#)



## METHODOLOGY(CONTD.)

### Step 3: Microsoft Sentinel Setup

- Created a Sentinel workspace for security log collection.
- Enabled log analytics to process incoming security data.

### Step 4: Connecting VM to Sentinel

- Installed and configured Azure Monitor Agent (AMA) on the VM.
- Linked the VM's security logs to the Sentinel workspace.



Microsoft Azure

Home > Microsoft Sentinel

Add Microsoft Sentinel to a workspace

Create a new workspace

Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

Workspace	Location	ResourceGroup	Subscription	Directory
ogscriptkiddle-LogAnalytics	canadacentral	ogscriptkiddle_group	Azure subscription 1	Default Directory

Notifications

More events in the activity log

Adding Microsoft Sentinel

Running

Adding Microsoft Sentinel to workspace 'ogscriptkiddle-LogAnalytics' was successful.

Go to resource

Pin to dashboard

3 minutes ago

Deployment succeeded

Deployment 'CreateVm-microsoftwindowsdesktop.windows-11-win11-20250212163805' to resource group 'ogscriptkiddle\_group' was successful.

Pin to dashboard

Go to resource group

5 minutes ago

Microsoft Azure

Home > Microsoft Sentinel

Microsoft Sentinel

Default Directory

Create

Manage view

Filter for any field...

ogscriptkiddle-LogAnalytics

Microsoft Sentinel | Data connectors

Selected workspace: 'ogscriptkiddle-loganalytics'

Search

Refresh

Guides & Feedback

Device specific AMA connectors have been deprecated. [Learn more](#)

2 Connectors

0 Connected

More content at Content Hub

Search by name or provider

Providers: Microsoft

Data Types: SecurityEvents

Status: Not connected (2)

Security Events via Legacy Agent

Windows Security Events via AMA

# STEP 3 AND 4 SCREENSHOTS

Tanish Rathore

Microsoft Azure

Home > Microsoft Sentinel | Data connectors

Content hub

Refresh

Install/Update

Delete

SIEM Migration

Guides & Feedback

382 Solutions

307 Standalone contents

0 Installed

0 Updates

Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. [Learn more](#)

windows security events

Status: All

Content type: Data connector (295)

Support: All

Provider: All

Category: All

Content sources: All

Content title	Status	Content source	Provider	Support	Category	Content type
Windows Security Events	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection	Analytics rule (20) Data connector
Windows Security Events via AMA	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection	Data connector
Security Events via Legacy Agent	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection	Data connector
Windows Firewall	Not installed	Solution	Microsoft	Microsoft	Security - Network	Data connector (2) Workbook
Windows Firewall Events via AMA	Not installed	Solution	Microsoft	Microsoft	Security - Network	Data connector
Windows Firewall	Not installed	Solution	Microsoft	Microsoft	Security - Network	Data connector
Windows Forwarded Events	Not installed	Solution	Microsoft	Microsoft	IT Operations	Analytics rule (2) Data connector
Windows Forwarded Events	Not installed	Solution	Microsoft	Microsoft	IT Operations	Data connector
Windows Server DNS	Not installed	Solution	Microsoft	Microsoft	Networking	Analytics rule (5) Data connector
Windows DNS Events via AMA	Not installed	Solution	Microsoft	Microsoft	Networking	Data connector
DNS	Not installed	Solution	Microsoft	Microsoft	Networking	Data connector
Microsoft Exchange Security for Exch...	Not installed	Solution	Microsoft	Community	Application	Analytics rule (2) Data connector
Microsoft Exchange Logs and Events	Not installed	Solution	Microsoft	Community	Application	Data connector
ARGOS Cloud Security	Not installed	Solution	ARGOS Cloud S...	ARGOS Cloud S...	Security - Cloud Security	Analytics rule Data connector +1
ARGOS Cloud Security	Not installed	Solution	ARGOS Cloud S...	ARGOS Cloud S...	Security - Cloud Security	Data connector

Windows Security Events

Microsoft Provider

Microsoft Support

3.0.9 Version

Description

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

Review the solution [Release Notes](#)

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

1. Windows Security Events via AMA - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). Microsoft recommends using this Data Connector.

2. Security Events via Legacy Agent - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by Aug 31, 2024, and thus should only be installed where AMA is not supported.

Data Connectors: 2, Workbooks: 2, Analytic Rules: 20, Hunting Queries: 50

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type

20 Analytics rule

2 Data connector

50 Hunting query

2 Workbook

Category

Security - Threat Protection

Principles

Microsoft Azure

Home > Microsoft Sentinel

Microsoft Sentinel | Overview

Selected workspace: 'ogscriptkiddle-loganalytics'

Search

Refresh

General

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Summary rules (Preview)

Watchlist

Automation

Settings

Incidents (0)

Last 24 hours

No incidents found

See incidents page for further information

Incidents

Automation

Last 24 hours

No automation rules found

Add automation rules to centrally manage automation of incident handling and response

Automation

Data

Last 24 hours

No data connectors found

Add data connectors to ingest data into Microsoft Sentinel

Data connectors

Analytics

Current status

1 Analytics rules

0 Disabled

0 Auto disabled

1 Enabled

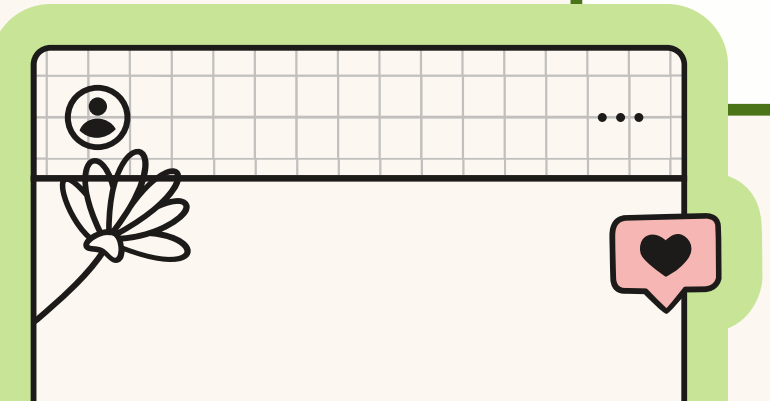


# METHODOLOGY(CONTD.)

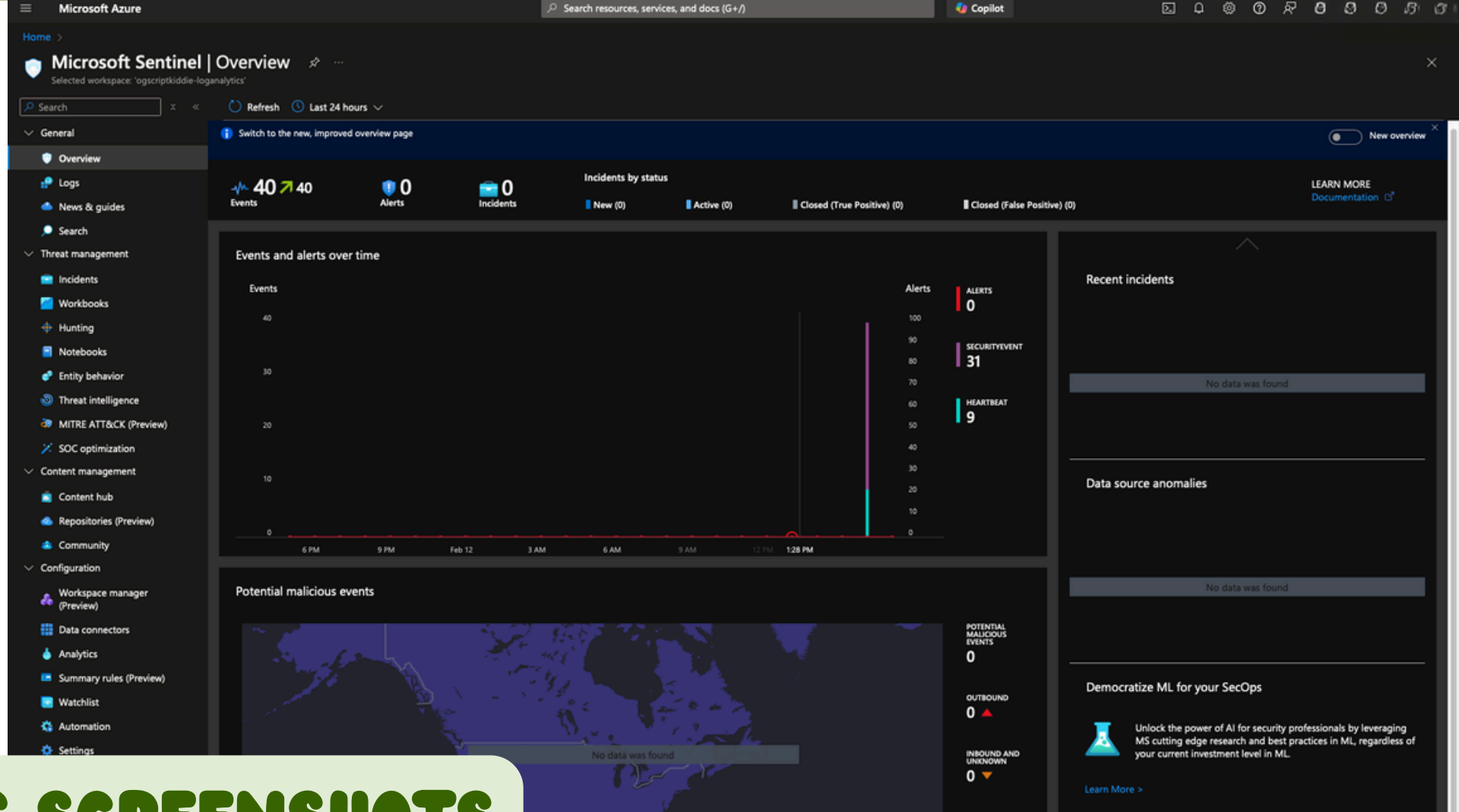
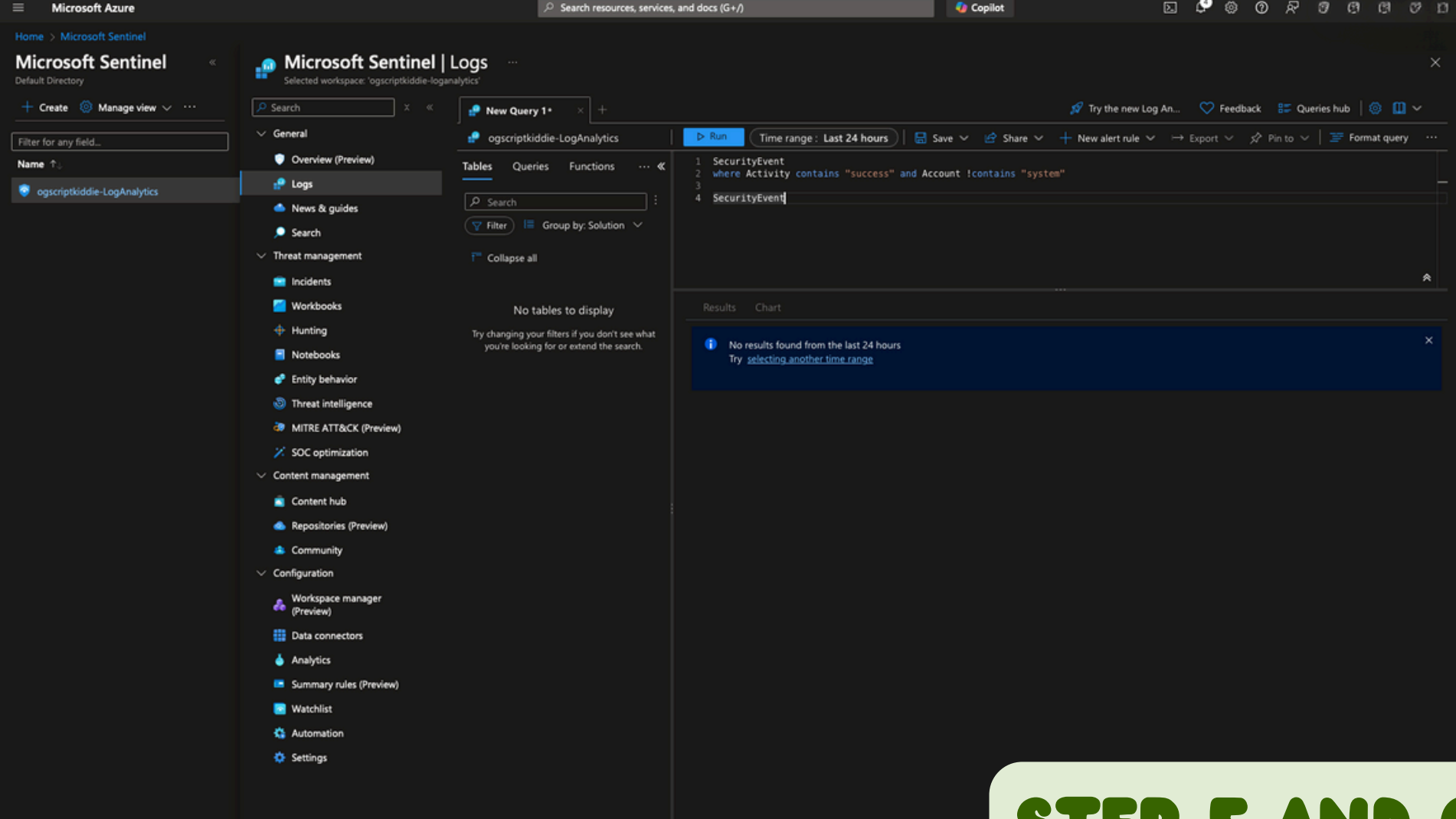
## Step 5: Creating Data Collection Rules

- Defined a log rule to capture successful login attempts.
- Configured alerts to trigger notifications on login events.

## Step 6: Monitoring and Alert Investigation

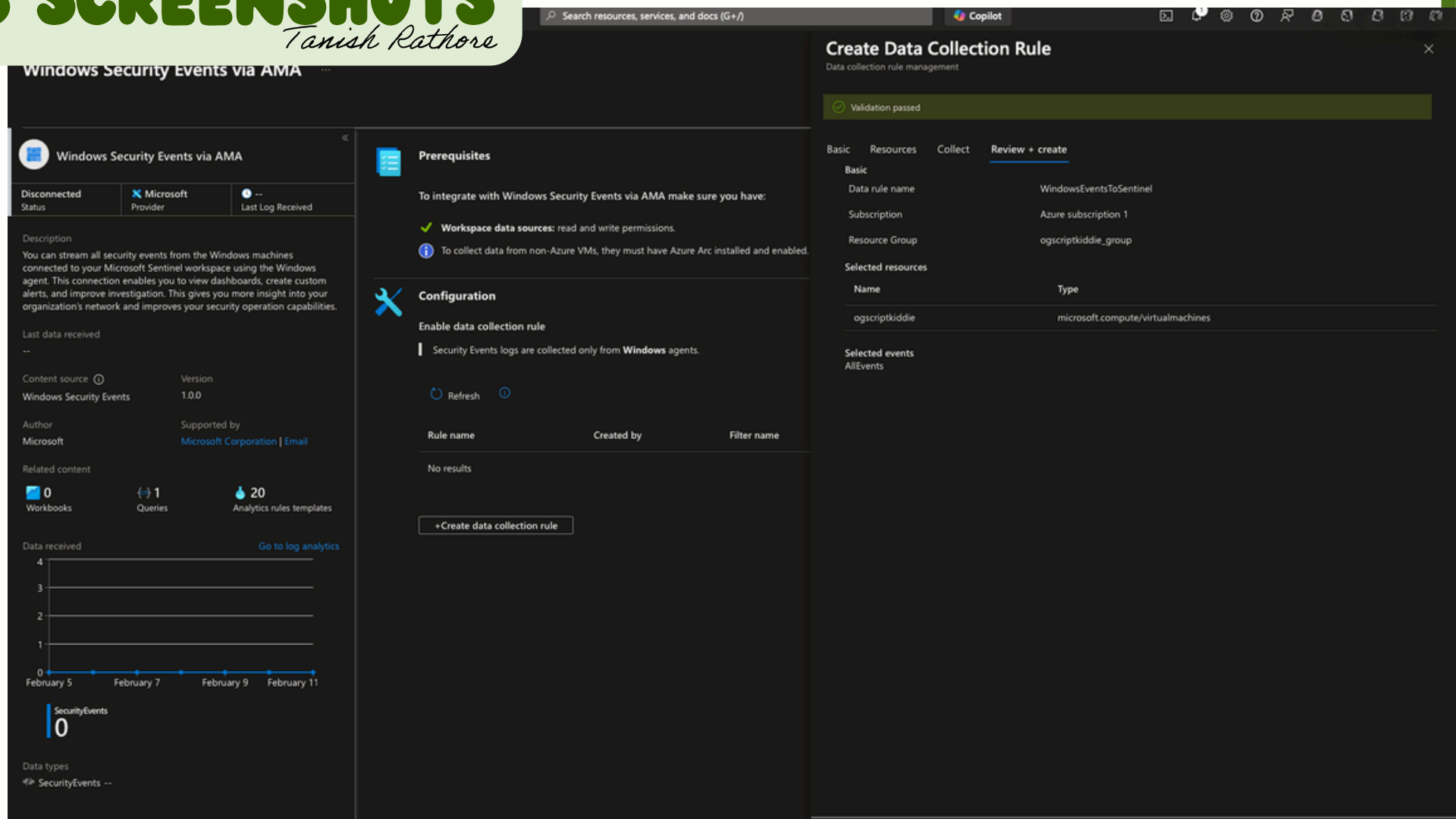
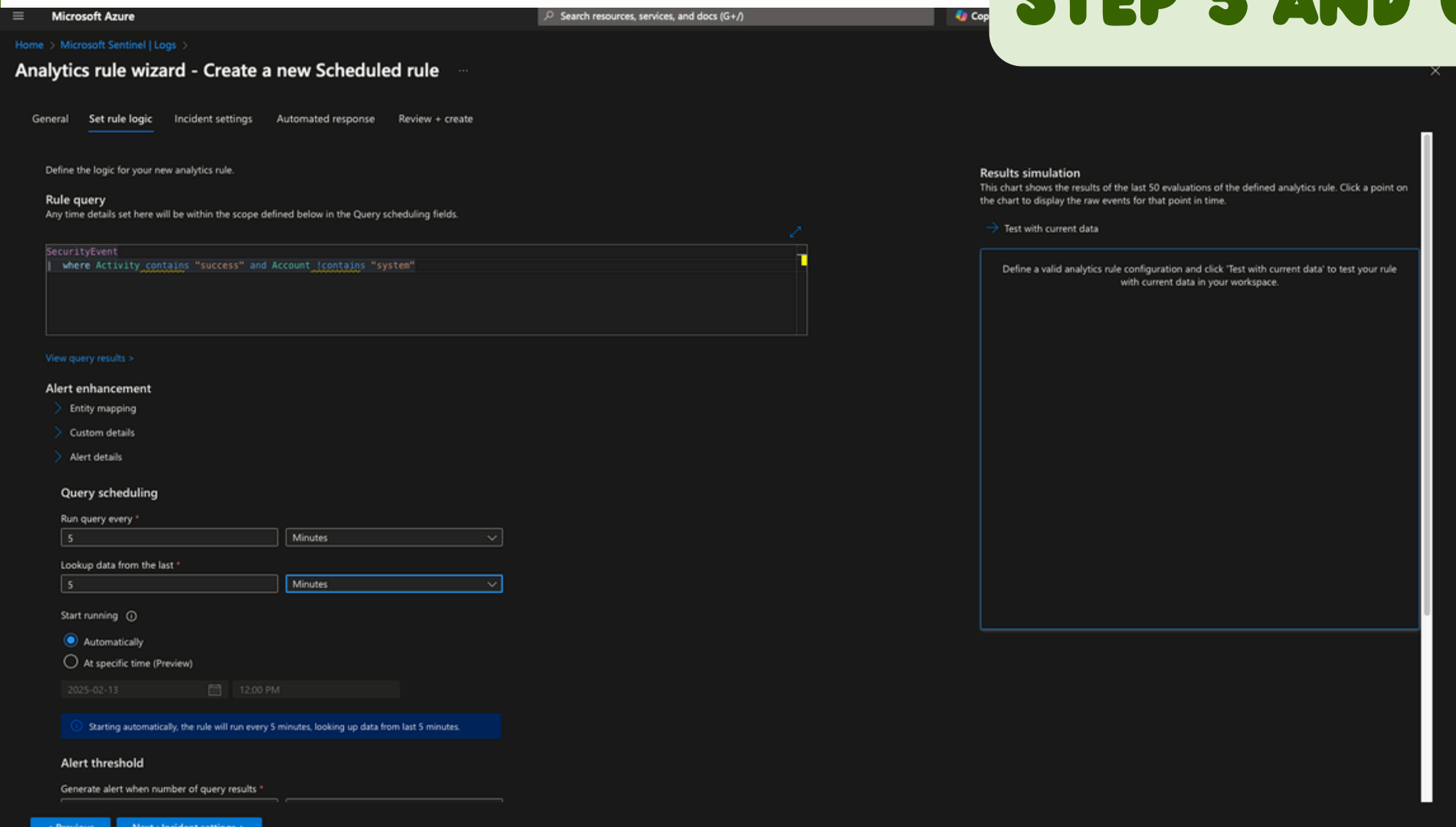
- Used Microsoft Sentinel Dashboards to track login attempts.
  - Investigated security logs and alerts to detect anomalies.
- 





## STEP 5 AND 6 SCREENSHOTS

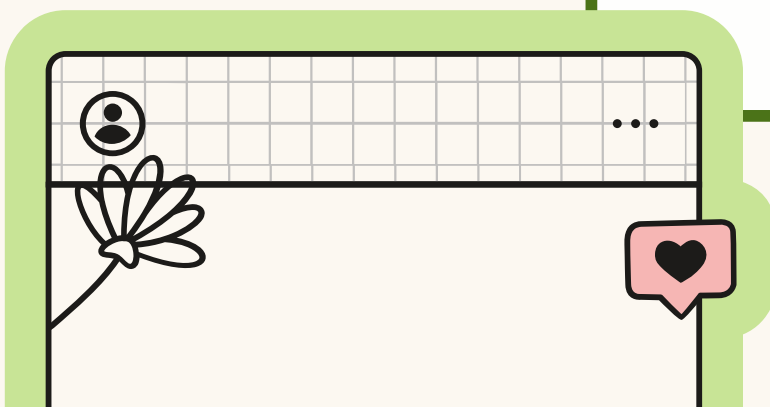
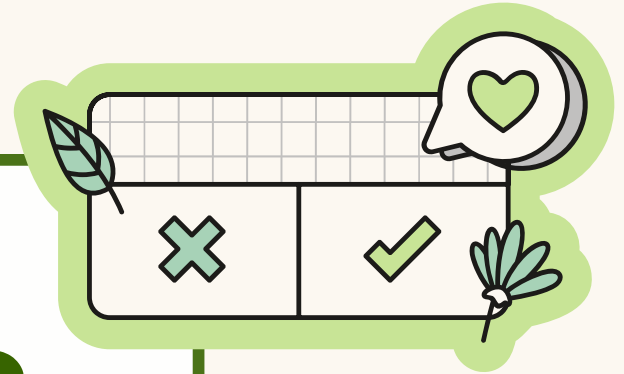
Tanish Rathore





# FINDINGS & OBSERVATIONS

- Real-time alerting: Successfully set up Sentinel alerts for login attempts.
- Enhanced visibility: Identified security events within the VM log stream.
- Threat detection capability: Enabled proactive security monitoring.





# CONCLUSION

This project provided valuable hands-on experience with cloud-based security monitoring using Microsoft Sentinel.

By deploying a SIEM, configuring log analytics, and setting up alert rules, I gained real-world cybersecurity skills applicable to SOC (Security Operations Center) environments.

This knowledge strengthens my ability to work with enterprise security monitoring and threat detection in cloud environments.

