SIEM DEPLOYMENT PROJECT

By Tanish Rathore

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.

Tanish Rathore

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.

Tanish Rathore

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.

Tanish Rathore

STEP 1 AND 2 SCREENSHOTS

Private
portal.azure.com
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot

Home > Virtual machines >

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help 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 Hibernate to enable this feature. Learn more

Administrator account

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	US$81.03
Virtual machine	US$81.03
Image Windows 11 Pro, version 24H2 Windows BYOL applied	US$0.00
Size Standard_D2s_v3	US$81.03
Disks	US$19.71
Networking	US$0.00
Management	US$0.00
Monitoring	US$0.00
Advanced	US$0.00
Estimated monthly cost	US$100.74

< Previous | Next : Disks > | Review + create

Give feedback

Tanish Rathore

METHODOLOGY(CONTD.)

Step 3: Microsoft Sentinel Setup

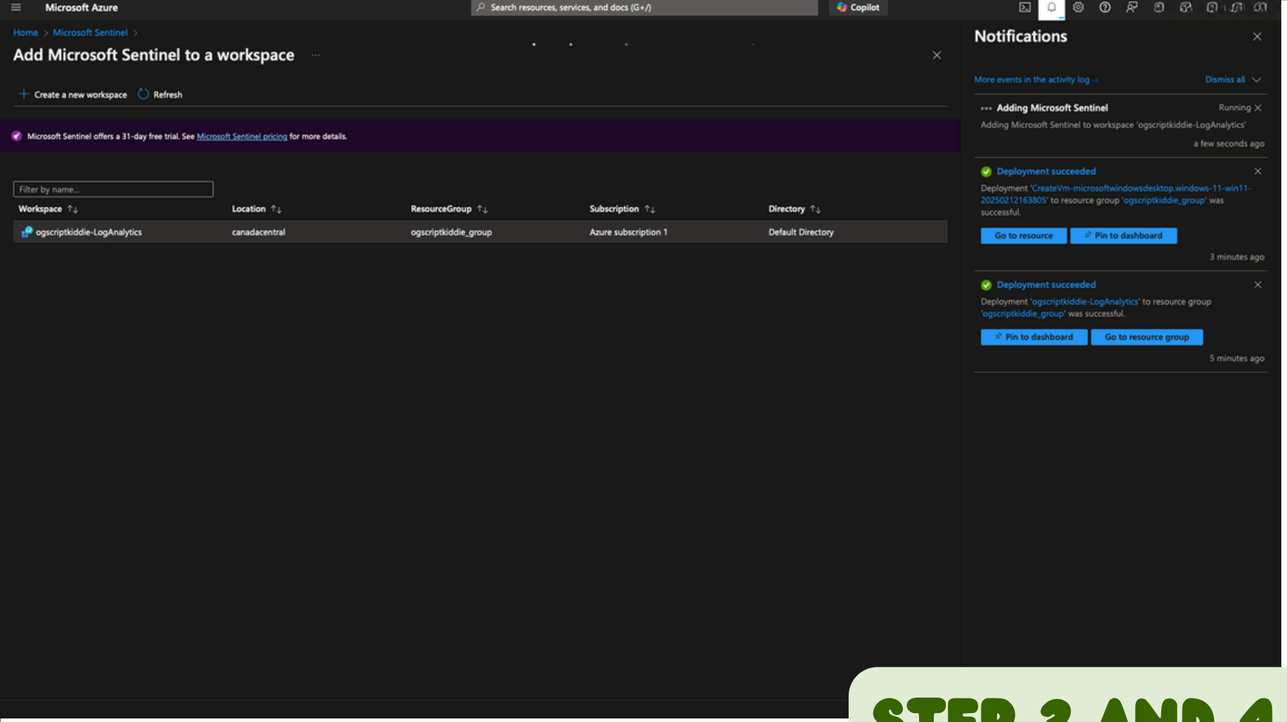
- Created a Sentinel workspace for security log collection.
- Enabled log analytics to process incoming security data.

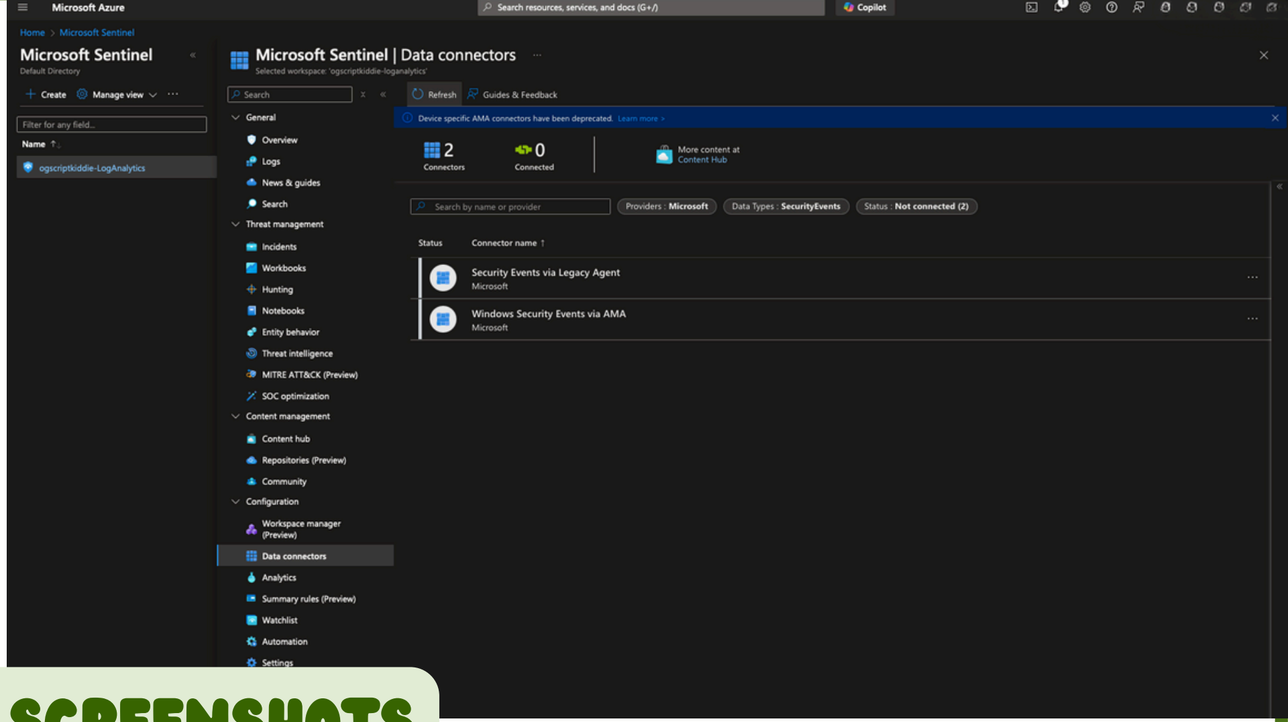
Step 4: Connecting VM to Sentinel

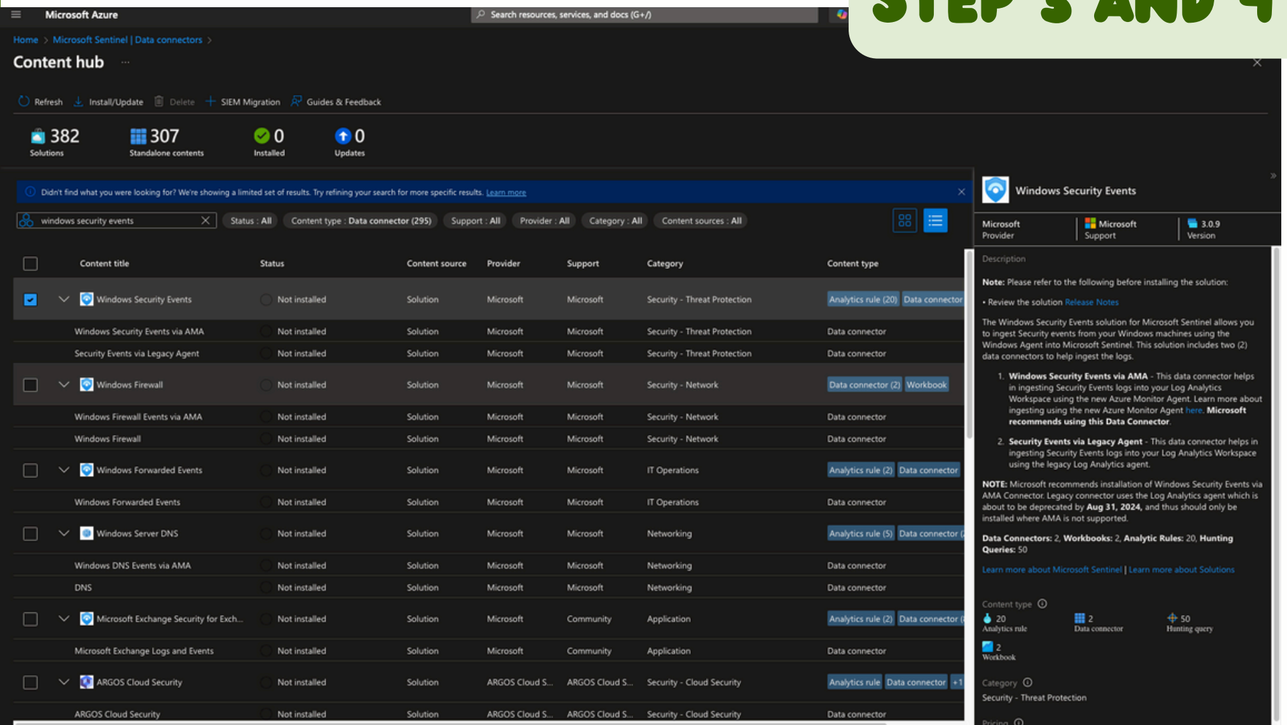
- Installed and configured Azure Monitor Agent (AMA) on the VM.
- Linked the VM's security logs to the Sentinel workspace.

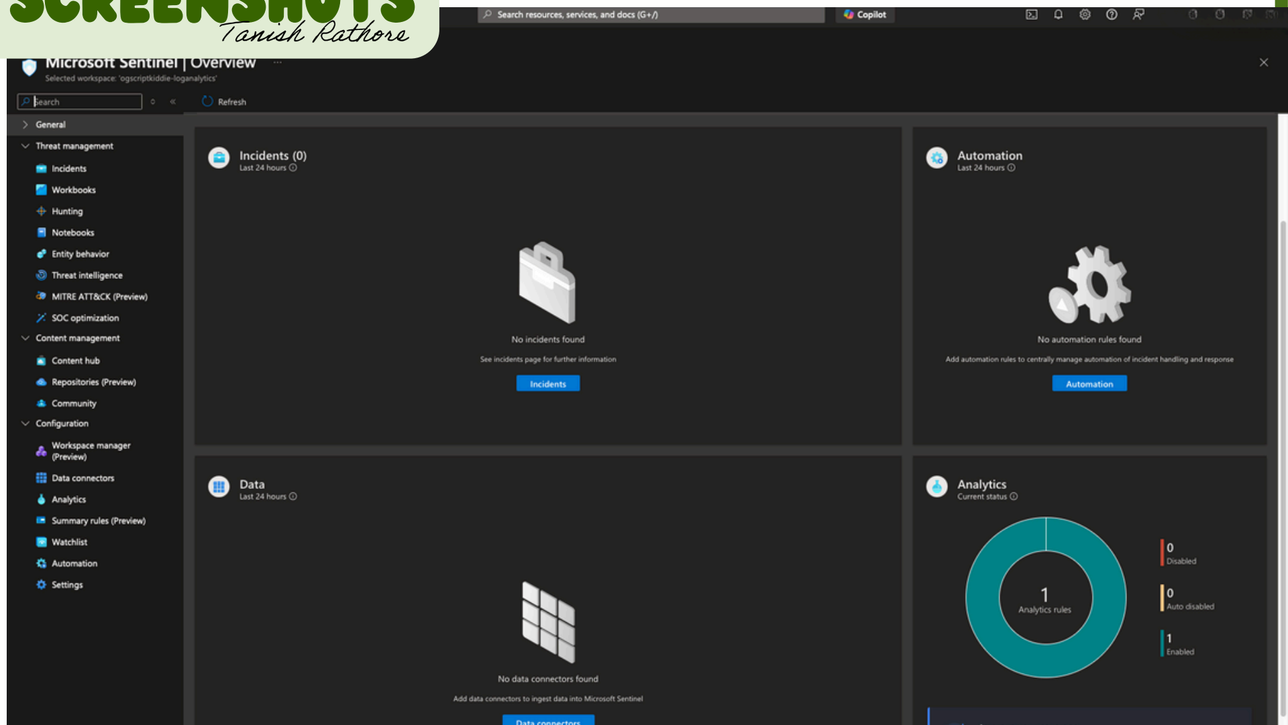
STEP 3 AND 4 SCREENSHOTS

Tanish Rathore









METHODOLOGY(CONTD.)

Step 5: Creating Data Collection Rules

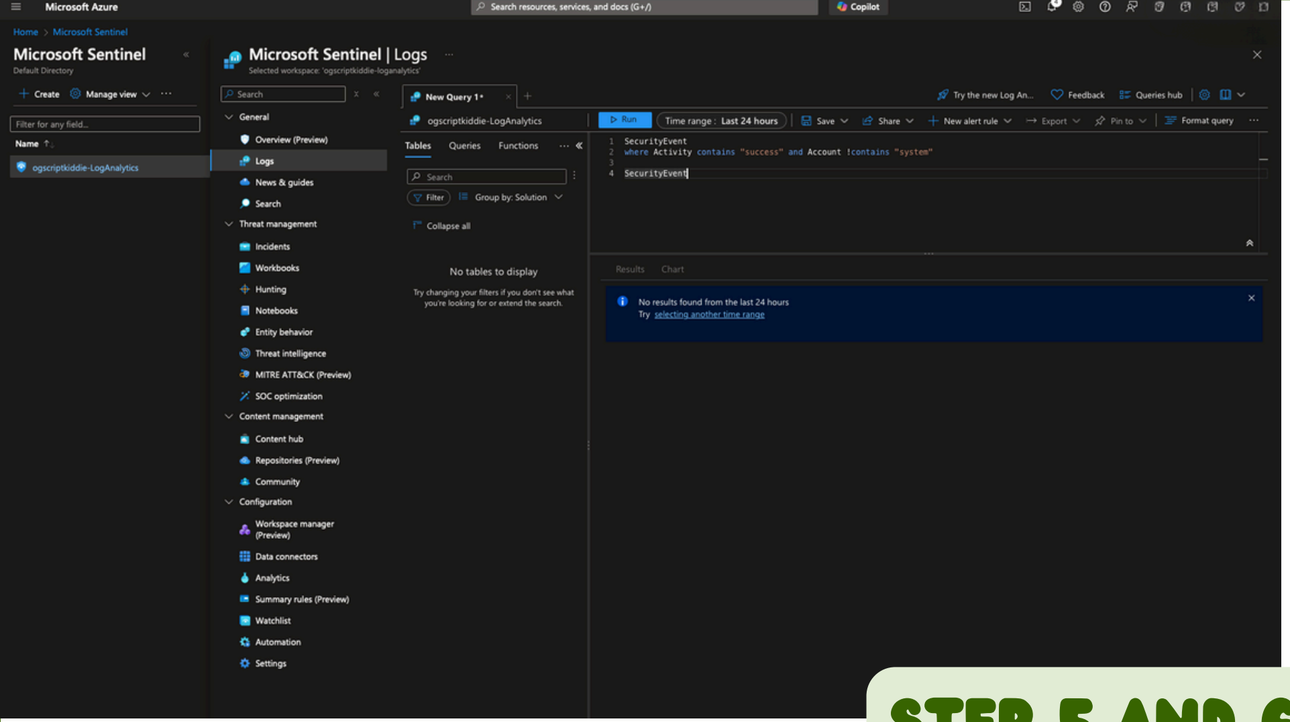
- Defined a log rule to capture successful login attempts.
- Configured alerts to trigger notifications on login events.

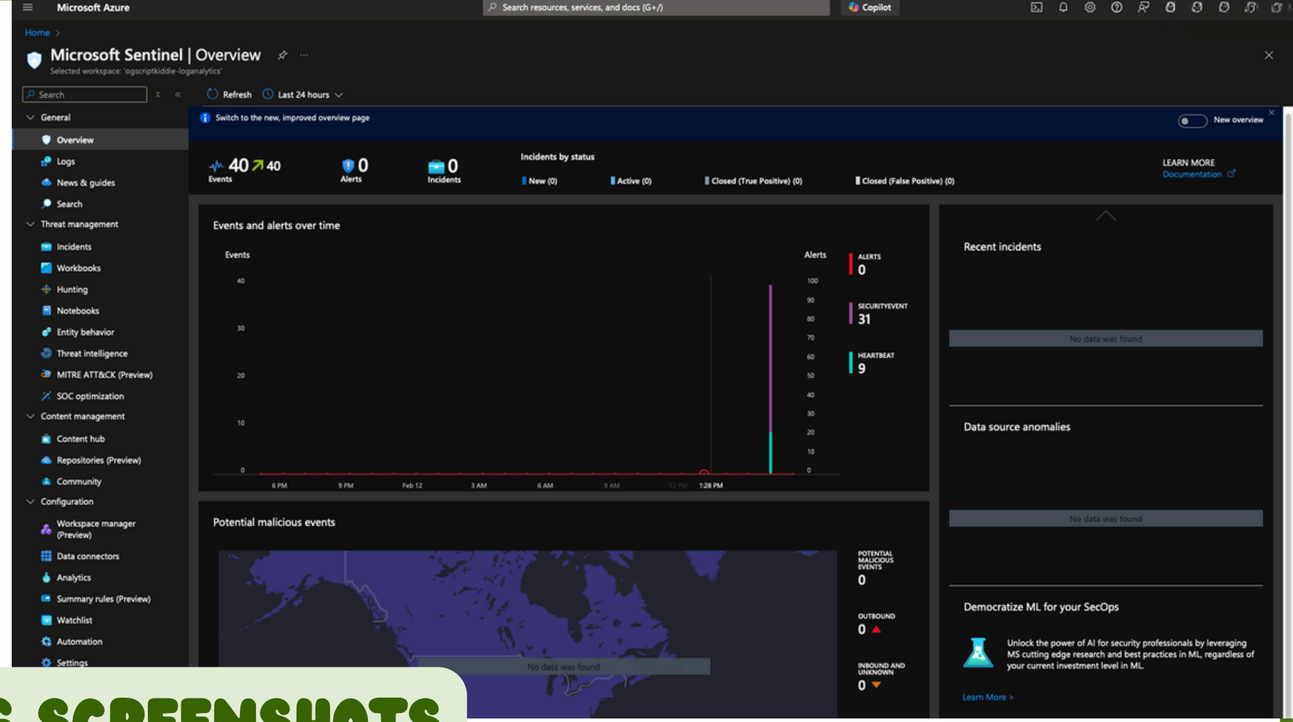
Step 6: Monitoring and Alert Investigation

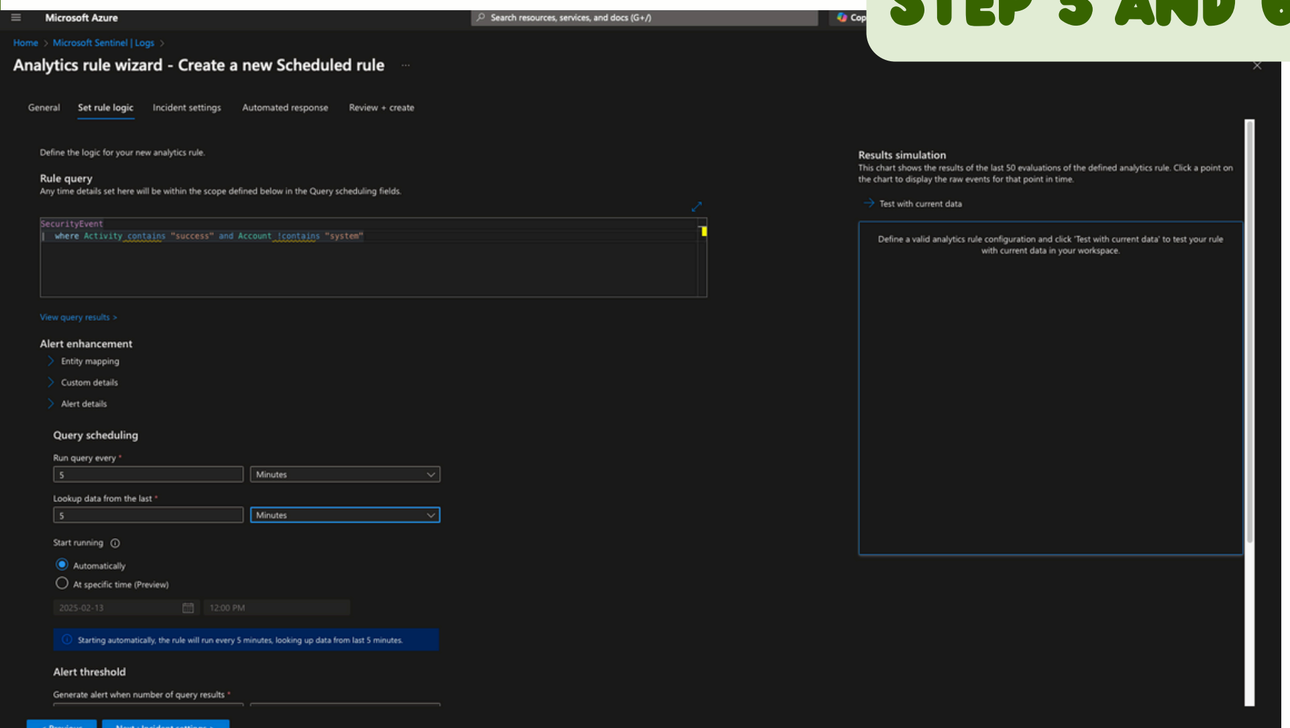
- Used Microsoft Sentinel Dashboards to track login attempts.
- Investigated security logs and alerts to detect anomalies.

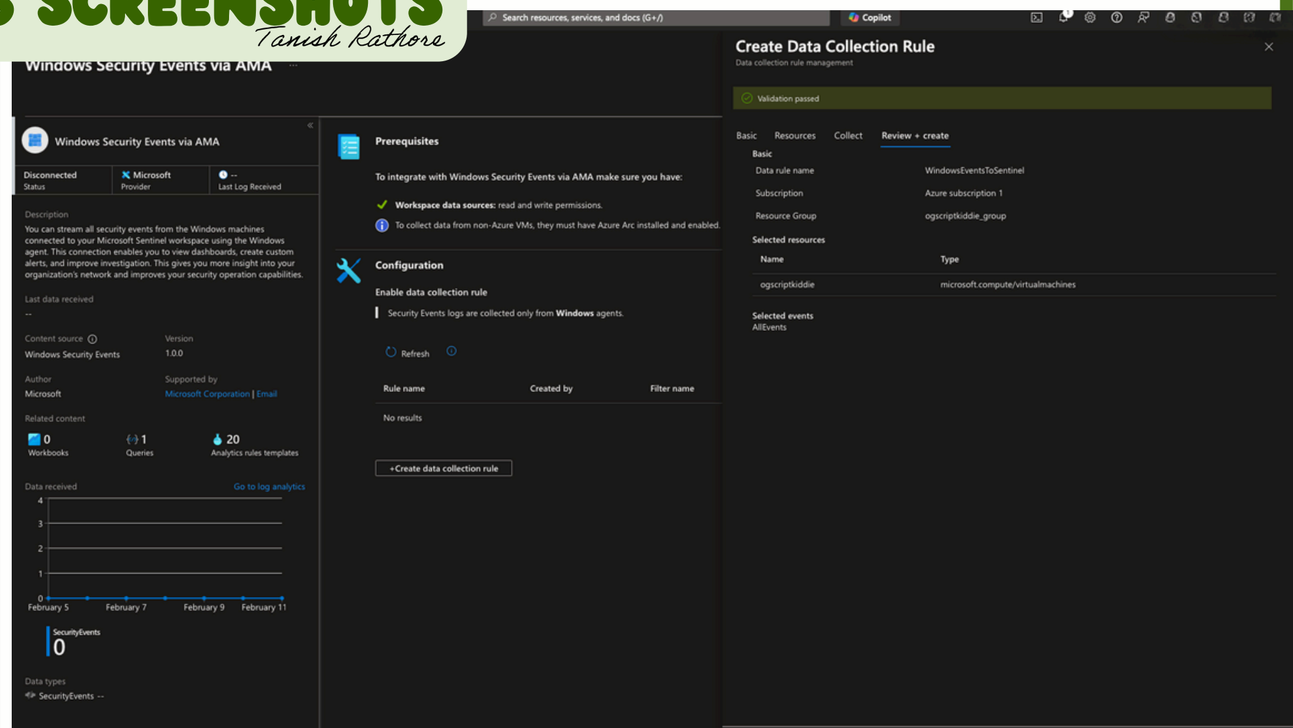
STEP 5 AND 6 SCREENSHOTS

Tanish Rathore









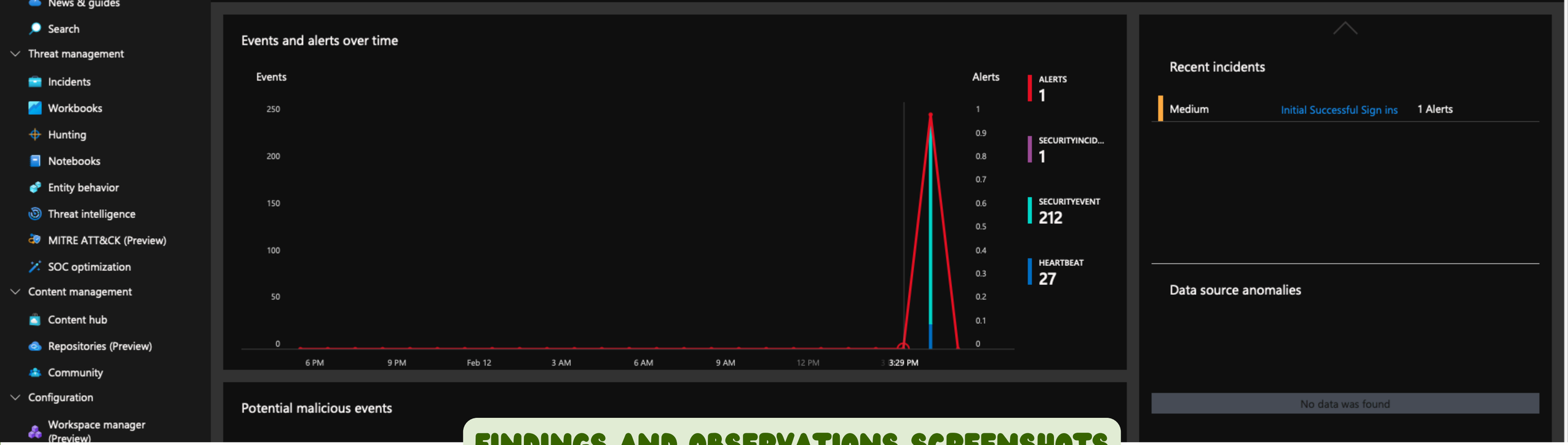
FINDINGS & OBSERVATIONS

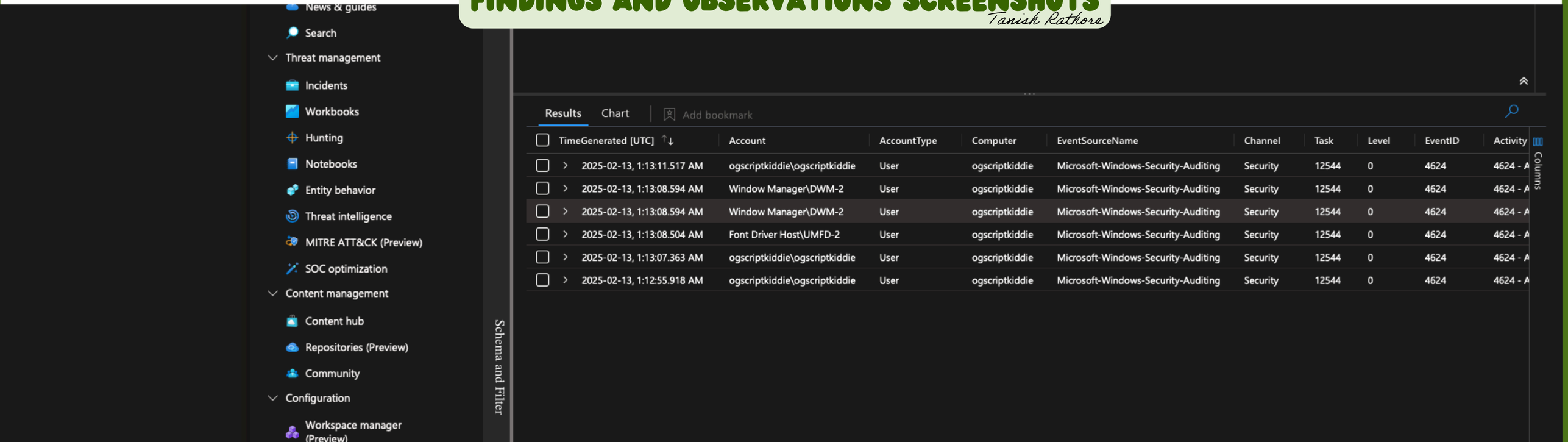
- Real-time alerting: Successfully set up Sentinel alerts for login attempts.
- Enhanced visibility: Identified security events within the VM log stream.
- Threat detection capability: Enabled proactive security monitoring.

Tanish Rathore

FINDINGS AND OBSERVATIONS SCREENSHOTS

Tanish Rathore





TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task	Level	EventID	Activity
2025-02-13, 1:13:11.517 AM	ogscriptkiddie\ogscriptkiddie	User	ogscriptkiddie	Microsoft-Windows-Security-Auditing	Security	12544	0	4624	4624 - A
2025-02-13, 1:13:08.594 AM	Window Manager\DWM-2	User	ogscriptkiddie	Microsoft-Windows-Security-Auditing	Security	12544	0	4624	4624 - A
2025-02-13, 1:13:08.594 AM	Window Manager\DWM-2	User	ogscriptkiddie	Microsoft-Windows-Security-Auditing	Security	12544	0	4624	4624 - A
2025-02-13, 1:13:08.504 AM	Font Driver Host\UMFD-2	User	ogscriptkiddie	Microsoft-Windows-Security-Auditing	Security	12544	0	4624	4624 - A
2025-02-13, 1:13:07.363 AM	ogscriptkiddie\ogscriptkiddie	User	ogscriptkiddie	Microsoft-Windows-Security-Auditing	Security	12544	0	4624	4624 - A
2025-02-13, 1:12:55.918 AM	ogscriptkiddie\ogscriptkiddie	User	ogscriptkiddie	Microsoft-Windows-Security-Auditing	Security	12544	0	4624	4624 - A

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 skillsapplicable to SOC (Security Operations Center) environments.

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

Tanish Rathore

THANK YOU

Tanish Rathore