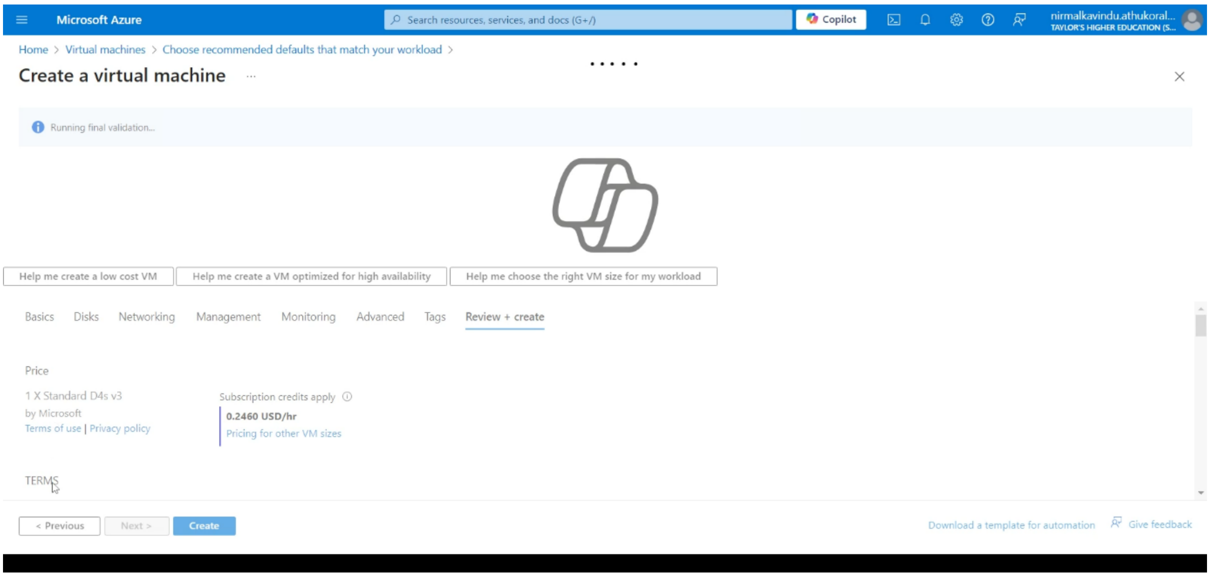
Building a mini-Security operations center (SOC) environment by deploying our own Security information and event management (SIEM) that monitors and generates alerts for our devices, on Azure

Setting up a threat intelligence feed for our SIEM, that sends us commonly seen and newly found compromise indicators whilst Monitoring RDP events

Creating the virtual machine

After logging in to Azure, We set up our first Virtual Machine
We then create a RESOURCE GROUP, name our virtual machine

Specify the Operating system we're using to be windows pro, for familiarity, and ease of use in a Microsoft based environment


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
nirmalkavindu.athukoral...
TAYLOR'S HIGHER EDUCATION (S...
Home > Virtual machines > Choose recommended defaults that match your workload >
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
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next >
Create
Download a template for automation
Give feedback

Create a virtual machine

Running final validation...

Price

1 X Standard D4s v3
by Microsoft
Terms of use | Privacy policy

Subscription credits apply
0.2460 USD/hr
Pricing for other VM sizes

TERMS

Figure 1. Creating the Virtual Machine

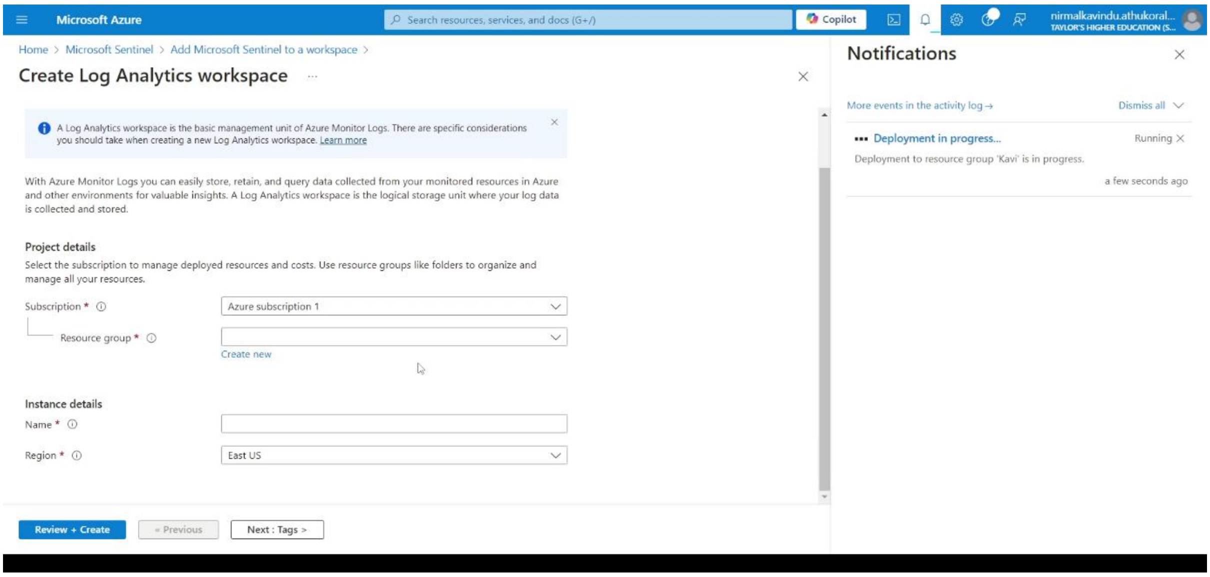
Deploying Sentinel

While that loads, we turn our attention to Deploying sentinel

We first add it to the resource group we created earlier

Give it its name

And importantly, make sure we set it up in same region as the virtual machine


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
nirmalkavindu.athukoral...
TAYLOR'S HIGHER EDUCATION (S...
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >
Review + Create
« Previous
Next : Tags >
More events in the activity log →
Dismiss all

Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

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.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure subscription 1

Resource group * :

Create new

Instance details

Name * :

Region * : East US

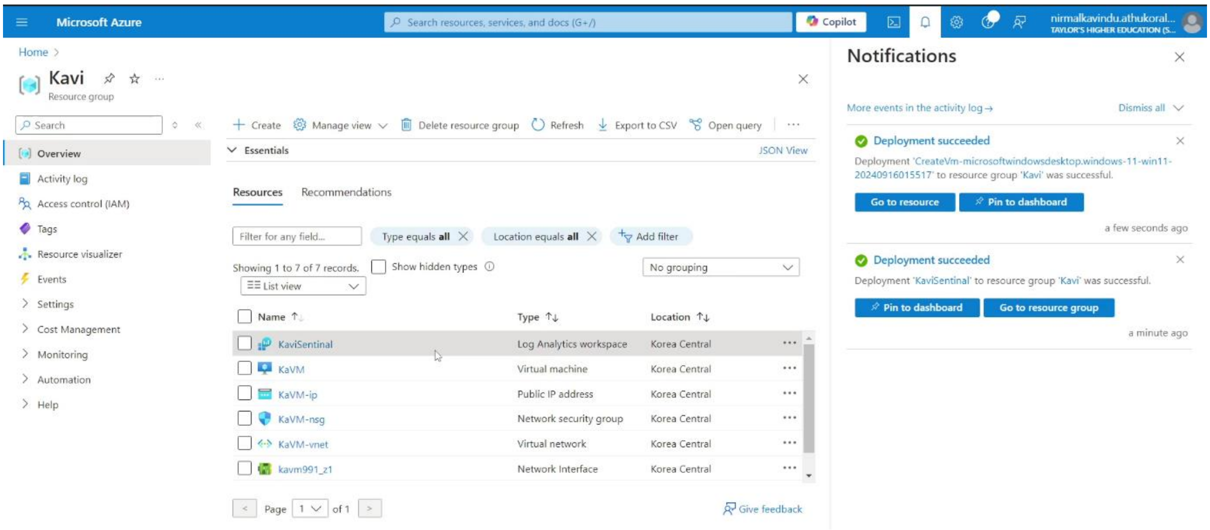
Notifications

Deployment in progress... Running

Deployment to resource group 'Kavi' is in progress.

a few seconds ago

Figure 2. Creating the log analytics workspace using Sentinal



Kavi

Resource group

Showing 1 to 7 of 7 records.

Name	Type	Location
KaviSentinal	Log Analytics workspace	Korea Central
KaVM	Virtual machine	Korea Central
KaVM-ip	Public IP address	Korea Central
KaVM-nsg	Network security group	Korea Central
KaVM-vnet	Virtual network	Korea Central
kavm991_z1	Network Interface	Korea Central

Notifications

Deployment succeeded

Deployment 'CreateVm-microsoftwindowsdesktop.windows-11-win11-20240916015517' to resource group 'Kavi' was successful.

a few seconds ago

Deployment succeeded

Deployment 'KaviSentinal' to resource group 'Kavi' was successful.

a minute ago

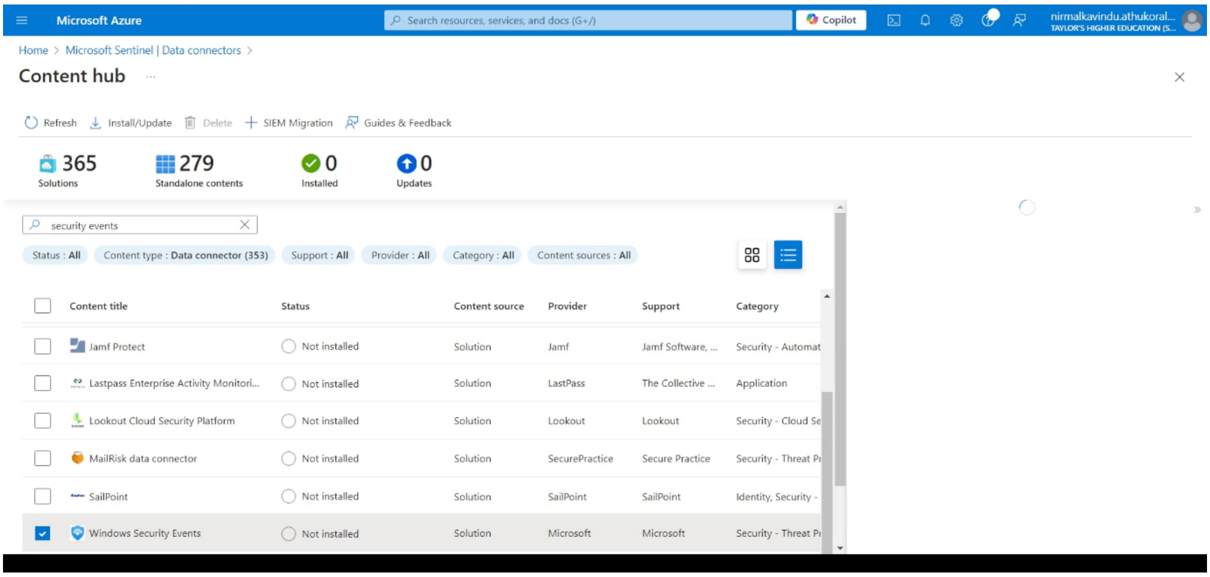
Figure 3. The GUI of our overview

Data Connectors

Add the virtual machines event logs to the Log analytics workspace which then sends it to sentinel
Then we set up a data connector to enable connections into the broader security ecosystem.

The content hub, contains established connectors

- install windows security events (azure monitor agent)



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
nirmalkavindu.athukoral...
TAYLOR'S HIGHER EDUCATION (S...

Home > Microsoft Sentinel | Data connectors >

Content hub ···

Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback

365 Solutions

279 Standalone contents

0 Installed

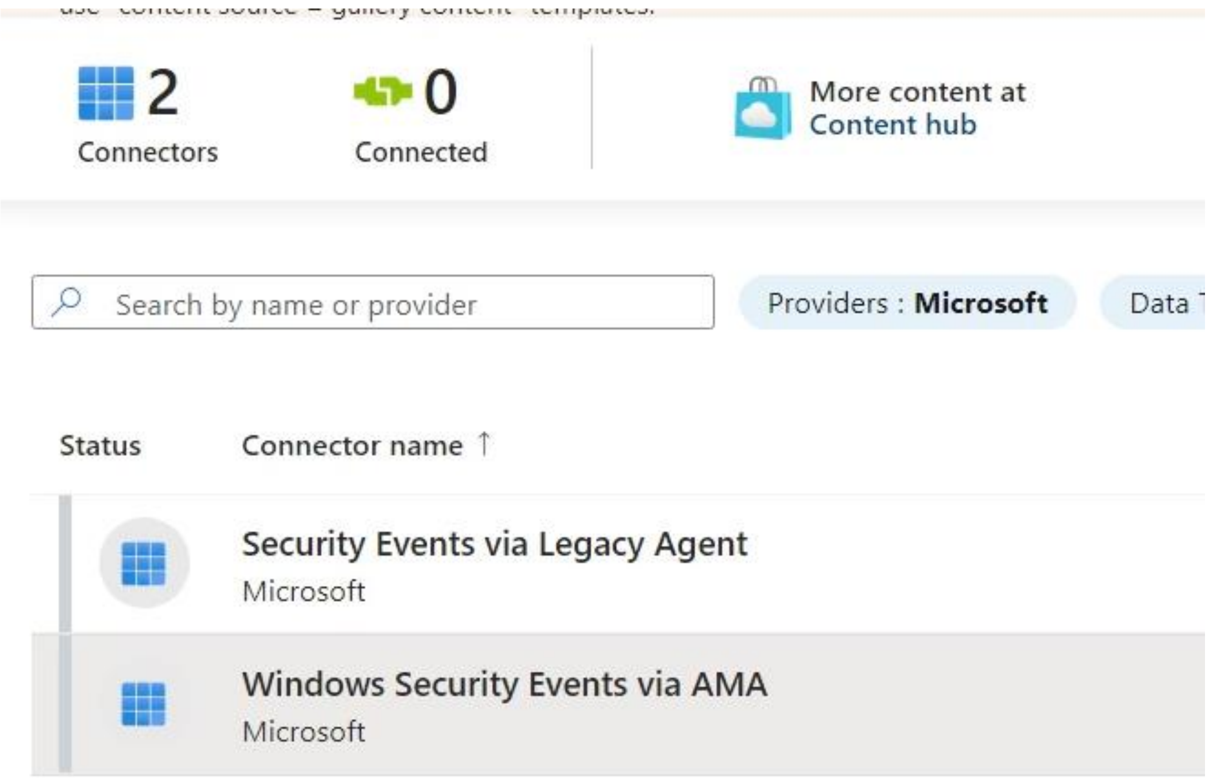
0 Updates

security events

Status : **All** | Content type : **Data connector (353)** | Support : **All** | Provider : **All** | Category : **All** | Content sources : **All**

☐	Content title	Status	Content source	Provider	Support	Category
☐	Jamf Protect	○ Not installed	Solution	Jamf	Jamf Software, ...	Security - Automat
☐	Lastpass Enterprise Activity Monitori...	○ Not installed	Solution	LastPass	The Collective ...	Application
☐	Lookout Cloud Security Platform	○ Not installed	Solution	Lookout	Lookout	Security - Cloud Se
☐	MailRisk data connector	○ Not installed	Solution	SecurePractice	Secure Practice	Security - Threat Pr
☐	SailPoint	○ Not installed	Solution	SailPoint	SailPoint	Identity, Security -
☑	Windows Security Events	○ Not installed	Solution	Microsoft	Microsoft	Security - Threat Pr

Figure 4. The content hub with established connectors



2 Connectors

0 Connected

More content at Content hub

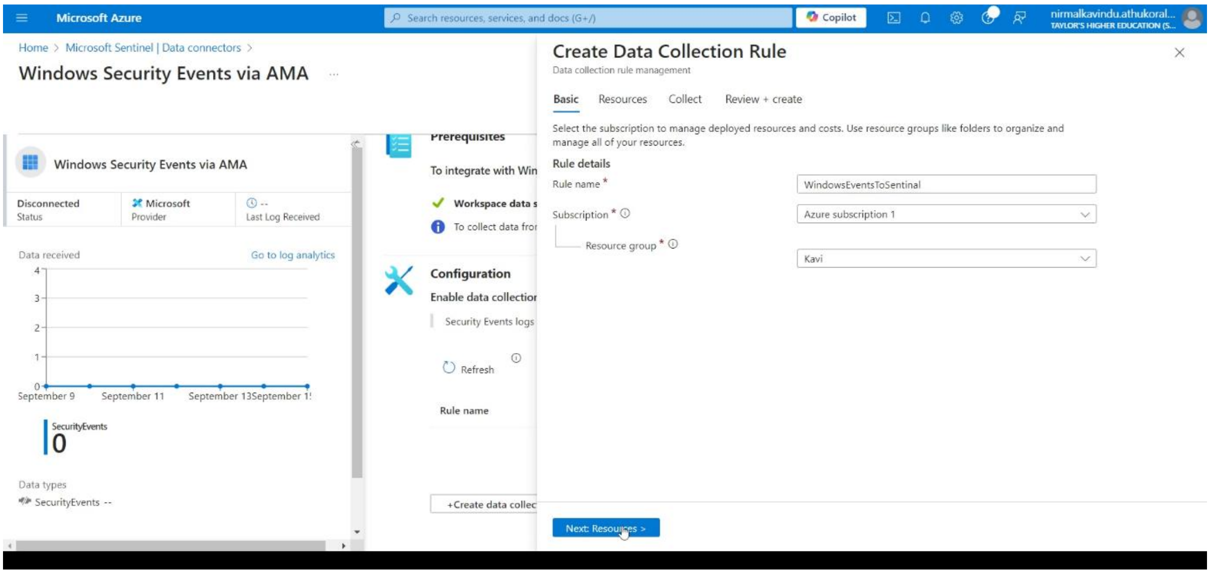
Search by name or provider

Providers : **Microsoft** | Data

Status	Connector name ↑
	Security Events via Legacy Agent Microsoft
	Windows Security Events via AMA Microsoft

Figure 5. The connectors when we install "Windows Security Events"

Setting up data collection rules



Windows Security Events via AMA

Disconnected Status | Microsoft Provider | -- Last Log Received

Create Data Collection Rule

Data collection rule management

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources.

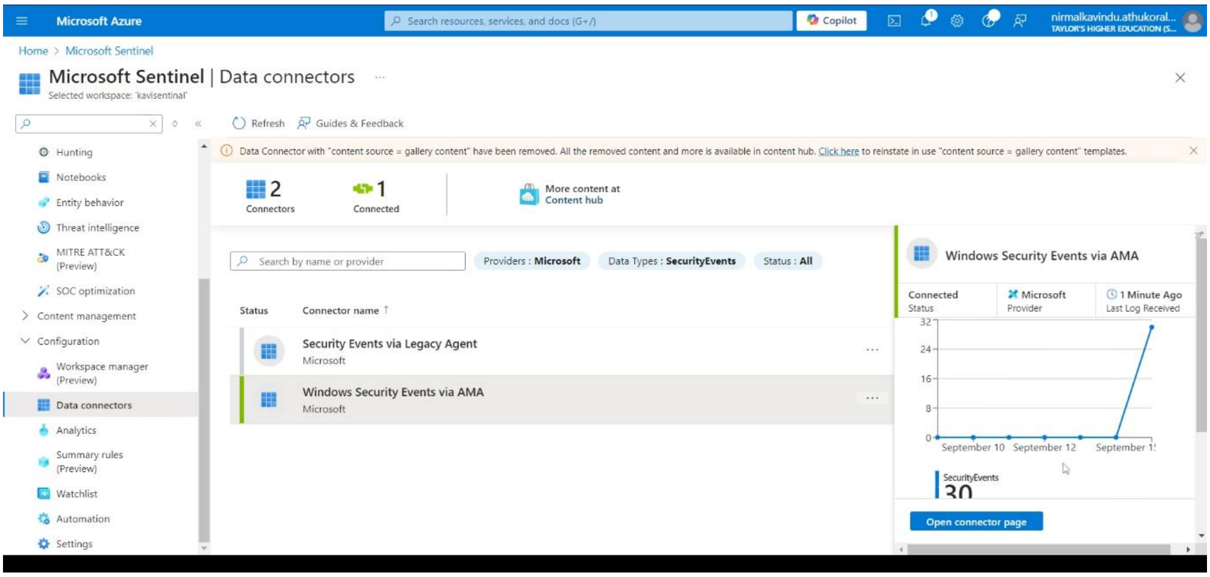
Rule details

Rule name * WindowsEventsToSentinal

Subscription * Azure subscription 1

Resource group * Kavi

Figure 6. Creating the data collection rule



Microsoft Sentinel | Data connectors

Selected workspace: 'kavisentinal'

Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.

2 Connectors | 1 Connected

Providers : Microsoft | Data Types : SecurityEvents | Status : All

Security Events via Legacy Agent
Microsoft

Windows Security Events via AMA
Microsoft

Windows Security Events via AMA

Connected Status | Microsoft Provider | 1 Minute Ago Last Log Received

Figure 7. Overview of the Data connectors page

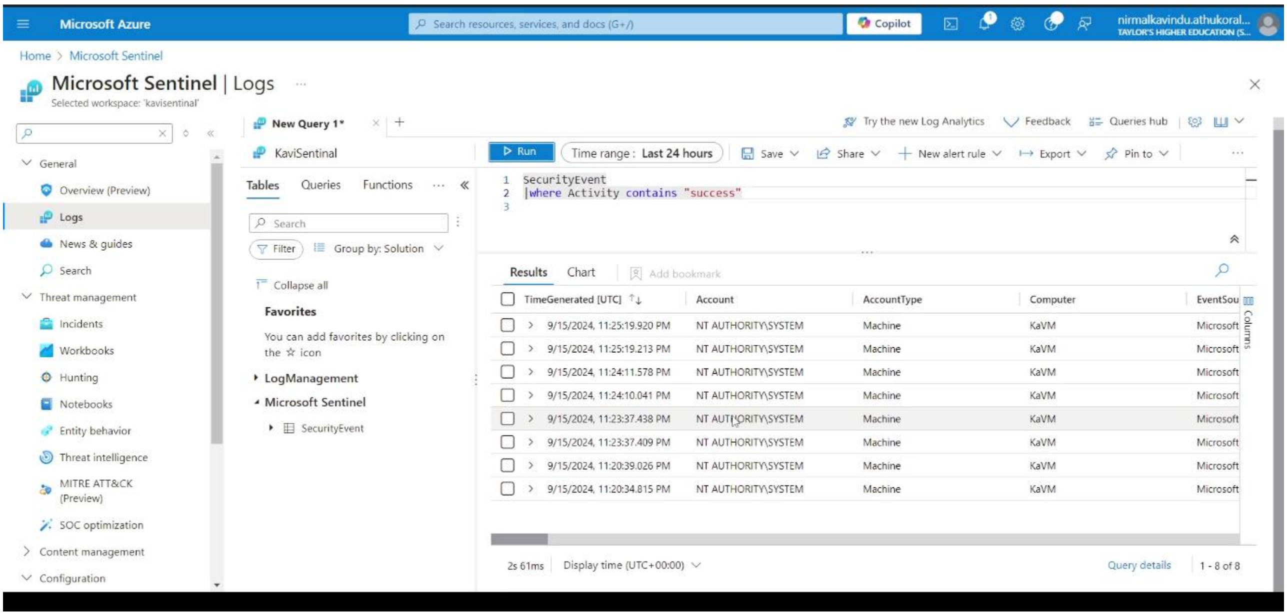
Testing our rules and using the wizard

We select our virtual machine, for all security events and now u can see logs being collected

Creating a rule that checks for successful sign in’s via rdp

-Creating sentinel rule using wizard

-testing query



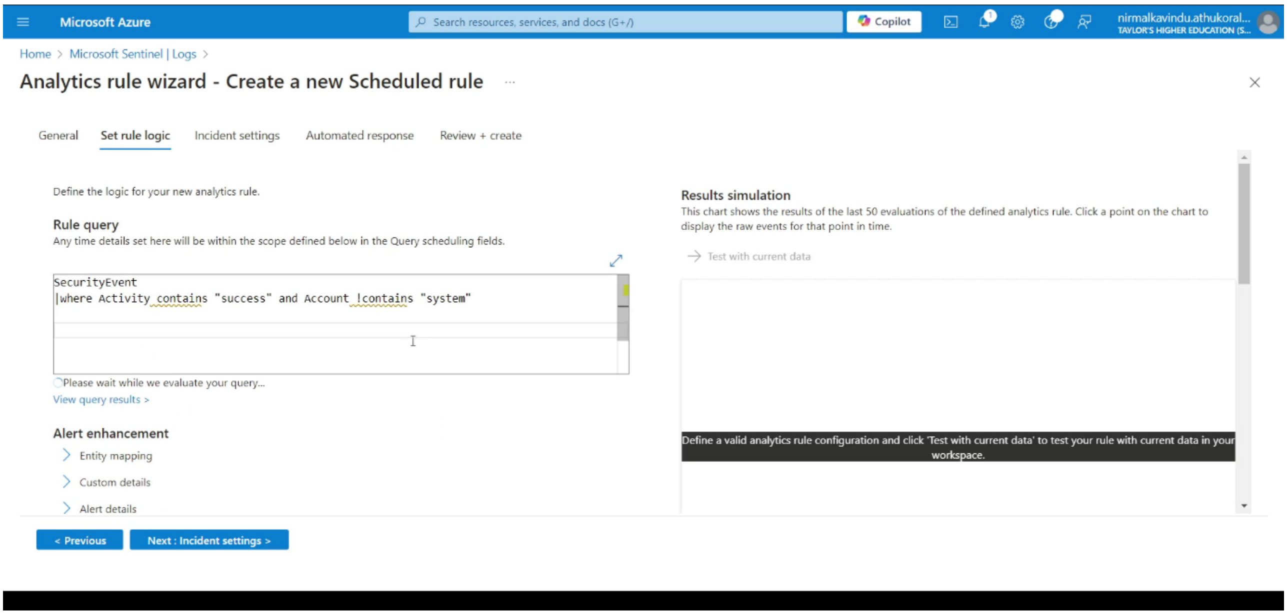
Time range : Last 24 hours

```
SecurityEvent
|where Activity contains "success"
```

TimeGenerated [UTC]	Account	AccountType	Computer	EventSou
9/15/2024, 11:25:19.920 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft
9/15/2024, 11:25:19.213 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft
9/15/2024, 11:24:11.578 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft
9/15/2024, 11:24:10.041 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft
9/15/2024, 11:23:37.438 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft
9/15/2024, 11:23:37.409 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft
9/15/2024, 11:20:39.026 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft
9/15/2024, 11:20:34.815 PM	NT AUTHORITY\SYSTEM	Machine	KaVM	Microsoft

2s 61ms Display time (UTC+00:00) Query details 1 - 8 of 8

Figure 8. Testing a security event query



Analytics rule wizard - Create a new Scheduled rule

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
SecurityEvent
|where Activity contains "success" and Account !contains "system"
```

Please wait while we evaluate your query...

View query results >

Alert enhancement

Results simulation

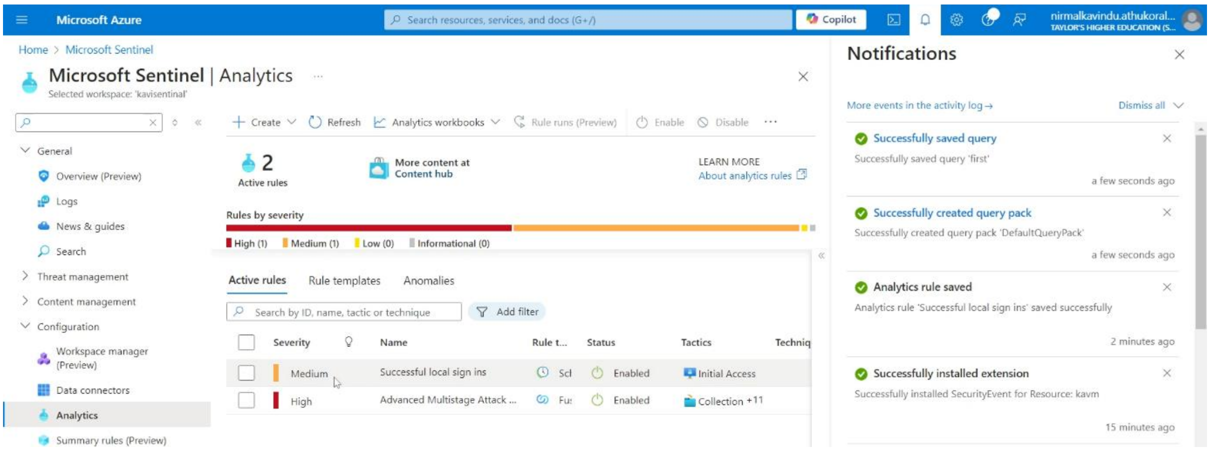
This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Define a valid analytics rule configuration and click 'Test with current data' to test your rule with current data in your workspace.

Figure 9. Using the wozard to crete a new rule

Overview and testing

In analytics page, we see the rules that we have created



Microsoft Sentinel | Analytics

Selected workspace: 'kavisentinal'

2 Active rules

Rules by severity

High (1) Medium (1) Low (0) Informational (0)

□	Severity	Name	Rule t...	Status	Tactics	Techniq
□	Medium	Successful local sign ins	Scl	Enabled	Initial Access	
□	High	Advanced Multistage Attack ...	Fu:	Enabled	Collection +11	

Notifications

More events in the activity log →

Dismiss all

Successfully saved query

Successfully saved query 'first'

a few seconds ago

Successfully created query pack

Successfully created query pack 'DefaultQueryPack'

a few seconds ago

Analytics rule saved

Analytics rule 'Successful local sign ins' saved successfully

2 minutes ago

Successfully installed extension

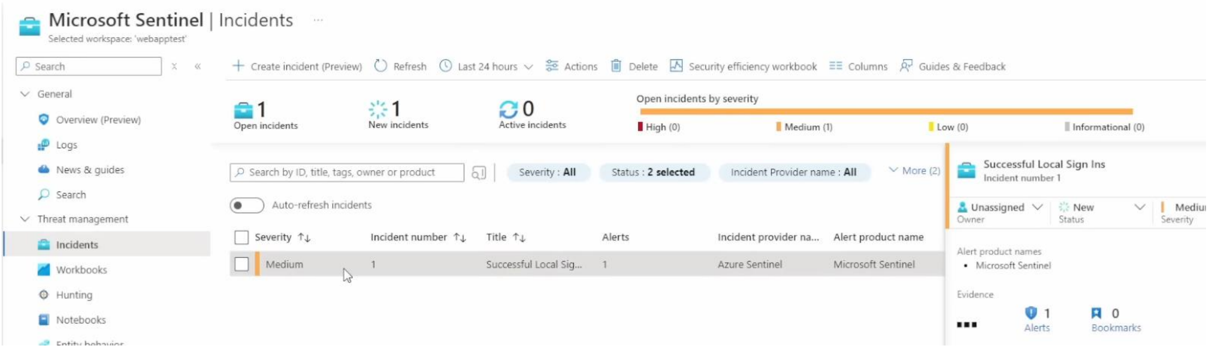
Successfully installed SecurityEvent for Resource: kavm

15 minutes ago

Figure 10. The Analytics page after we have created our rules, an overview.

This rule runs approximately every 5 mins

So, if I sign in after 5 mins it will give me an alert for a sign in



Microsoft Sentinel | Incidents

Selected workspace: 'webapptest'

1 Open incidents

1 New incidents

0 Active incidents

Open incidents by severity

High (0) Medium (1) Low (0) Informational (0)

Severity : All

Status : 2 selected

Incident Provider name : All

□	Severity	Incident number	Title	Alerts	Incident provider na...	Alert product name
□	Medium	1	Successful Local Sig...	1	Azure Sentinel	Microsoft Sentinel

Successful Local Sign Ins

Incident number 1

Owner: Unassigned

Status: New

Severity: Mediu

Alert product names

- Microsoft Sentinel

Evidence

1 Alerts

0 Bookmarks

Figure 11. The Rule has run successfully, sending me an alert after I have logged in.