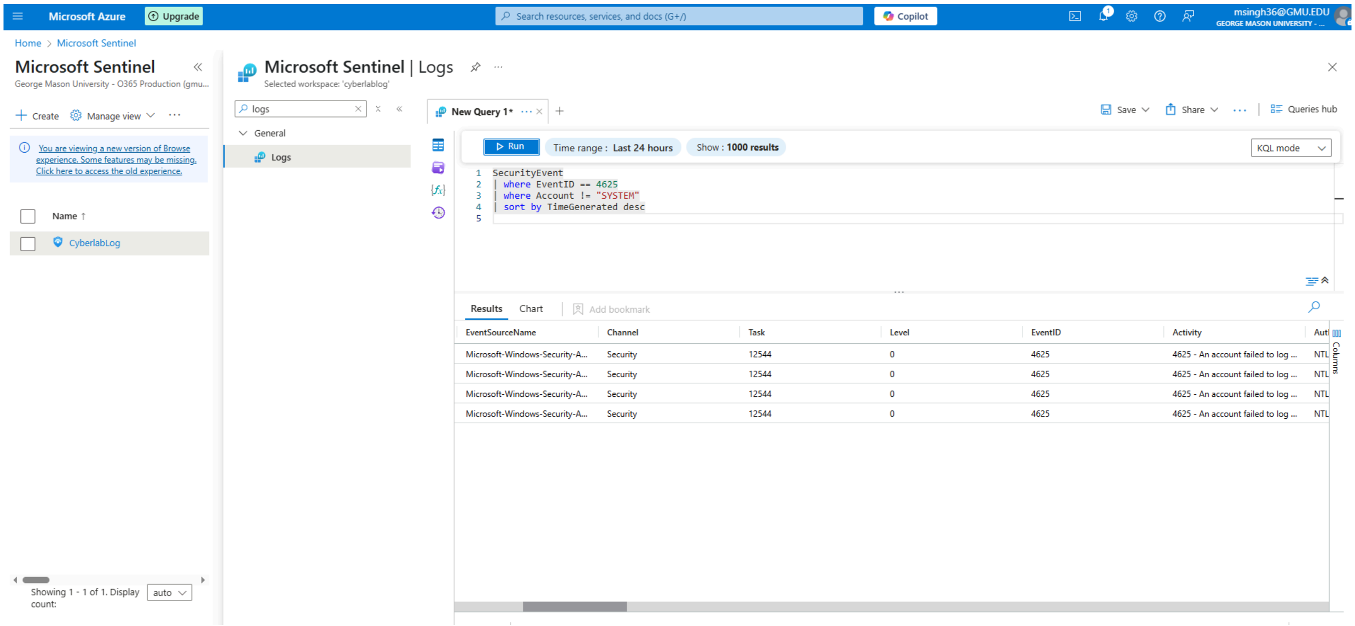


Microsoft Sentinel | Logs

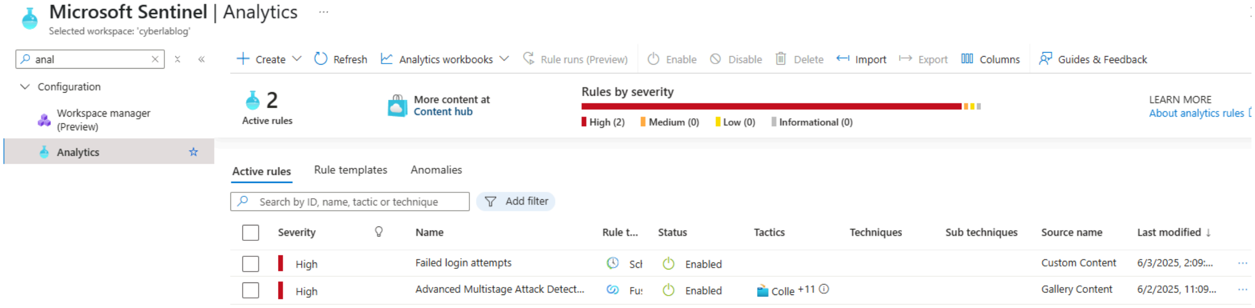
Selected workspace: 'cyberlablog'

```
SecurityEvent
| where EventID == 4625
| where Account != "SYSTEM"
| sort by TimeGenerated desc
```

EventSourceName	Channel	Task	Level	EventID	Activity	Aut
Microsoft-Windows-Security-A...	Security	12544	0	4625	4625 - An account failed to log ...	NTL
Microsoft-Windows-Security-A...	Security	12544	0	4625	4625 - An account failed to log ...	NTL
Microsoft-Windows-Security-A...	Security	12544	0	4625	4625 - An account failed to log ...	NTL
Microsoft-Windows-Security-A...	Security	12544	0	4625	4625 - An account failed to log ...	NTL

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
msingh36@GMU.EDU
GEORGE MASON UNIVERSITY - ...
Home > Microsoft Sentinel
Microsoft Sentinel
George Mason University - O365 Production (gmu...
Create
Manage view
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name ↑
CyberlabLog
Showing 1 - 1 of 1. Display count:
auto
logs
General
Logs
New Query 1*
Save
Share
Queries hub
Run
Time range : Last 24 hours
Show : 1000 results
KQL mode
Results
Chart
Add bookmark
Columns

This image represents the event ID of 4625 when doing a brute force attack on a windows VM. The logs within the Microsoft Sentinel shows that it was recognized as an attack.



Microsoft Sentinel | Analytics

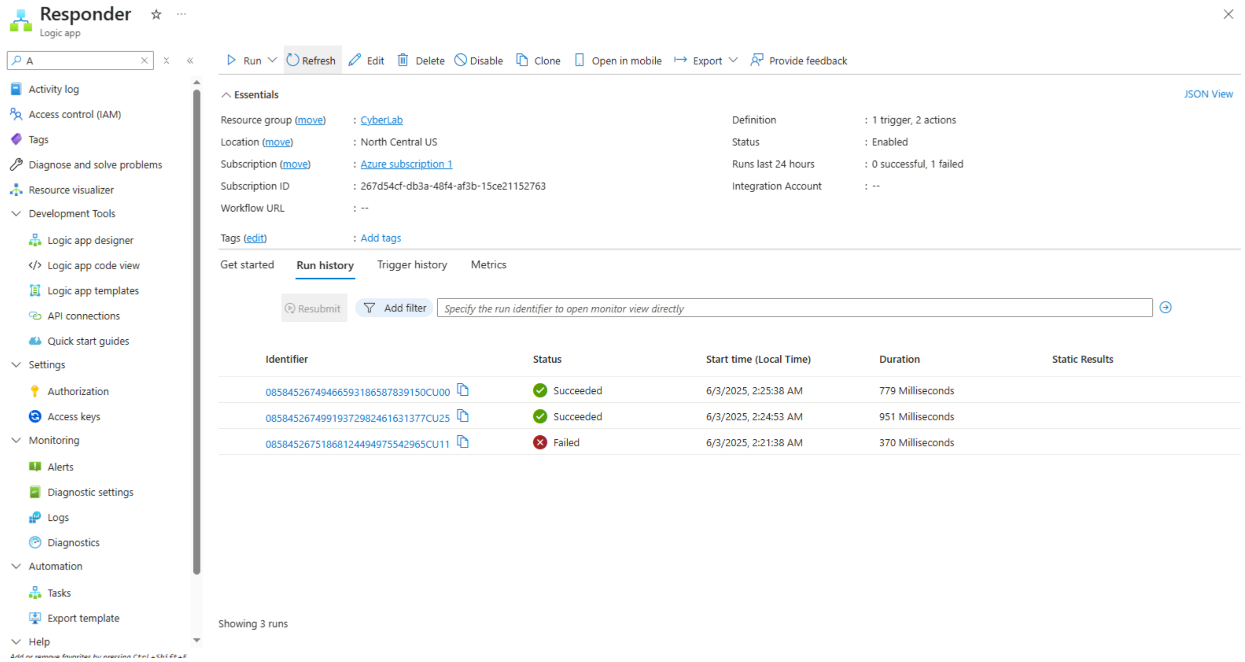
Selected workspace: 'cyberlablog'

2 Active rules

Rules by severity: High (2) Medium (0) Low (0) Informational (0)

Severity	Name	Rule t...	Status	Tactics	Techniques	Sub techniques	Source name	Last modified ↓
High	Failed login attempts	Scl	Enabled				Custom Content	6/3/2025, 2:09:...
High	Advanced Multistage Attack Detect...	Fu:	Enabled	Colle +11			Gallery Content	6/2/2025, 11:09...

This image shows that there is a high severity risk that was detected by Microsoft Sentinels. This high severity risk was the brute force attack done of multiple login attempts done by me.



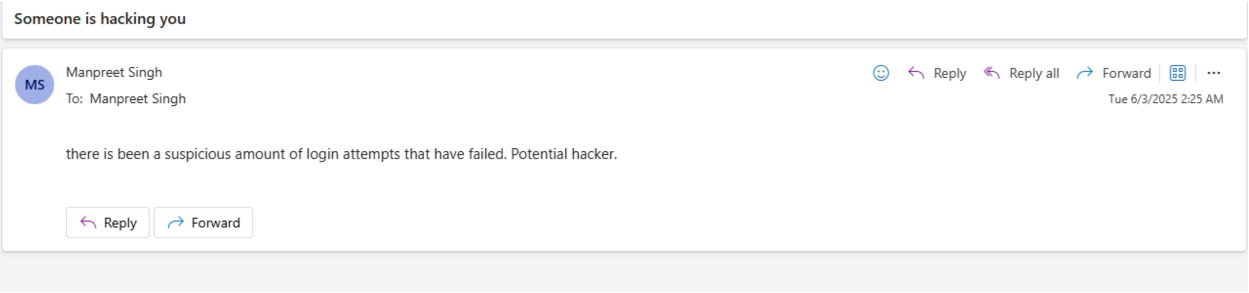
Essentials

Resource group (move)	: CyberLab	Definition	: 1 trigger, 2 actions
Location (move)	: North Central US	Status	: Enabled
Subscription (move)	: Azure subscription 1	Runs last 24 hours	: 0 successful, 1 failed
Subscription ID	: 267d54cf-db3a-48f4-af3b-15ce21152763	Integration Account	: --
Workflow URL	: --		
Tags (edit)	: Add tags		

Identifier	Status	Start time (Local Time)	Duration	Static Results
08584526749466593186587839150CU00	✓ Succeeded	6/3/2025, 2:25:38 AM	779 Milliseconds	
08584526749919372982461631377CU25	✓ Succeeded	6/3/2025, 2:24:53 AM	951 Milliseconds	
08584526751868124494975542965CU11	✗ Failed	6/3/2025, 2:21:38 AM	370 Milliseconds	

Showing 3 runs

This image shows the response of sending an email when detecting an attack being successful.



Someone is hacking you

MS Manpreet Singh
To: Manpreet Singh
Tue 6/3/2025 2:25 AM

there is been a suspicious amount of login attempts that have failed. Potential hacker.

This was the email that was sent to me after Windows Sentinel detected a high risk attack being introduced.