

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot mainph36@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

Microsoft Sentinel | Logs
Selected workspace: 'cyberlablog'

logs

New Query 1* ... x +

Run Time range: Last 24 hours Show: 1000 results KQL mode

```
1 SecurityEvent
2 | where EventID == 4625
3 | where Account != "SYSTEM"
4 | sort by TimeGenerated desc
5
```

Results Chart Add bookmark

EventSourceName	Channel	Task	Level	EventID	Activity	Auth
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

Showing 1 - 1 of 1. Display count: auto

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'

anal

+ Create Refresh Analytics workbooks Rule runs (Preview) Enable Disable Delete Import Export Columns Guides & Feedback

Configuration

Workspace manager (Preview)

Analytics

2 Active rules

More content at Content hub

Rules by severity

High (2) Medium (0) Low (0) Informational (0)

LEARN MORE About analytics rules

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique Add filter

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...	Fut	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.

Responder ☆ ...

Logic app

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Development Tools

Logic app designer

Logic app code view

Logic app templates

API connections

Quick start guides

Settings

Authorization

Access keys

Monitoring

Alerts

Diagnostic settings

Logs

Diagnostics

Automation

Tasks

Export template

Help

Run Refresh Edit Delete Disable Clone Open in mobile Export Provide feedback

JSON View

Essentials

Resource group (move) : CyberLab

Location (move) : North Central US

Subscription (move) : Azure subscription 1

Subscription ID : 267d54cf-db3a-48f4-af3b-15ce21152763

Workflow URL : --

Tags (edit) : Add tags

Definition : 1 trigger, 2 actions

Status : Enabled

Runs last 24 hours : 0 successful, 1 failed

Integration Account : --

Get started Run history Trigger history Metrics

Resubmit Add filter Specify the run identifier to open monitor view directly

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

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

Reply Forward

Tue 6/3/2025 2:25 AM

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