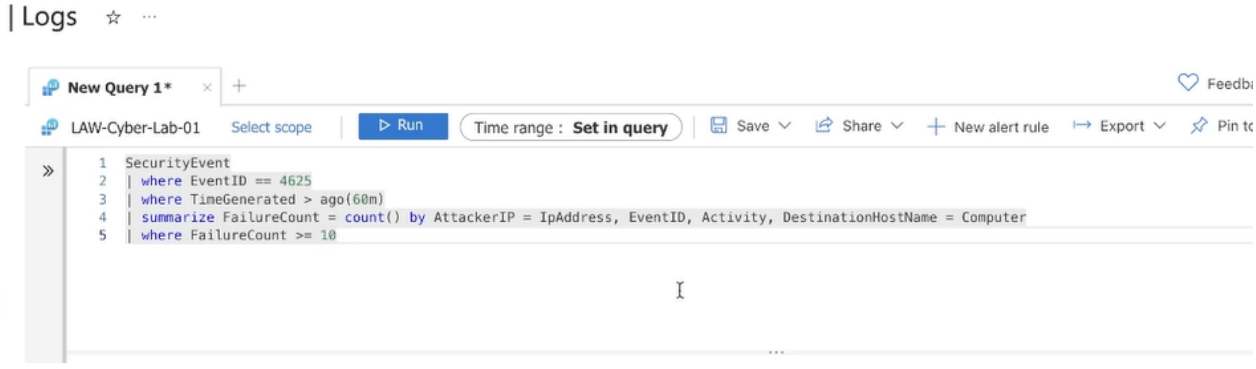
Incident Response
in
SIEM Microsoft Sentinel Using NIST 800-61

In this project I observed potential brute force attacks against Windows VM, this VM a part of the Security group created in Azure that was intentionally weakened by having weak login, inbound rules open to all traffic and firewalls turned off. Within the project I applied custom analytics rules that are query based that will be used to trigger potential alerts, this will then generate incidents within sentinel leading to performing the proper incident response procedures using NIST 800-61 Preparation, Detection and Analysis,Containment, Eradication and recovery, Post Incident Activity.

Preparation:

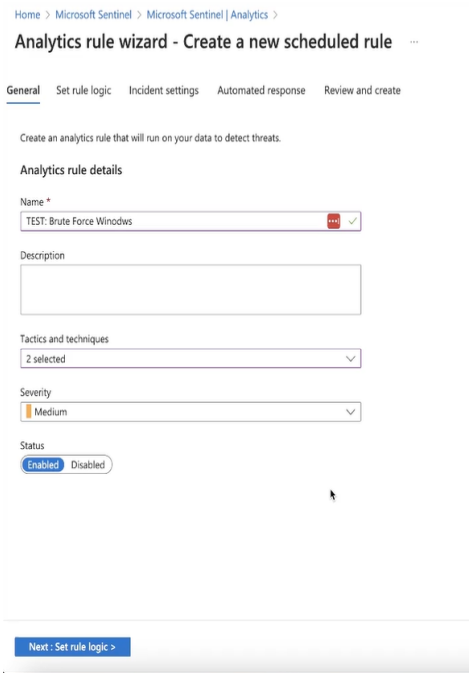
Initiated by having already ingested logs in Log analytics workspace and Sentinel then configure rules for alerts.

- Implemented this query that logs the alert when multiple failed logins which are likely brute force attempts. Here the query shows if there are 10 failed logins within a 1 hour period alert would be logged.

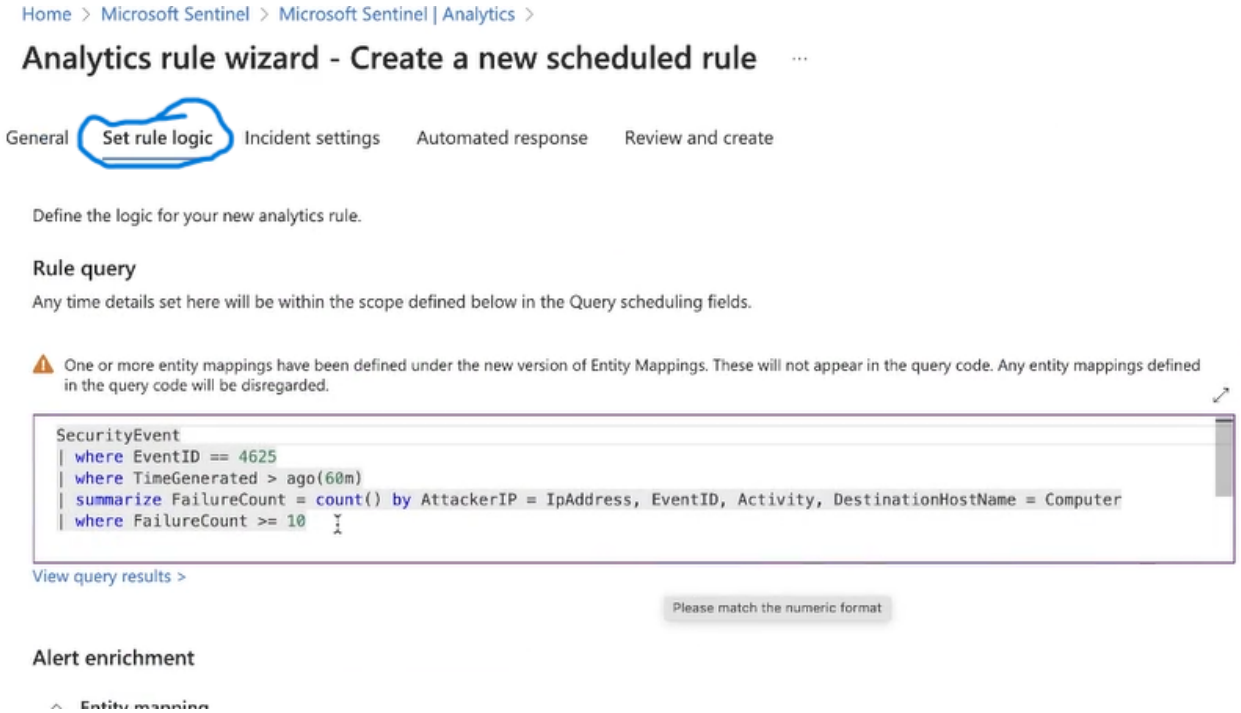


- Configured query rule Detection & Analysis:
  -setting severity, status, Owner
  -View full details
  -Observe Activity Log

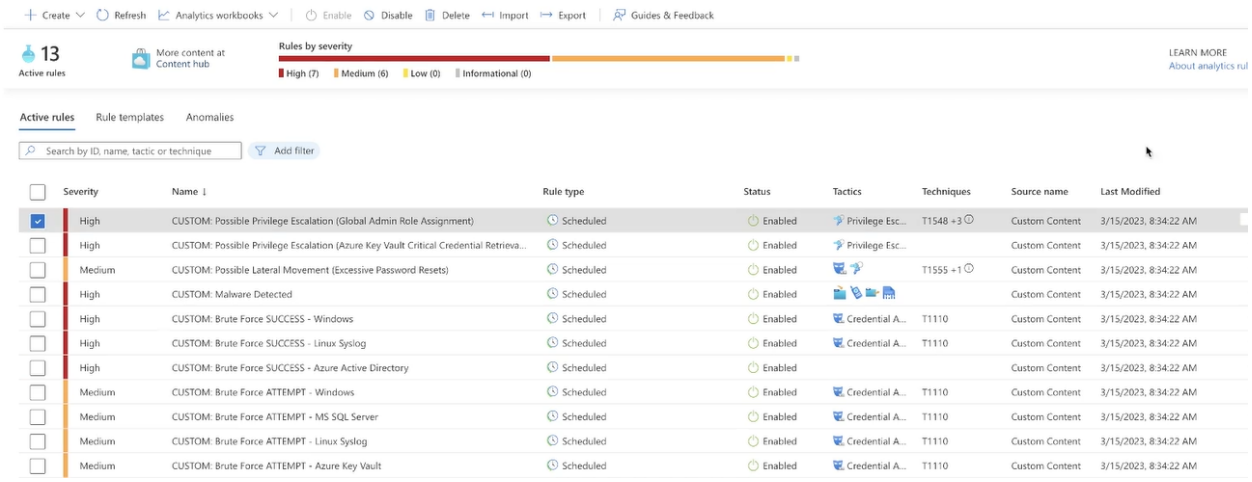
-Observe Entities and Incident timelines etc
-Determine true positive



- Setting rule logic

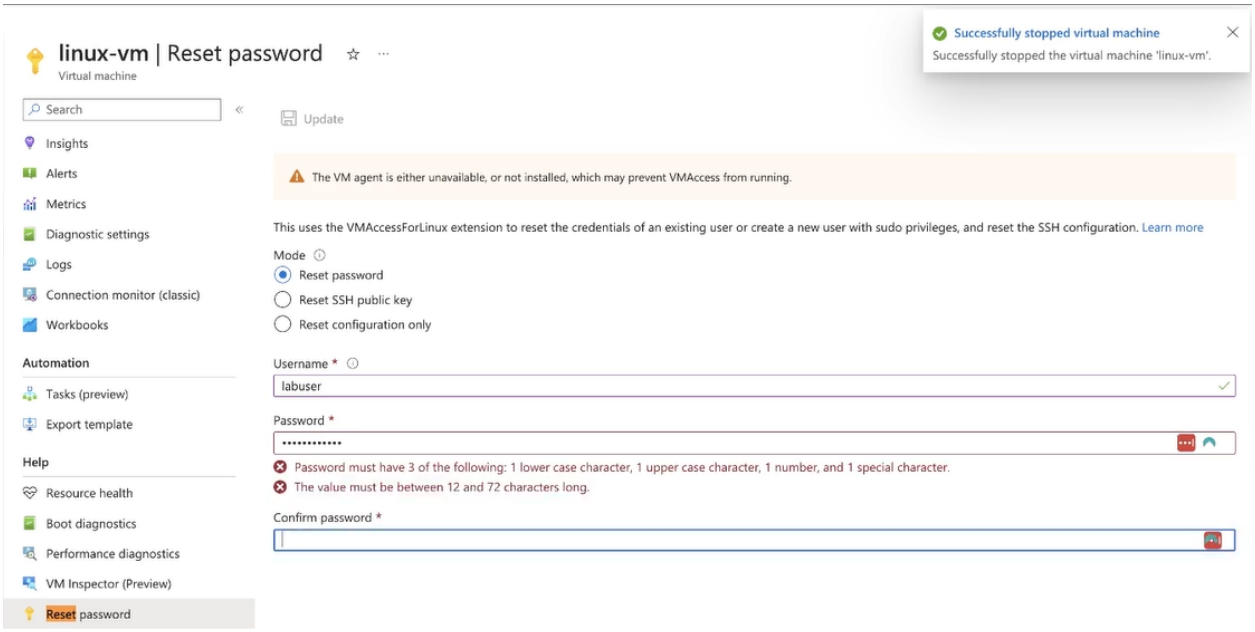


- Waited to trigger incident on intentionally weakened VM's host with the rules that have been set



Incident response Containment was done by stopping VM.

Eradication of incident by resetting password:



Recovery and Post Event Activity

- Determine the origin of the attack and determine if the targets are against anything else.
- Remediated incident by Resetting password of the host and enabling 2 multi factor authentication.
  -Locked down group where the host was present
- Assess potential impact of incident.