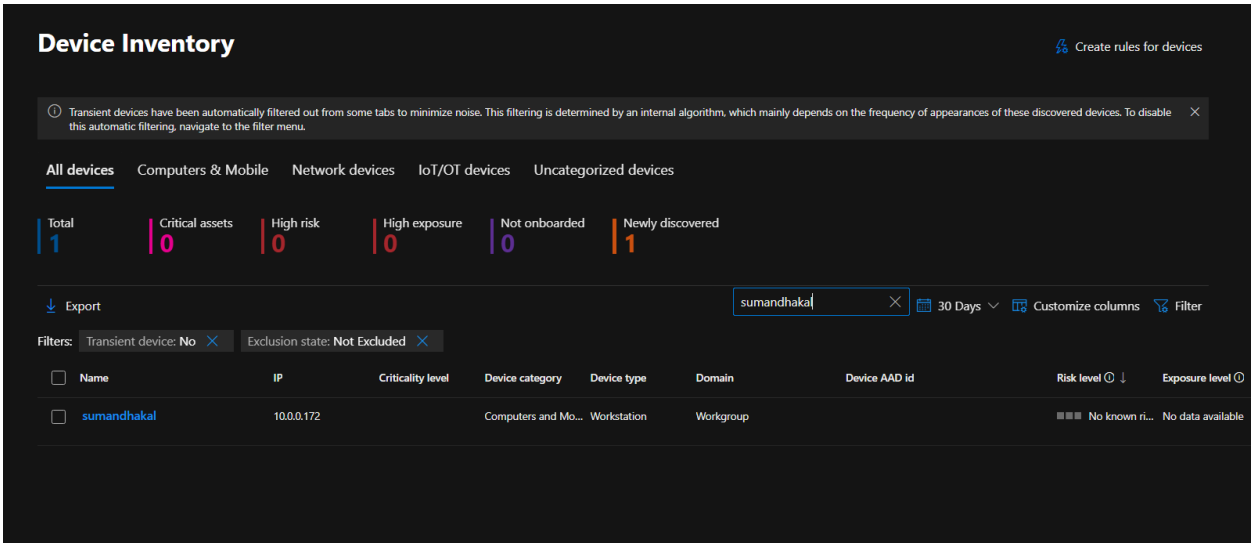
Scenario 1: Virtual Machine Brute Force Detection

For this Lab I have created a Virtual Machine using Microsoft Azure. This Virtual Machine has been Onboarded to Microsoft Defender for Endpoint (MDE).



Virtual Machine Device Name as shown in screenshot: sumandhakal
IP Address: 10.0.0.172

Explanation:

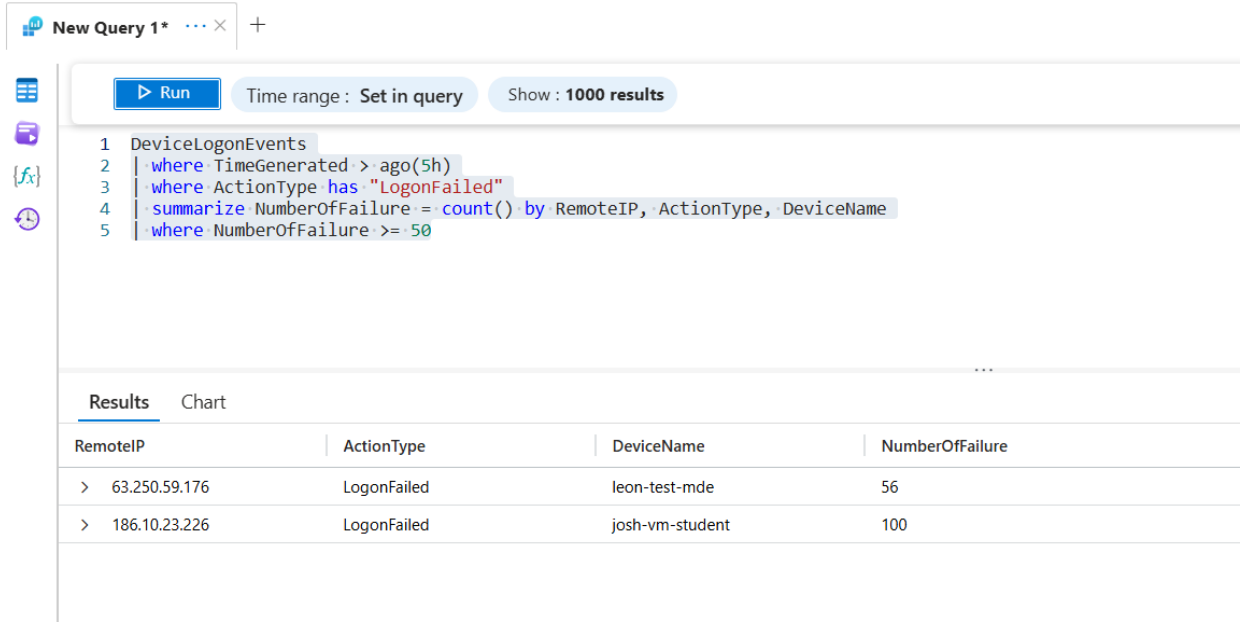
When entities (local or remote users, usually) attempt to log into a virtual machine, a log will be created on the local machine and then forwarded to Microsoft Defender for Endpoint under the DeviceLogonEvents table. These logs are then forwarded to the Log Analytics Workspace being used by Microsoft Sentinel, our SIEM. Within Sentinel, we will define an alert to trigger when the same entity fails to log into the same VM a given number of times within a certain time period. (i.e. 10 failed logons or more per 5 hours).

Part 1: Create Alert Rule (Brute Force Attempt Detection)

Design a Sentinel Scheduled Query Rule within Log Analytics that will discover when the same remote IP address has failed to log in to the same local host (Azure VM) 10 times or more within the last 5 hours.
Using the DeviceLogonEvents table, this query has been created:

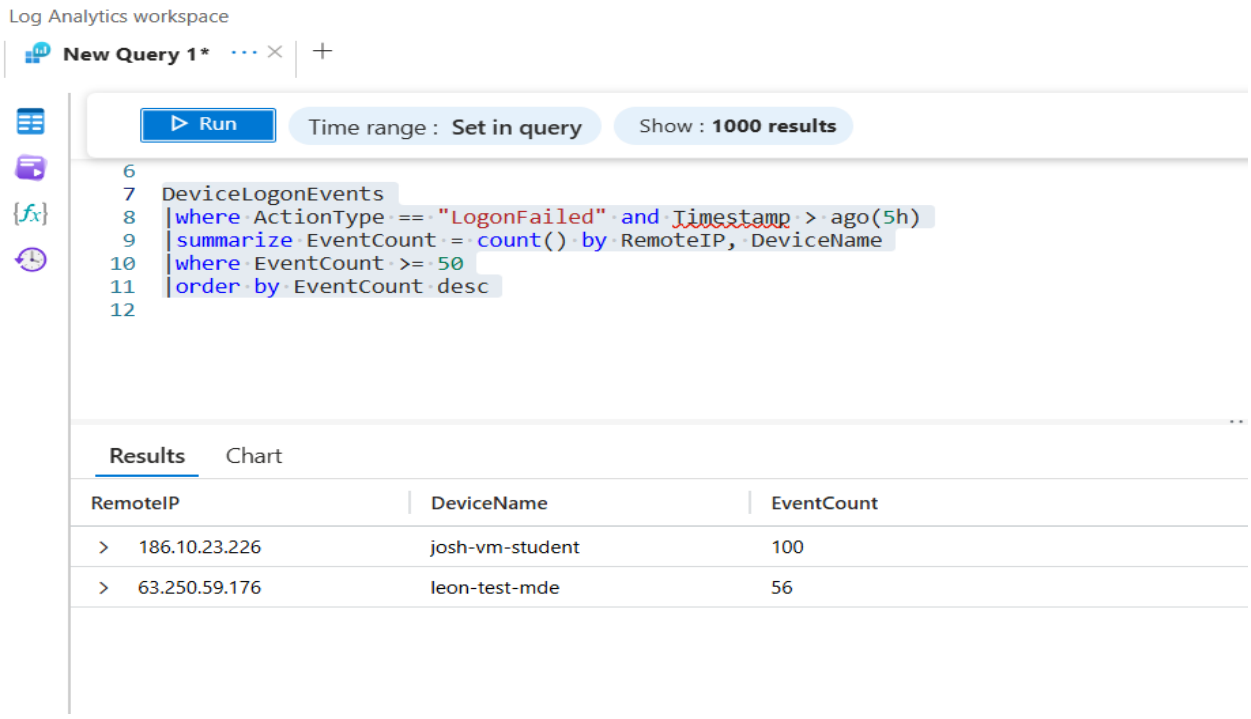
```
DeviceLogonEvents
 | where TimeGenerated >= ago(5h)
 | where ActionType has "LogonFailed"
```

```
| summarize NumberOfFailures = count() by RemoteIP, ActionType, DeviceName
| where NumberOfFailures >= 50
```



And this query has been created:

```
DeviceLogonEvents
| where ActionType == "LogonFailed" and Timestamp > ago(5h)
| summarize EventCount = count() by RemoteIP, DeviceName
| where EventCount >= 50
| order by EventCount desc
```



Now I created the Schedule Query Rule in: Sentinel → Analytics → Schedule Query Rule.

Analytics Rule Settings:

- Enable the Rule
- Set Mitre ATT&CK Framework Categories based on the query
- Run query every 4 hours
- Lookup data for last 5 hours (can define in query) ● Stop running query after alert is generated == Yes
- Configure Entity Mappings for the Remote IP and DeviceName
- Automatically create an Incident if the rule is triggered ● Group all alerts into a single Incident per 24 hours
- Stop running query after alert is generated (24 hours)

This is the Rule script:

```
DeviceLogonEvents
 | where TimeGenerated >= ago(5h)
 | where ActionType has "LogonFailed"
 | summarize NumberOfFailures = count() by RemoteIP, ActionType, DeviceName
 | where NumberOfFailures >= 30
```

Relevant MITRE ATT&CK Techniques:

T1110 – Brute Force

Sub-technique: T1110.001 – Password Guessing

Repeated failed login attempts from the same remote IP address fit this

exactly. (Optional, depending on interpretation)

T1078 – Valid Accounts

If successful logins are later seen from the same IP after failures, it may indicate stolen/guessed credentials.

How it would be written in the rule:

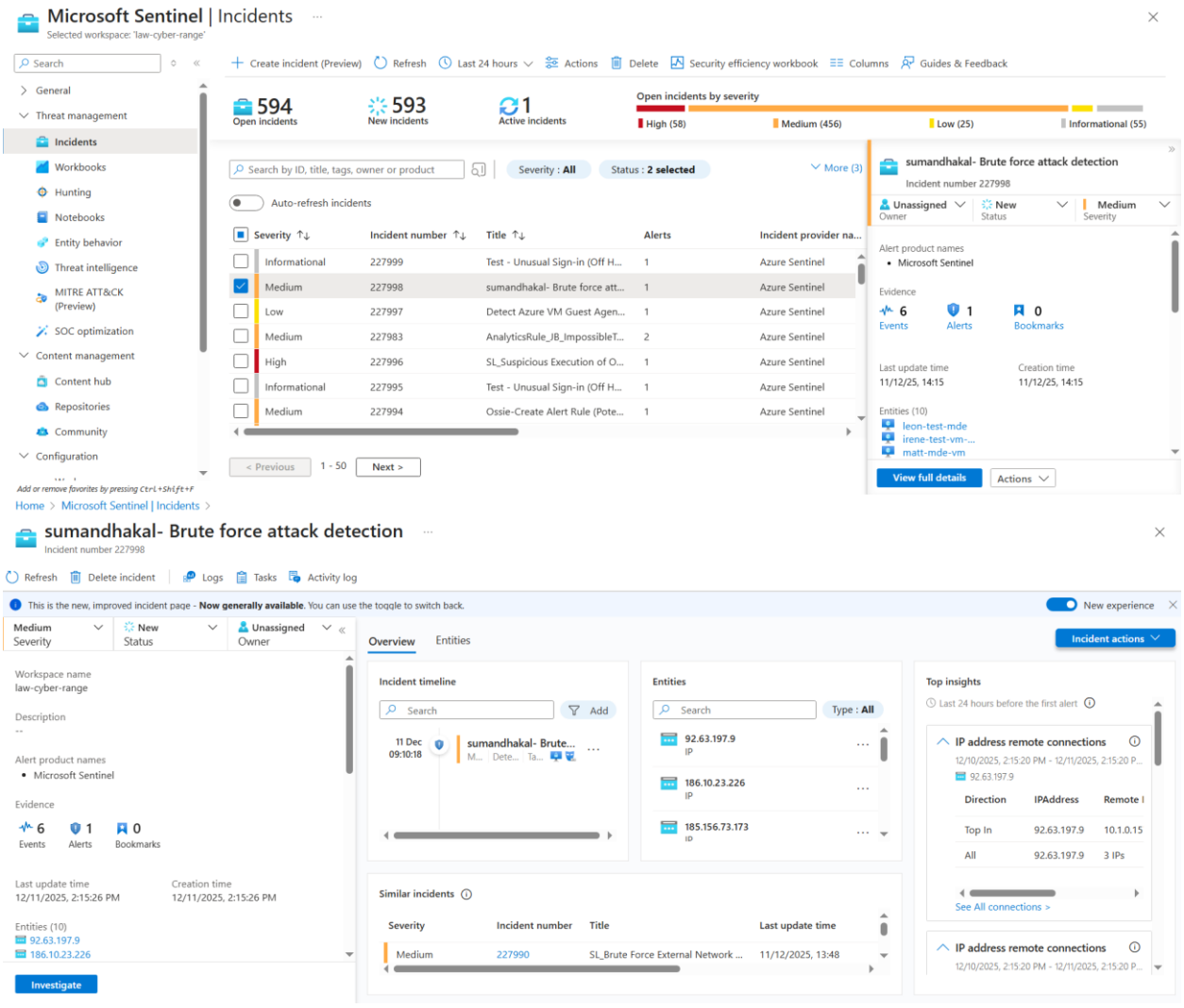
MITRE ATT&CK Mapping:

T1110 – Brute Force (T1110.001 – Password Guessing)

Possible related: T1078 – Valid Accounts

Part 2: Trigger Alert to Create Incident

Generated Alert:



These alerts were generated immediately after creating and launching this detection rule. 6 total events at this time

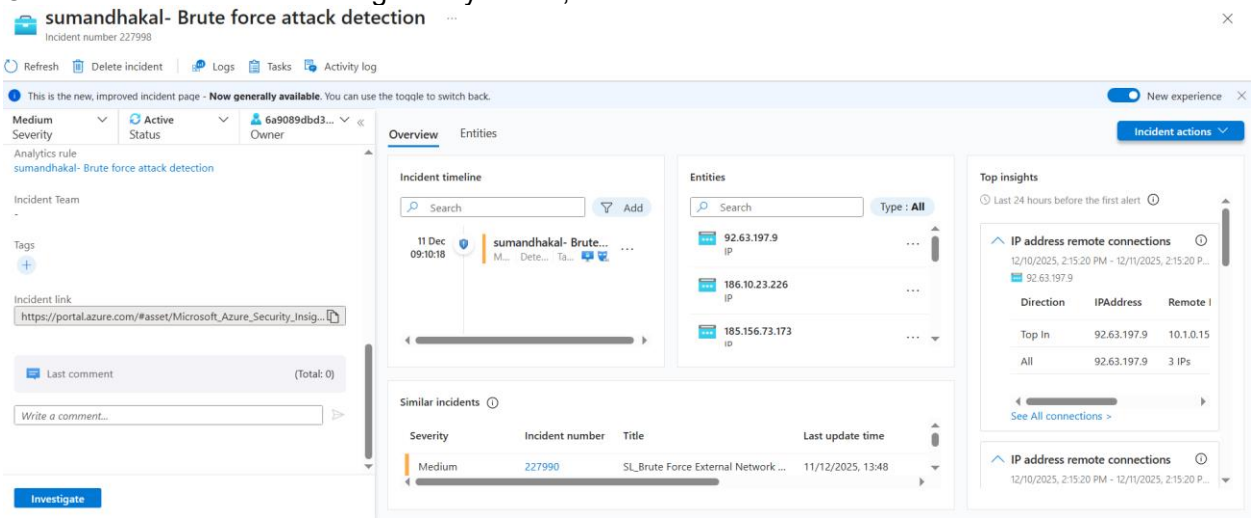
Part 3: Work Incident

Now this incident is worked to completion and will be closed out, in accordance with the NIST 800-61: Incident Response Lifecycle.

Detection and Analysis Steps:

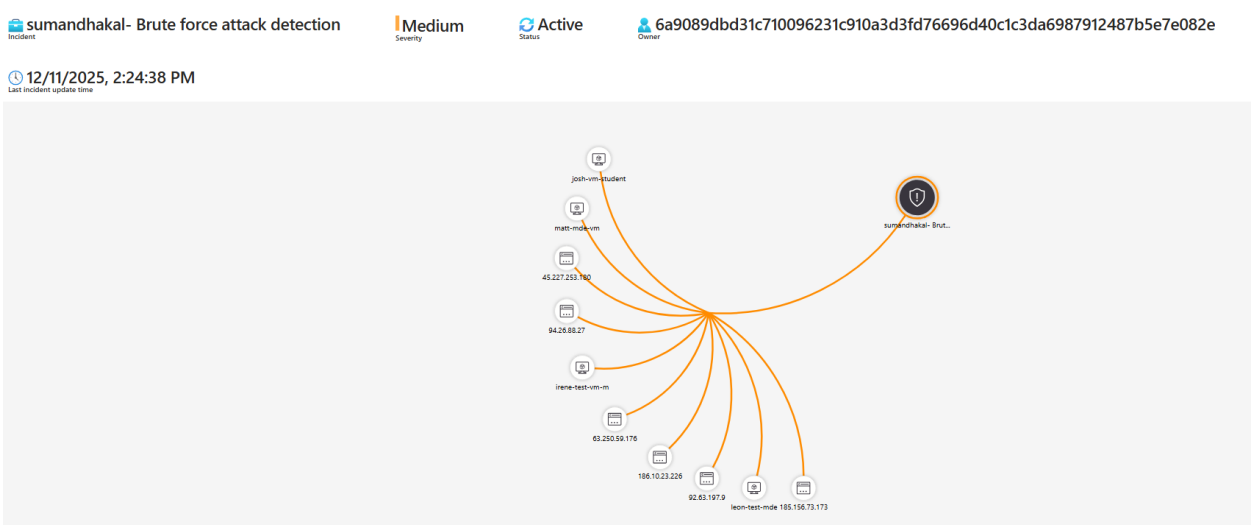
Identify and validate the incident.

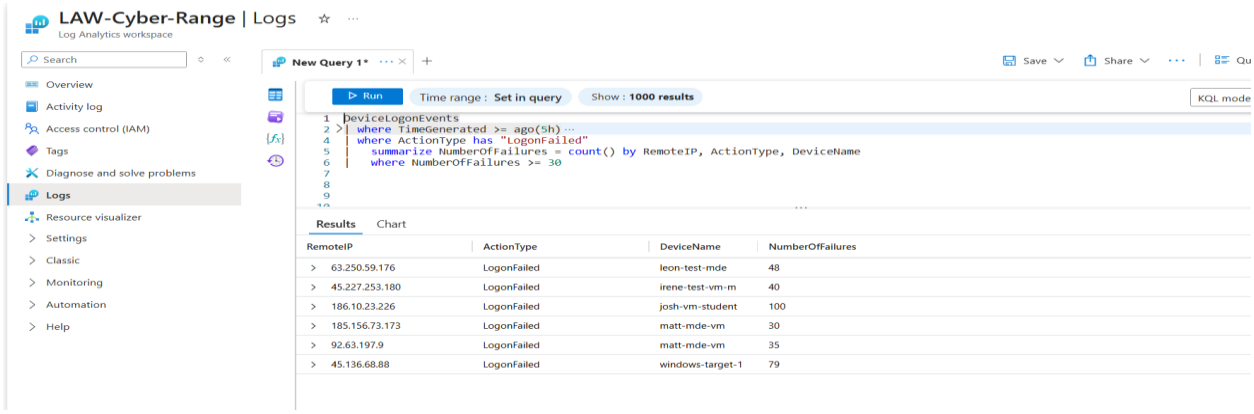
Observe the incident and assign it to yourself, set the status to Active



Investigate the Incident by Actions → Investigate Gather relevant evidence and assess impact.

Observations of the different entity mappings and notes:





This evidence shows the 6 remote IP addresses that are attempting to Brute Force their way into the Virtual Machine that run alongside this one on the Cyber Range System

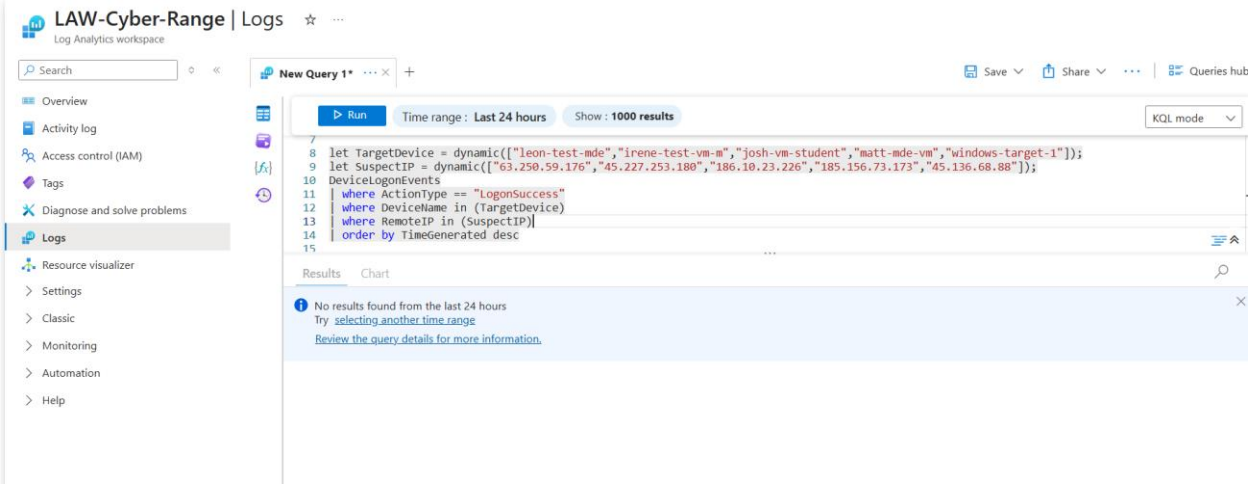
Containment, Eradication, and Recovery Steps:

- **Checked to make sure none of the IP addresses attempting to brute force the machine actually logged in.**

Ran this script to verify that there were no "LogonSuccess" in the ActionType from this suspicious IP Address: 5.188.118.202

```
let TargetDevice = dynamic(["leon-test-mde","irene-test-vm-m","josh-vm-student","matt-mde-vm","windows-target-1"]);
let SuspectIP = dynamic(["63.250.59.176","45.227.253.180","186.10.23.226","185.156.73.173","45.136.68.88"]);
DeviceLogonEvents
| where ActionType == "LogonSuccess"
| where DeviceName in (TargetDevice)
| where RemoteIP in (SuspectIP)
| order by TimeGenerated desc
```

This was the return:



No results found from the last 24 hours
Try selecting another time range

There were no "LogonSuccess" in the ActionType from these suspicious IP Addresses,

---

Isolated affected systems/Virtual Machines to prevent further damage.

This can be done with Defender for Endpoint.
Conducted Anti-Virus and Anti-Malware scans.

For future prevention, there will be created or updated Network Security Group (NSG) rules attached to your Virtual Machine to prevent any traffic except your local PC from reaching the VM.

NSG was locked down to prevent RDP attempts from the public internet.
Corporate policy was proposed to require this for all VMs going forward. (this can be done with Azure Policy)

Brute Force was not successful, so no threats related to this incident.

Summary:

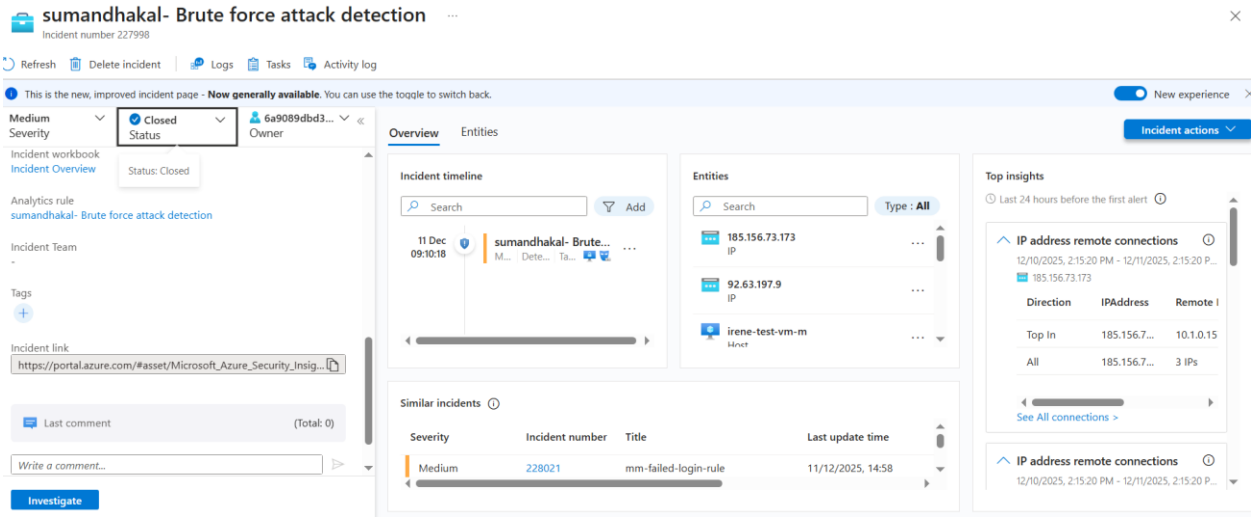
This detection rule monitors the DeviceLogonEvents table in Microsoft Sentinel for brute force activity against Azure VMs. It triggers when the same remote IP fails to log in 30 or more times within a 5-hour window. In this scenario, the rule identified multiple external IPs attempting repeated logons against the VM in the Cyber Range System. No successful logons were observed from the suspicious IPs. Containment and recovery steps included verifying no credential compromise, isolating the VM, and applying stricter NSG rules to block RDP from the internet.

MITRE ATT&CK Mapping:

T1110 – Brute Force (T1110.001 – Password Guessing)

Possible related: T1078 – Valid Accounts (if success occurs after failures)

Closed out the Status.



This has been classified as a “True Positi