Lab #12: **Manual Alert Creation**

Purpose:

- We'll be creating alerts in Sentinel. In this lab, we'll create one custom 'test' alert (which looks for brute force attempts against our Windows VM).

Tasks:

1. **Create a test 'Brute Force Attempt' rule in Sentinel**
2. **Test a custom query in Log Analytics workspace**
3. **Attempt to trigger the rule**
4. **View the incident in Sentinel**
5. **Delete the rule when finished**

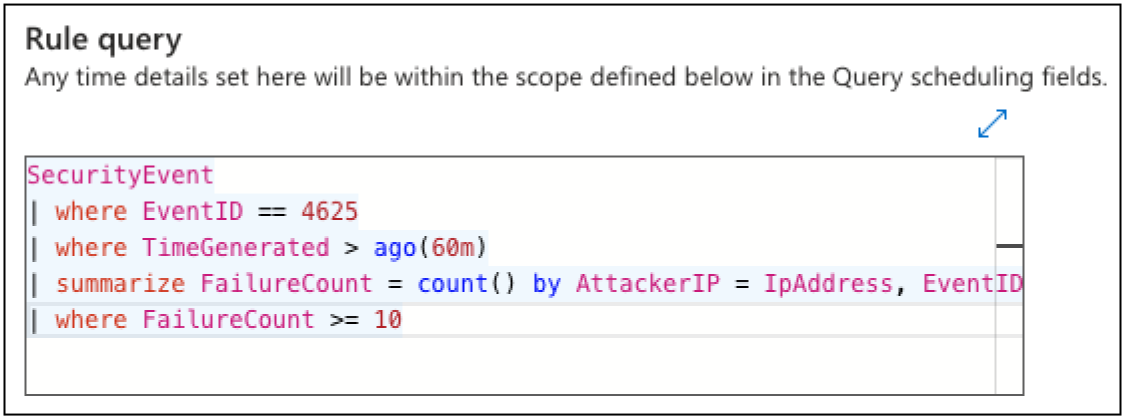
Task 1: Create a test 'Brute Force Attempt' rule in Sentinel

1. **Azure** portal > **Sentinel** > select your workpace > **Analytics** > **Create** > **Scheduled Query Rule**

   > ***Note***: *The 'Analytics' section of Sentinel is where we create alerts ("rules"). We'll be creating a scheduled query rule.*

2. **General** tab:
   a. **Name**: TEST: Brute Force ATTEMPT - Windows
   b. **Description**: When the same person fails to log into the same VM at least 10 times in the last 60 minutes.
3. **Set Rule Logic** tab:
   a. Paste this custom query into the **Rule Query** box:

```
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = IpAddress, EventID, Activity, DestinationHostName = Computer
| where FailureCount >= 10
```

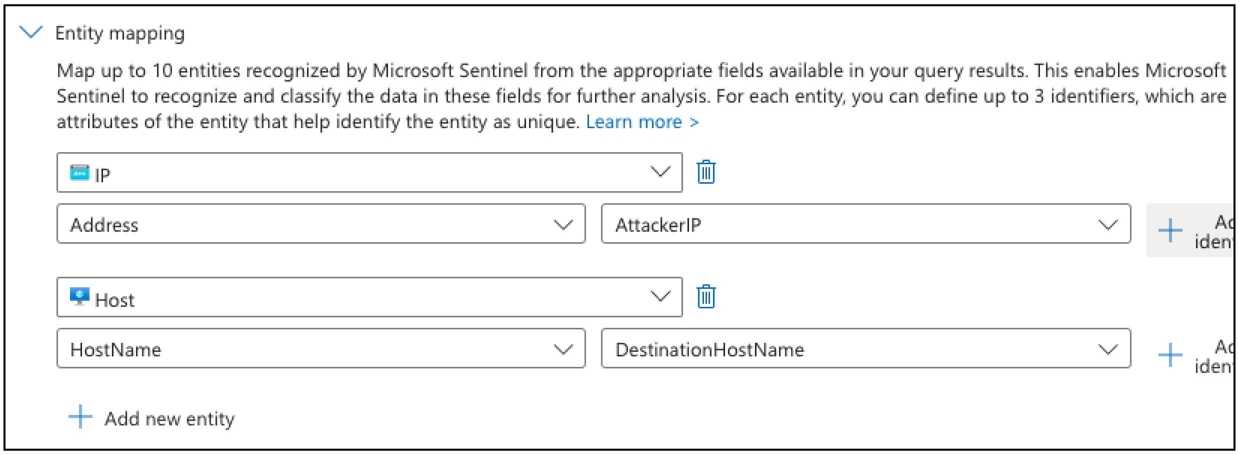


Rule query

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

```
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = IpAddress, EventID
| where FailureCount >= 10
```

b. Select **Entity Mapping** > +**Add new entry** >



Entity mapping

Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. Learn more >

IP

Address — AttackerIP

Host

HostName — DestinationHostName

> ***Note**: If multiple bad logins occur from a single AttackerIP, it'll allow Sentinel to correlate this data and recognize malicious hosts and IPs.*

c. **Query Scheduling**: Run query every 5 minutes, Lookup data from the last 5 hours.

d. **Alert Threshold**: Is greater than 0.

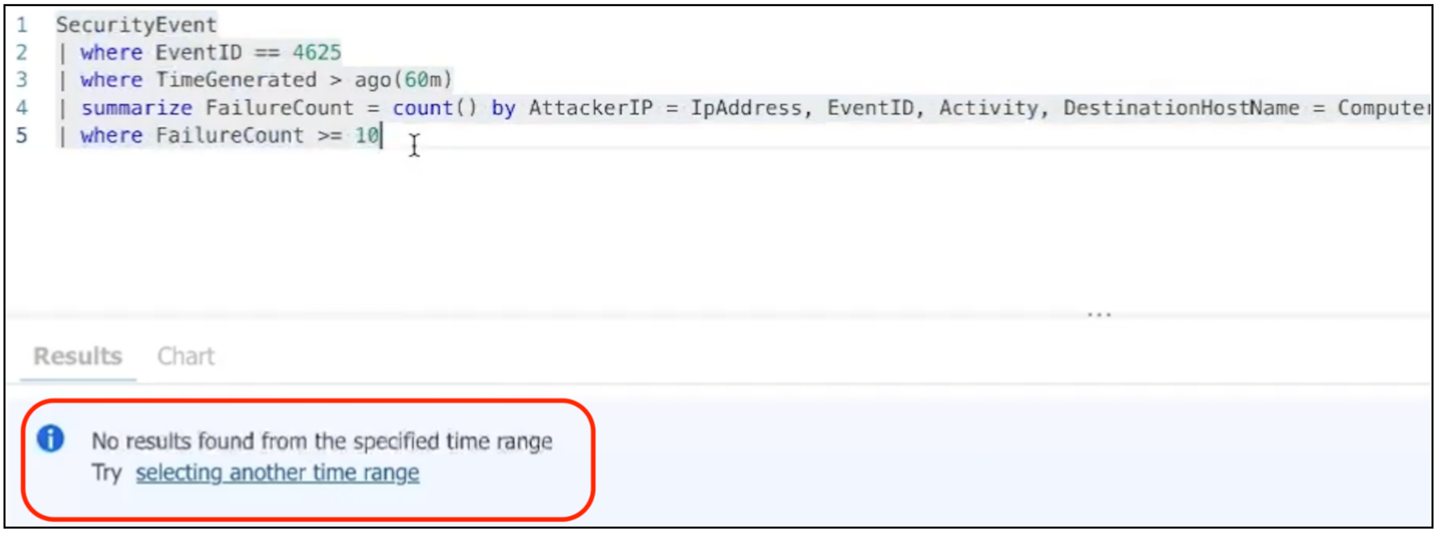
e. **Event Grouping**: Group all events into a single alert.

f. **Supression**: OFF.

4. **Incident Settings** tab:
    a. **Create incidents from alerts triggered by this analytics rule**: Enabled.
    b. **Alert grouping**: Enabled.
    c. **Re-open closed matching incidents**: Disabled.
5. **Automated Response** tab:
    a. (skip)
6. **Review and Create** tab:
    a. Select **Save**.

Task 2: Test a custom query in Log Analytics workspace

1. **Azure** portal > **Log Analytics workspace** > select your workspace > **Logs**
2. In the query box, paste the custom query (above):
3. Run the command.



```
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = IpAddress, EventID, Activity, DestinationHostName = Compute
| where FailureCount >= 10
```

No results found from the specified time range
Try selecting another time range

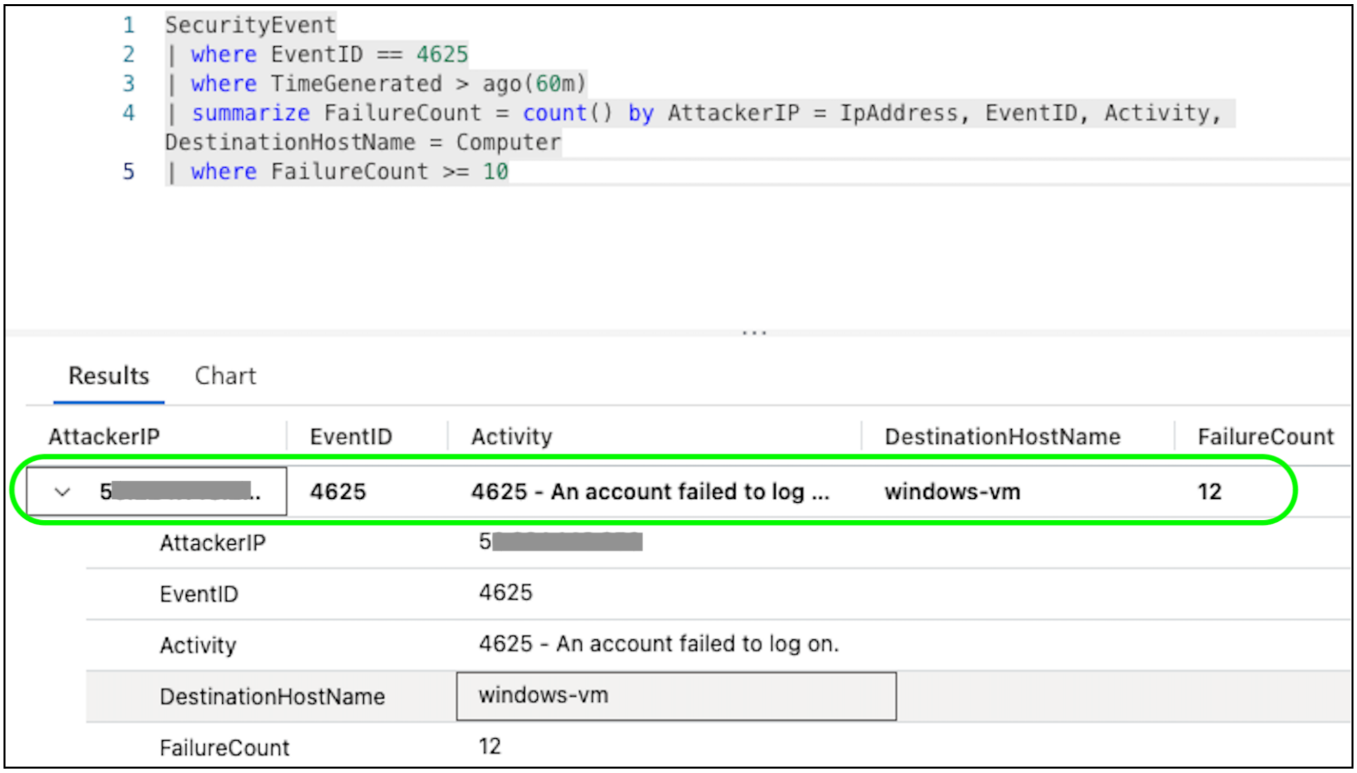
> ***Note**: No results appeared yet, so let's try to trigger the rule by attempting failed logon attempts.*

Task 3: Attempt to trigger the rule

1. Open your **Windows Remote Desktop app** > select the **windows-vm**.

   ***Note**: Verify the windows-vm Public IP by going to **Azure** > **Virtual Machines**.*

   a. Attempt to sign in 10x using incorrect credentials.
   b. Done. Close the **Windows Remote Desktop** app.
2. Go back to **Azure** portal > **Log Analytics workspace** > select your workspace > **Logs**
   a. In the query box, paste the custom query (above):
   b. Re-run the command:



```
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = IpAddress, EventID, Activity,
DestinationHostName = Computer
| where FailureCount >= 10
```

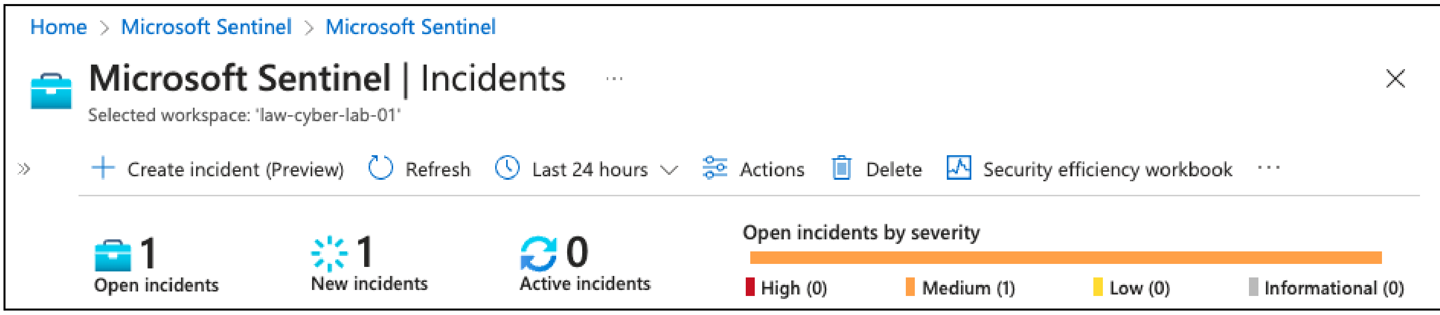
AttackerIP	EventID	Activity	DestinationHostName	FailureCount
5[redacted]..	4625	4625 - An account failed to log ...	windows-vm	12

AttackerIP	5[redacted]
EventID	4625
Activity	4625 - An account failed to log on.
DestinationHostName	windows-vm
FailureCount	12

Task 4: View the incident in Sentinel

1. **Azure** portal > **Sentinel** > select your workpace > **Incidents**

   ***Note**: We see one new incident!*



Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'law-cyber-lab-01'

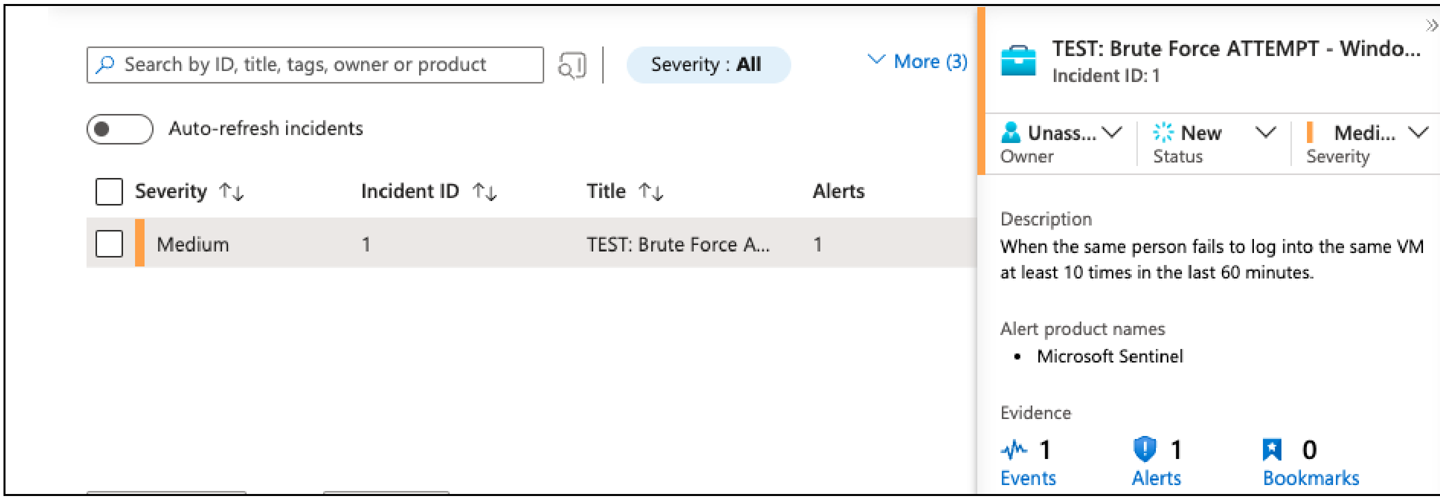
1 Open incidents

1 New incidents

0 Active incidents

Open incidents by severity

🟥 High (0) 🟧 Medium (1) 🟨 Low (0) ⬜ Informational (0)



Search by ID, title, tags, owner or product

Severity : **All**

More (3)

Auto-refresh incidents

□ Severity	Incident ID	Title	Alerts
□ Medium	1	TEST: Brute Force A...	1

TEST: Brute Force ATTEMPT - Windo...
Incident ID: 1

Unass... Owner | New Status | Medi... Severity

Description
When the same person fails to log into the same VM at least 10 times in the last 60 minutes.

Alert product names
- Microsoft Sentinel

Evidence
1 Events | 1 Alerts | 0 Bookmarks

Task 5: Delete the rule when finished

1. **Azure** portal > **Sentinel** > select your workpace > **Analytics** >
2. Select the checkbox of the ‘TEST’ rule > **Delete**

End:

- We tested the creation of a SIEM rule. In future labs we’ll be importing more rules and triggering more incidents.