

Sentinel: Creating a Scheduled Query Rule

Scheduled query rules are custom analytics rules in Microsoft Sentinel that automatically run queries on collected data at regular intervals. These rules help detect specific patterns or suspicious activities and can generate alerts and incidents based on defined thresholds.

Key Features:

1. **Automated Detection:** Run KQL (Kusto Query Language) queries on data in the Log Analytics workspace. Detect anomalies, breaches, or specific security events.
2. **Customizable:** Define specific conditions (e.g., Event ID, time range) to suit organizational needs. Adjust thresholds and intervals for alerts.
3. **Alert Generation:** Trigger alerts when query results meet predefined criteria (e.g., more than one failed login attempt in 5 minutes).
4. **Incident Creation:** Automatically convert alerts into incidents for detailed investigation. Assign tactics or metadata (e.g., "Brute Force" for failed login attempts).
5. **Flexible Scheduling:** Specify the query's run frequency (e.g., every 5 minutes, every hour). Define the data lookback period for analysis.
6. **Integration:** Combine with automation rules for immediate response actions.

Use Cases:

1. Detect brute force attacks by monitoring failed login attempts.
2. Identify suspicious data exfiltration patterns.
3. Monitor specific event IDs or log patterns in security data.

The end goal of creating a rule in Microsoft Sentinel is to proactively detect and respond to potential security threats, such as failed login attempts (e.g., Event ID 4625). By setting up a scheduled query rule, Microsoft Sentinel monitors security events in near real-time, triggers alerts when specific thresholds are met, and generates incidents for investigation. This process enables security engineers to identify suspicious activities, such as brute force attacks, and take necessary actions to mitigate risks. Ultimately, it strengthens an organization's security posture by automating threat detection and facilitating efficient incident management and resolution.

To begin with the lab

1. In the previous lab you have learned how data is being collected via data connector in Microsoft Sentinel. Now in this lab, you will create a rule that look at this data.
2. Ensure data is being collected in the Log Analytics workspace using the data connector.

Logs ... vmworkspace120

New Query 1* ... +

Save Share ... Queries hub

Run Time range: Last 24 hours Limit: 30000 KQL mode

```

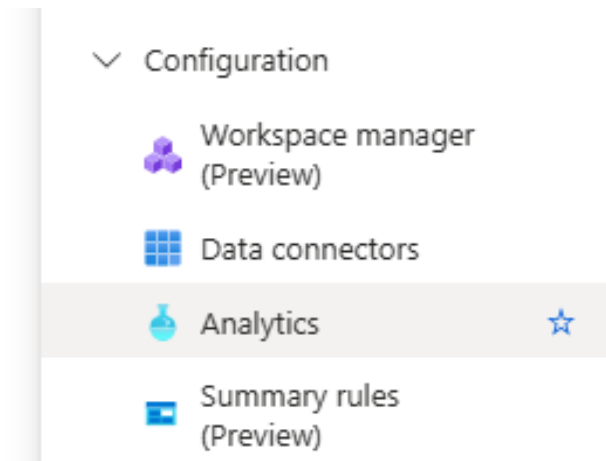
1 SecurityEvent
2

```

Results Chart

TimeGenerated [UTC] ↑↓	Account	AccountType	Computer	EventSourceName	Channel	Task
> 12/20/2024, 11:28:18.020 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security	1:1
> 12/20/2024, 11:28:18.020 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security	1:1
> 12/20/2024, 11:28:18.012 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security	1:1
> 12/20/2024, 11:28:18.012 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security	1:1
> 12/20/2024, 11:27:18.010 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security	1:1
> 12/20/2024, 11:27:18.010 AM	WORKGROUP\demo-vm\$	Machine	demo-vm	Microsoft-Windows-Security-A...	Security	1:1

- Access Microsoft Sentinel within the Azure portal and proceed to the Analytics section in the left pane.



- Click on **Create Scheduled Query Rule**.

Microsoft Sentinel | Analytics ...

Selected workspace: 'vmworkspace120'

Search

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Create Refresh Analytics workbooks Rule runs (Preview) Enable

Scheduled query rule

NRT query rule

Microsoft incident creation rule

Rules by severity

High (1) Medium (0) Low (0) Inform

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique Add filter

Severity	Name	Rule t...	Status	Tactics
High	Advanced Multi...	Fu:	Enabled	Collection + 11

5. Now name the analytics rule (e.g., "Rule 4688").

Analytics rule wizard - Create a new Scheduled rule ...

General Set rule logic Incident settings Automated response Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *

Rule-4688

Description

Severity

Medium

6. And then select the event type to monitor (e.g., failed logins, Event ID 4688). You can set up a rule in Microsoft Sentinel to detect specific events, like failed login attempts (Event ID 4688). When such an event is detected, you can configure Sentinel to trigger an incident. You can also add additional context, like tagging the incident with relevant metadata.
7. Select credential access and then select Brute Force.

✓ ☒ Credential Access

- > ☐ T1003 - OS Credential Dumping
- ☐ T1040 - Network Sniffing
- > ☐ T1056 - Input Capture
- > ☒ T1110 - Brute Force
- ☐ T1111 - Two-Factor Authentication Interception
- ☐ T1187 - Forced Authentication
- ☐ T1212 - Exploitation for Credential Access

8. Now go to Set Rule Logic and enter following query in query pane:

SecurityEvent
where EventID == '4688'

Alert threshold

Generate alert when number of query results *

Is greater than

Event grouping

Configure how rule query results are grouped into alerts

- ☐ Group all events into a single alert
- ☒ Trigger an alert for each event

11. Enable **incident generation** for each alert. Optionally, map the rule to tactics like "Credential Access" or "Brute Force." Double-check all settings. Click **Create** to finalize the rule.
12. Wait **10-15 minutes** for the rule to generate alerts. Then go to the **Incidents** section under **Threat Management**.

The screenshot shows the Microsoft Sentinel 'Incidents' page. On the left, the navigation pane is open, showing 'General' and 'Threat management' sections. Under 'Threat management', 'Incidents' is selected. The main content area shows three incident counts: 'Open incidents' (0), 'New incidents' (0), and 'Active incidents' (0). Below these counts is a search bar with the placeholder text 'Search by ID, title, tags, owner or product'. There is also a toggle for 'Auto-refresh incidents' which is currently turned off. At the bottom, a table header is visible with columns for 'Severity' (sortable), 'Incident number' (sortable), and 'Title' (sortable).

13. Open incidents to review details like Event ID and activity. Assign incidents to a security engineer for further investigation.