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.

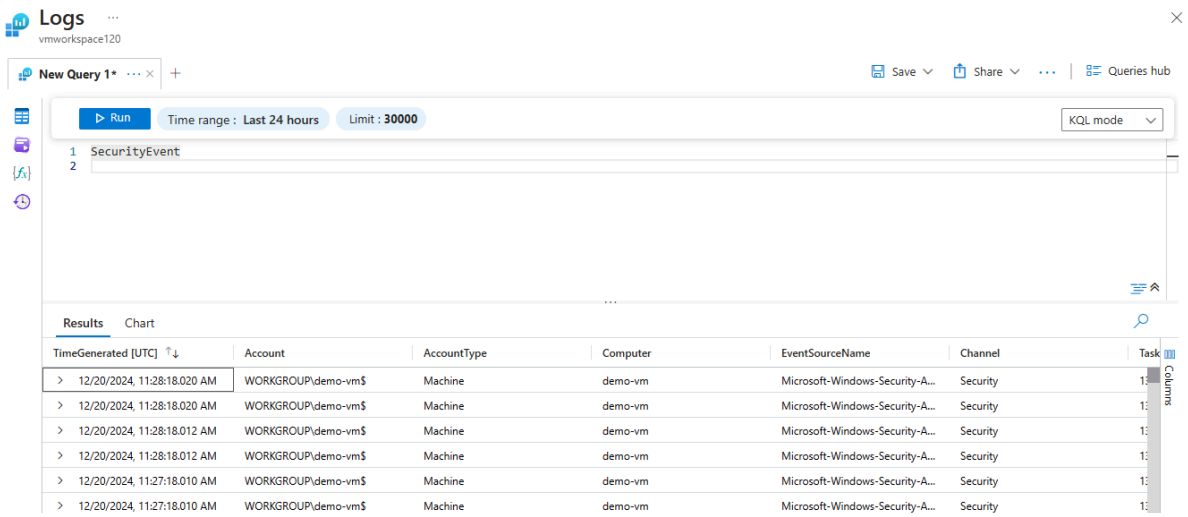
Use Cases:

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.

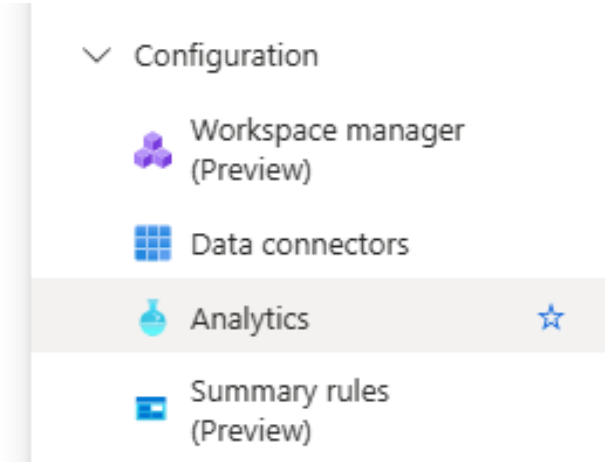
The end goal of creating a rule in Microsoft Sentinel is to proactively detect and respond to potential security threats, such as failed login attempts (e.g., Event ID 4625). By setting up a scheduled query rule, Microsoft Sentinel monitors security events in near real-time, triggers alerts when specific 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

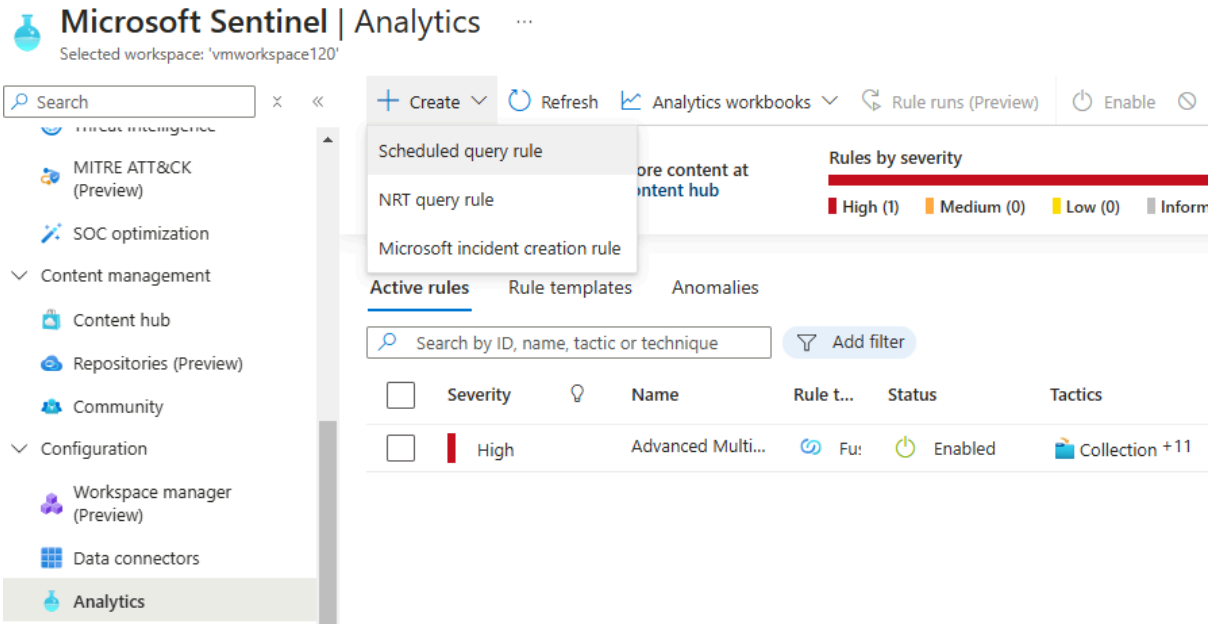
1. In the previous lab you have learned how data is being collected via data connector in Microsoft Sentinel. Now in this lab, you will create a rule that look at this data.
2. Ensure data is being collected in the Log Analytics workspace using the data connector.



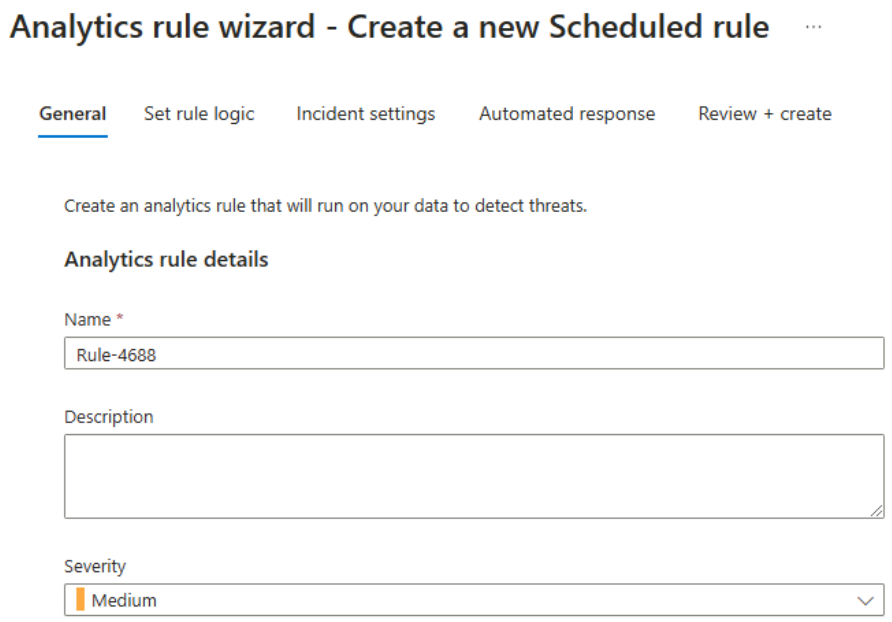
3. Access Microsoft Sentinel within the Azure portal and proceed to the Analytics section in the left pane.



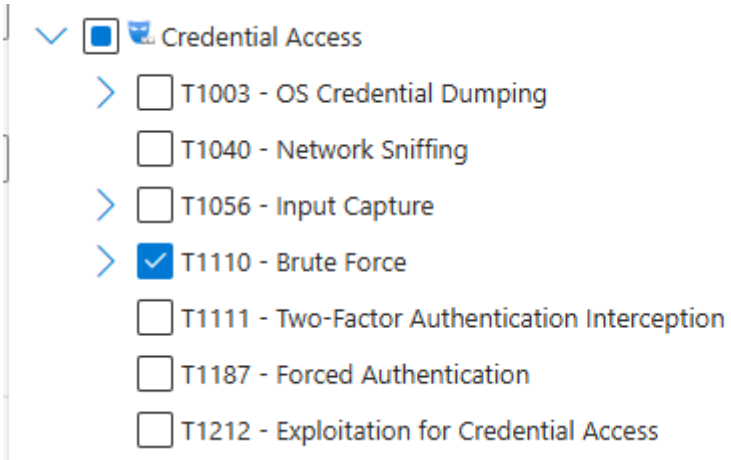
4. Click on **Create Scheduled Query Rule**.



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

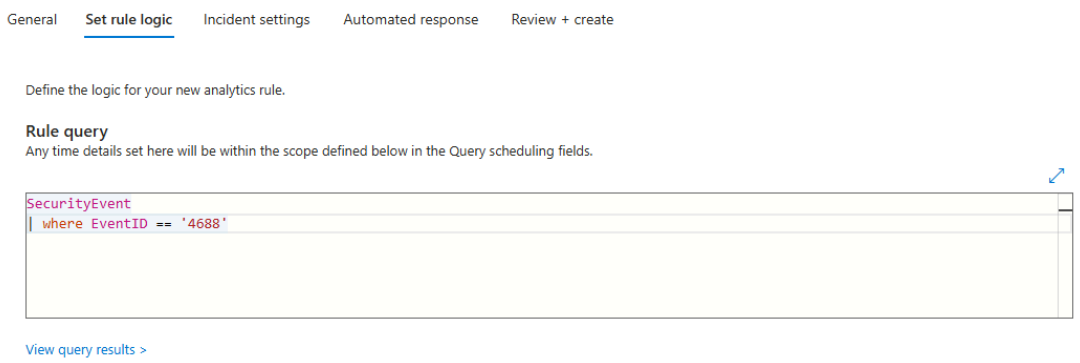


6. And then select the event type to monitor (e.g., failed logins, Event ID 4688). You can set up a rule in Microsoft Sentinel to detect specific events, like failed login attempts (Event ID 4688). When such an event is detected, you can configure Sentinel to trigger an incident. You can also add additional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

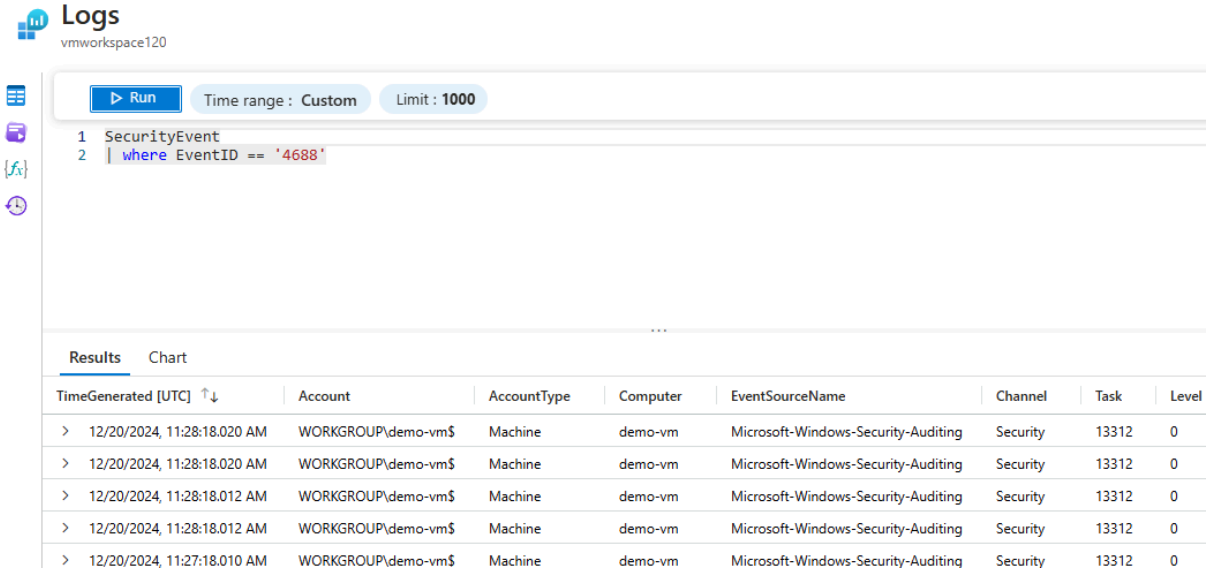


8. Now go to Set Rule Logic and enter following query in query pane:

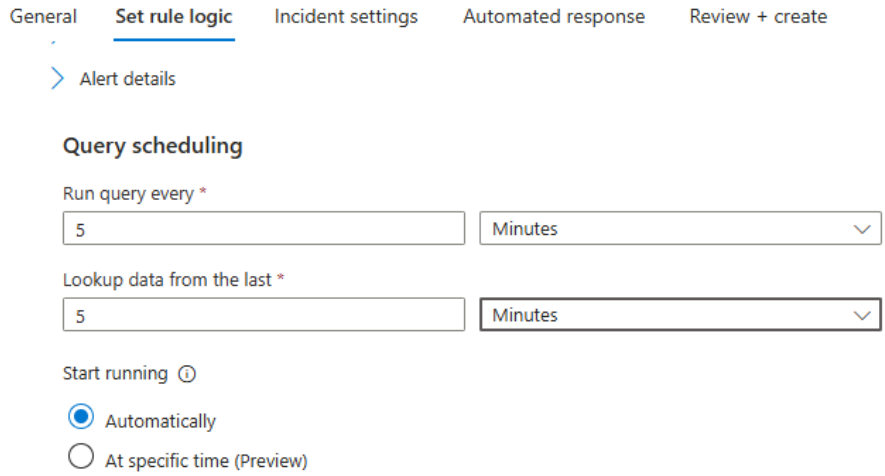
SecurityEvent
where EventID == '4688'

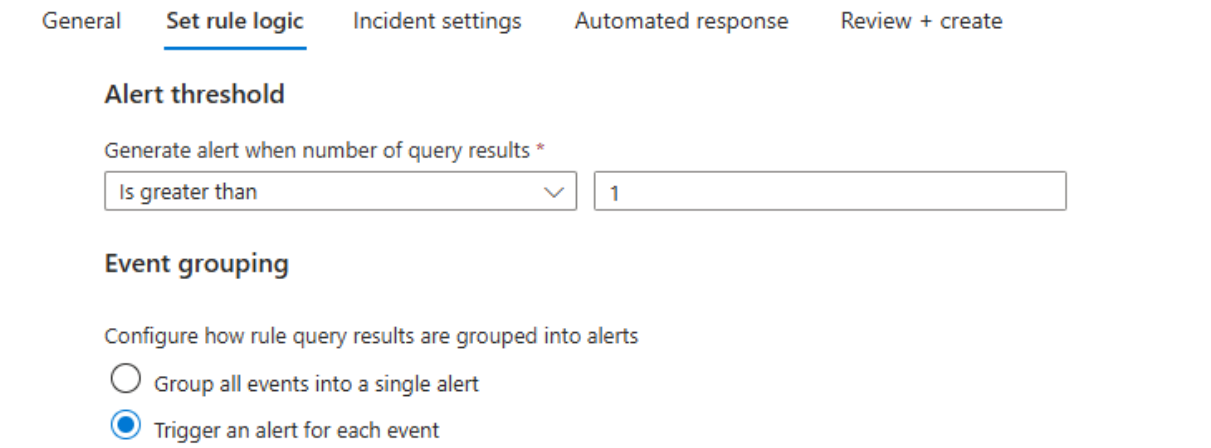


9. Test the query to confirm it captures the intended events.

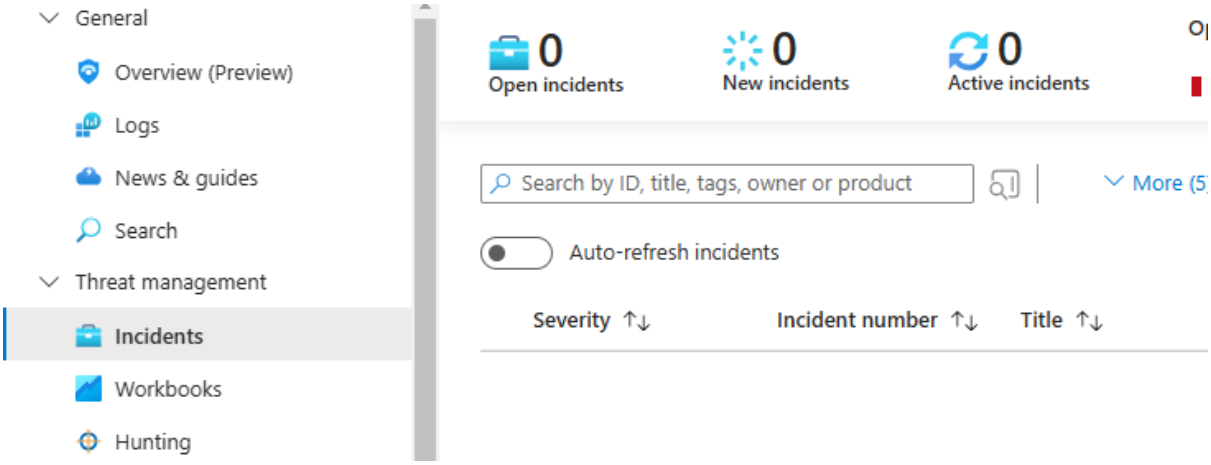


10. Configure the query to execute at five-minute intervals. Examine the data collected over the preceding five minutes. Establish a threshold for alerts (for instance, activate if results exceed 1).





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**.



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