Microsoft Sentinel - Collecting Data

A **data connector** in Microsoft Sentinel is a feature that integrates various data sources into the Sentinel platform, enabling seamless collection and analysis of security data. It acts as a bridge between Microsoft Sentinel and external systems, services, or applications, allowing them to send logs and telemetry data to the underlying Log Analytics workspace for monitoring and investigation.

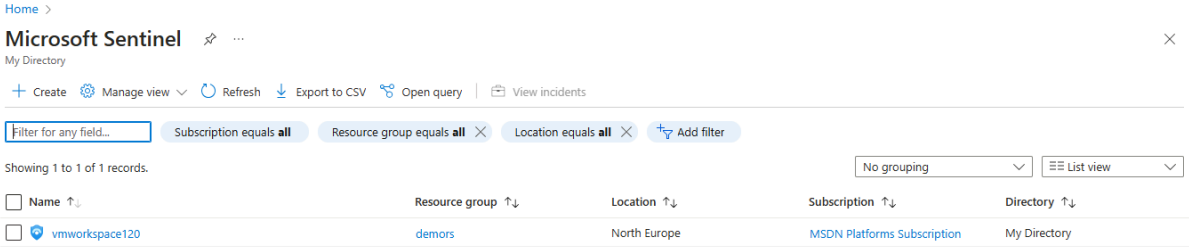
Key Points About Data Connectors:

1. **Sources**: Collect data from Microsoft services (e.g., Azure, Office 365) and third-party systems (e.g., firewalls, endpoint protection tools).
2. **Types**: Includes built-in connectors for popular systems and custom connectors for unique use cases.
3. **Purpose**: Enables centralized monitoring, threat detection, and response by aggregating data from diverse sources.
4. **Configuration**: Typically involves setting up diagnostics, creating data collection rules, and specifying the events to monitor.

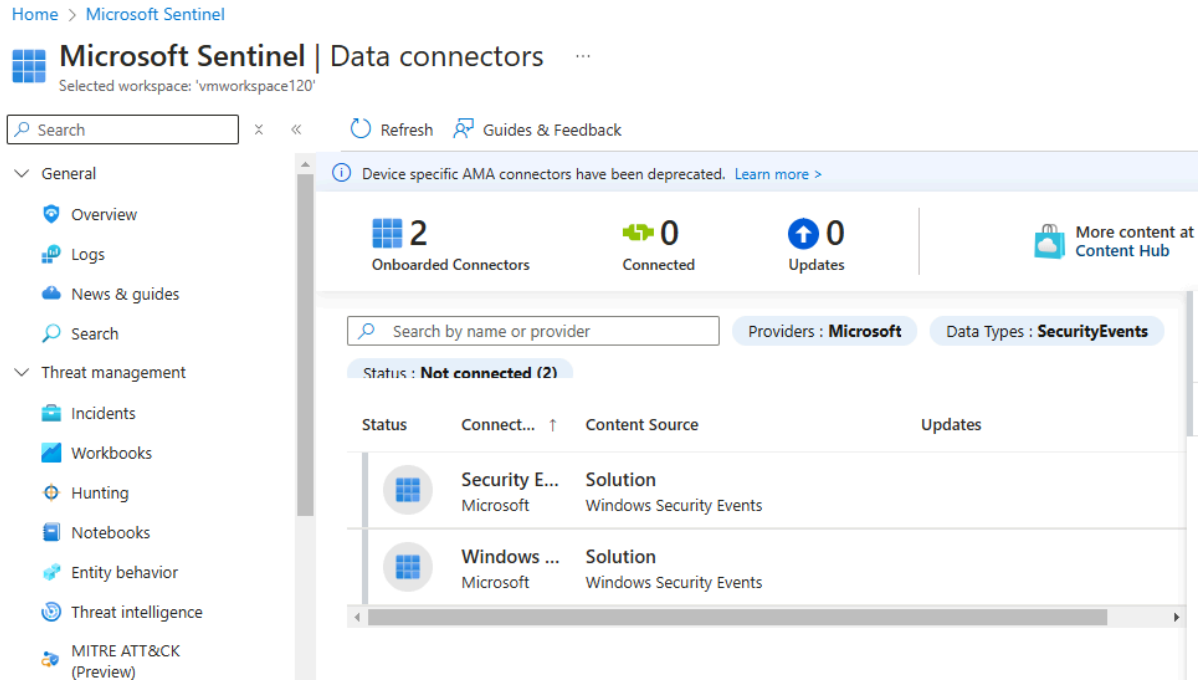
The goal of enabling a data connector in Microsoft Sentinel is to centralize and monitor security event data from various sources like Azure VMs. By configuring a connector and creating a Data Collection Rule (DCR), data is collected and sent to the Log Analytics workspace, where it can be queried and analyzed. This allows organizations to gain insights, detect potential threats (e.g., failed login attempts), and proactively respond to security issues. Microsoft Sentinel integrates this data, enabling automated alerts and comprehensive security management to enhance the organization's overall security posture and streamline threat detection and response efforts.

To begin with the lab

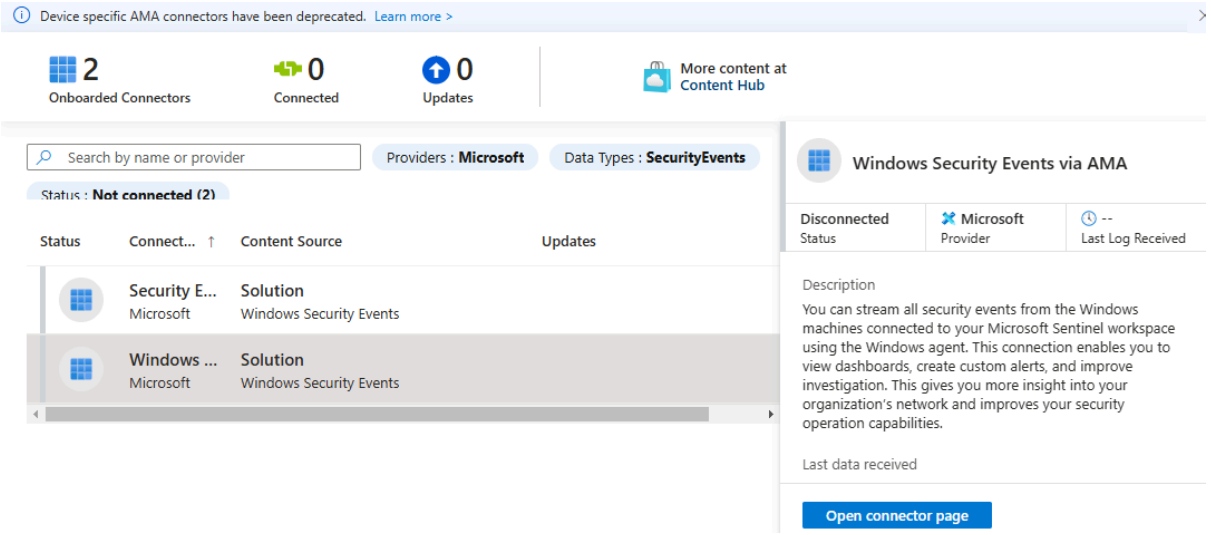
1. Access the Microsoft Sentinel service within the Azure portal.



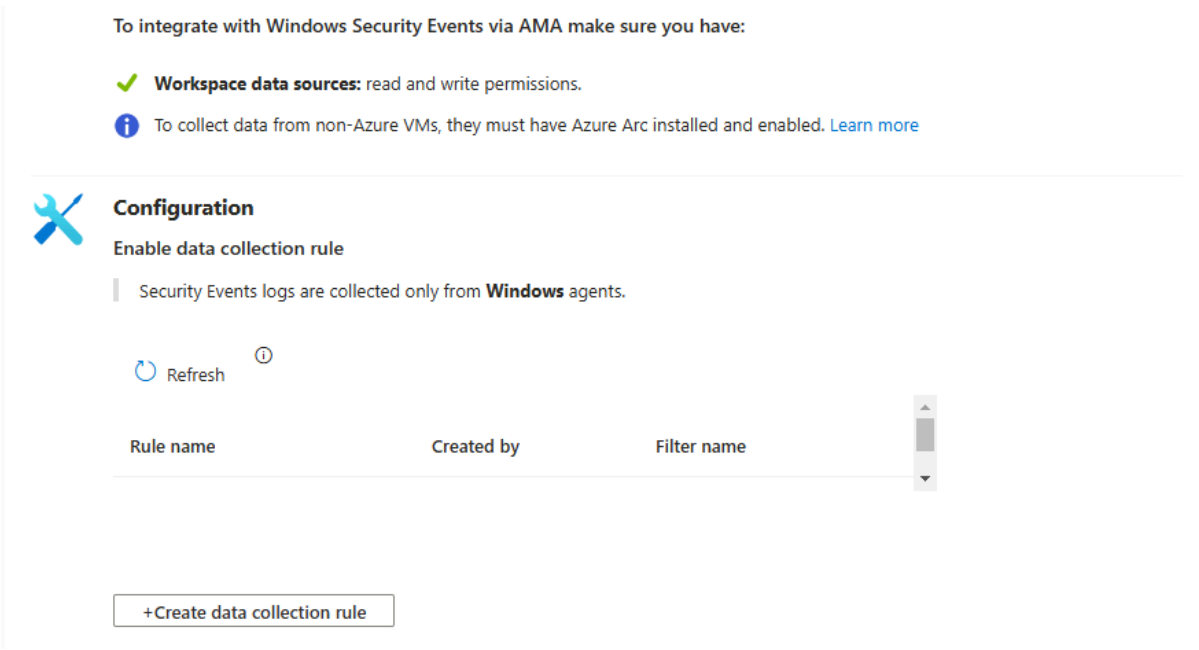
2. Access the Data Connectors section in the left pane and locate and choose the desired connector.



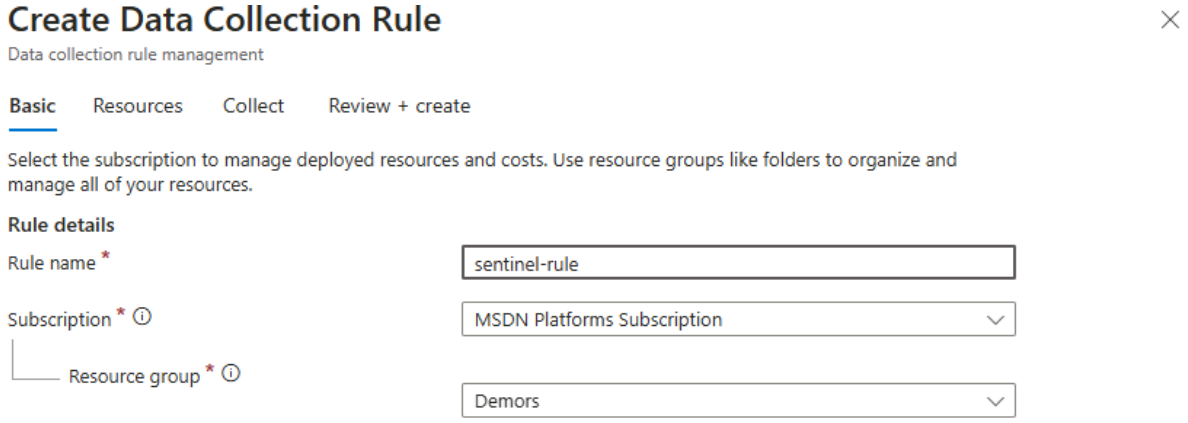
3. Here go through all the connectors and select Window Security Event via AMA(Azure Monitoring Agent).



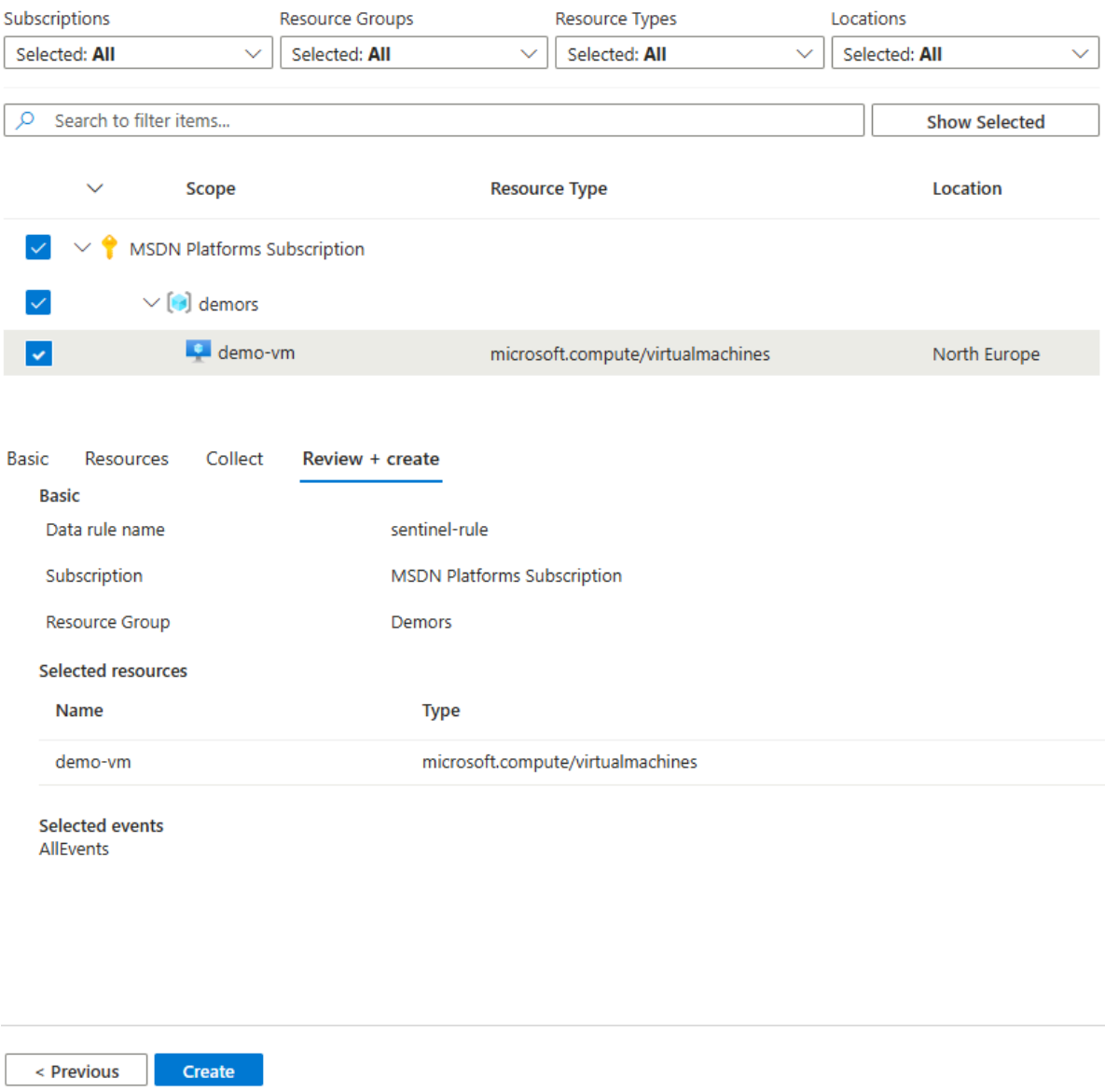
4. Open the connector page and it will provide you instructions on how to use the connector so read the provided steps to configure the connector.



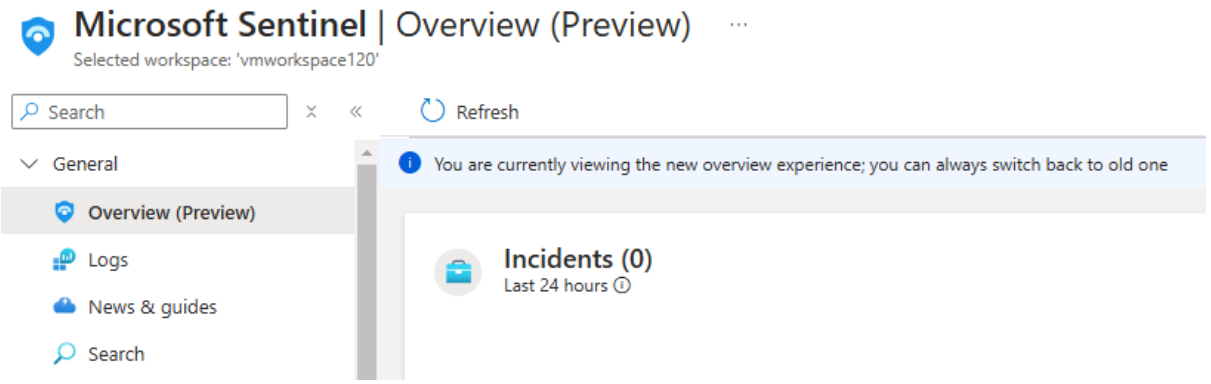
5. Initiate the process by selecting the option to Create Data Collection Rule and give a name for the rule.



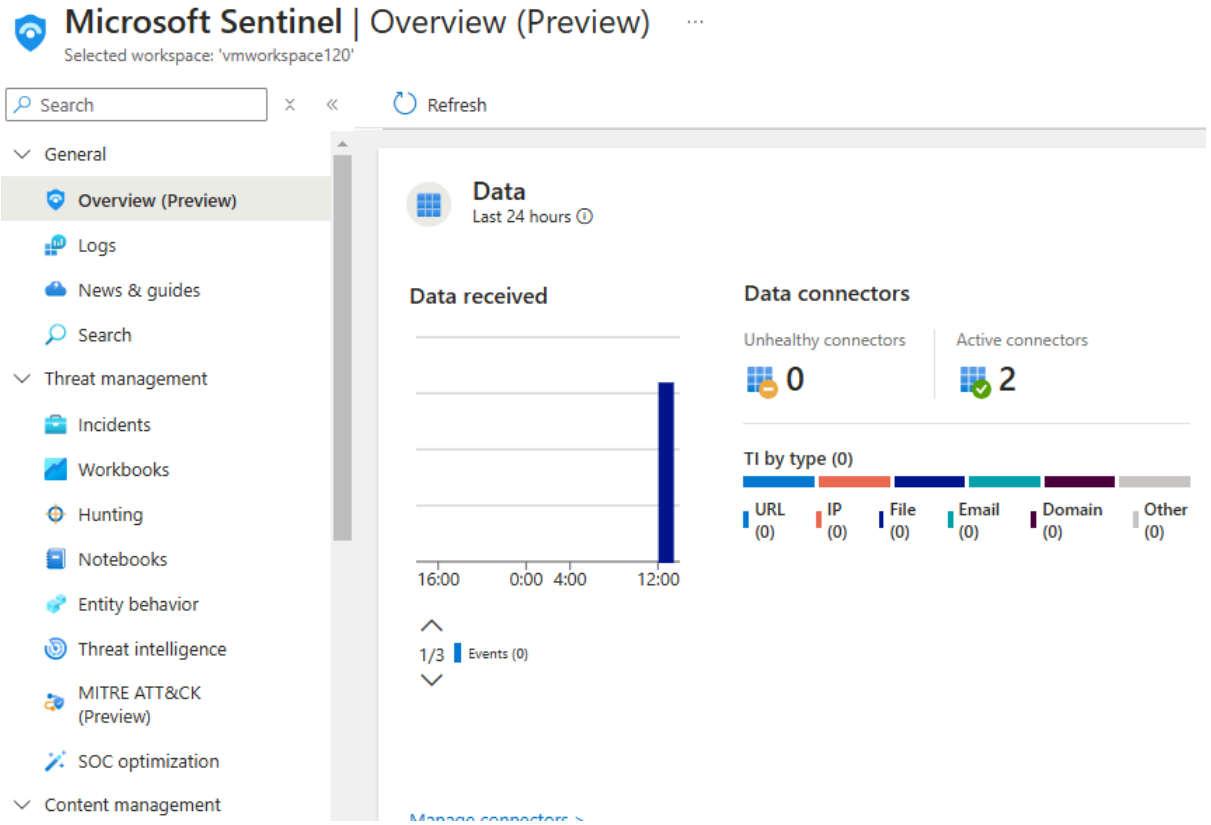
6. Then choose the relevant resource, such as your Azure Virtual Machine and Identify the security events you wish to gather, for instance, all events and after that conclude by clicking Review and Create to complete the establishment of the rule.



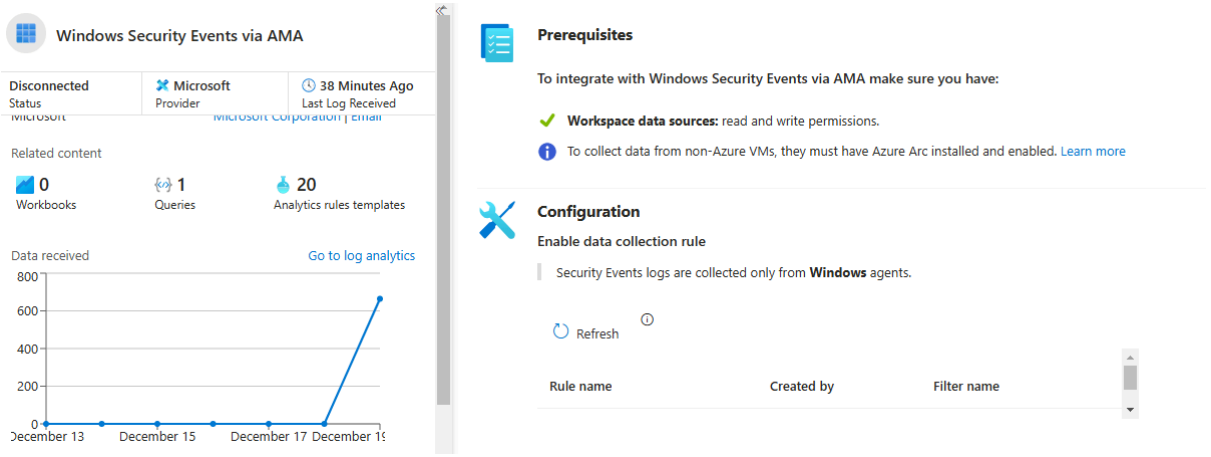
7. Now allow time for the data collection process to complete. Subsequently, navigate to the Overview section of Microsoft Sentinel to verify that data is being successfully received.



8. Here you will see something named as incidents is being created. If you scroll down you will see some data is being collected.

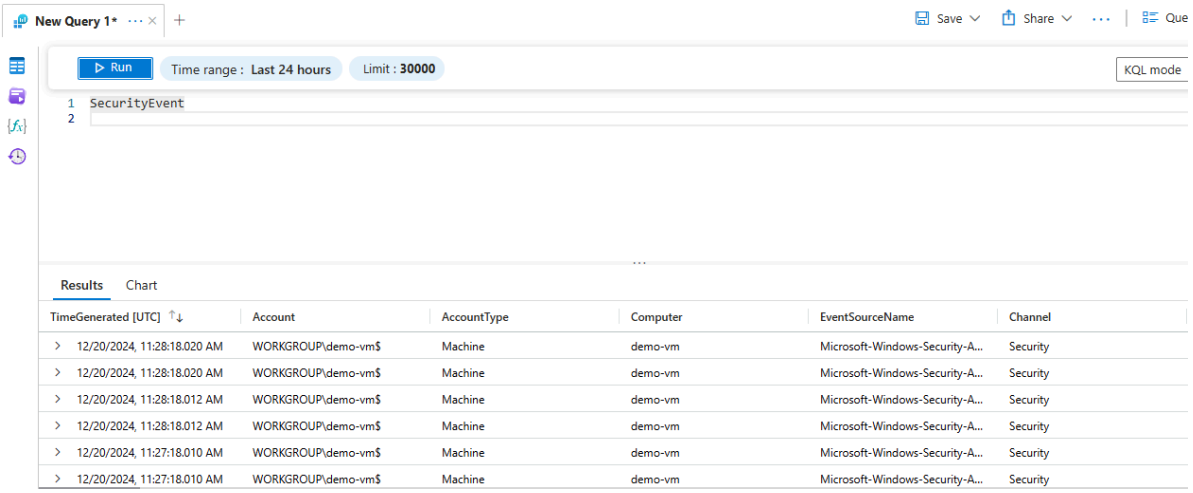


9. Now go to manage connectors in bottom of the data section. It will take you to the data collector page.
10. Select a data collector here and on left side scroll down and go to the **Log Analytics Workspace** to query data.



11. You will see some by default queries running here which are part of the connector. If you go on the results you will see some values based on time frames.

12. Run a query to view events in the **SecurityEvent** table.



13. Examine the particulars of the event, including the event identification number and associated activities. Investigate particular actions, such as unsuccessful login attempts, to detect possible security concerns.
14. You have effectively activated a data connector, established a data collection rule, and confirmed that data is being gathered and transmitted to Microsoft Sentinel.