Microsoft Sentinel - Integration Guide

Microsoft Sentinel will be used to receive alerts and events from Seraphic. To support this feature, we exposed a dedicated endpoint for this:

```
admin/integrations/microsoft-sentinel/pull-events-alerts
```

Microsoft Sentinel can periodically call the above endpoint and as a response, we will return the next batch of data. After we have returned this list of items, we will save the IDs of the last returned alert and the last returned event. Based on that values we will calculate the records we should return on the next call.

> Only Alerts and Events created after the integration was established will be returned

Enabling Microsoft Sentinel integration from Seraphic Admin Console

To enable the Microsoft Sentinel integration, you need to go in the admin console to **SETTINGS->Third-Party Integration** and click the **Add Integration** button. From the **SIEM** category select **MICROSOFT SENTINEL**, press the **NEXT** button and then the **SAVE** button. You will receive a new API key for this integration. This key should be sent in every request made on this endpoint at the top of the document.

Protect endpoint and filter data at tenant level

There are different mechanisms we can use to protect this type of integration but in our case, we are using a public API key. After the admin user has enabled the Microsoft Sentinel integration from the Seraphic Admin Console , a unique API key will be generated. This key should be sent on every request being made on this endpoint on the top of the document.

How to do the configurations at Microsoft Sentinel dashboard

Onboard Microsoft Sentinel on Azure

See this Quickstart to learn how to enable Microsoft Sentinel and configure the Seraphic Web Security data connector: https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

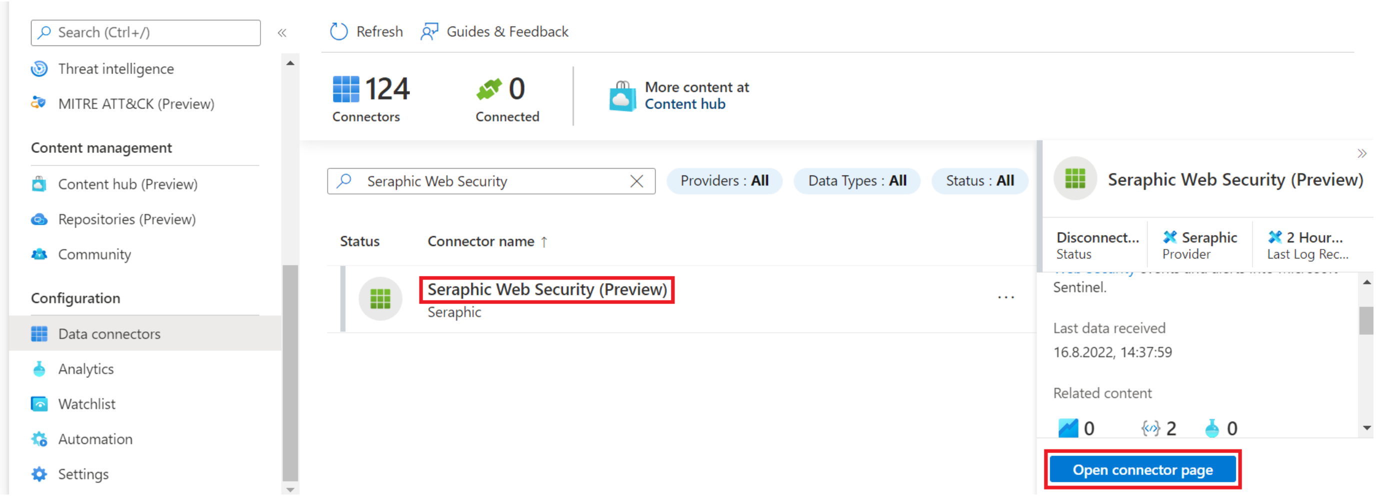
When you need to select a data connector from the data connectors gallery, there are two ways to use our data connector - through our solution in the Azure Marketplace or by deploying a custom template:

Using data connector by Seraphic Web Security solution from the Azure Marketplace

Select the **Seraphic Web Security** data connector in the data connectors gallery and then select the **Open connector page** button on it.

Using data connector by deploy a custom template

1. Download the connector ARM template JSON file from here.
2. In the Azure portal, search for **Deploy a custom template**.
3. On the **Custom deployment** page, select **Build your own template in the editor** > **Load file**. Browse to and select the local ARM template, and then save your changes.
4. Select your **Subscription** and **Resource group**, and then enter the Log Analytics **Workspace** where you want to deploy the data connector. If you want, you can also change the default values of **Retry Count** (the number of retries the request will try. Default: 3) and of **Query Window In Min** (the available query window, in minutes. Default: 5).
5. Select **Review + create** to deploy the custom connector to Microsoft Sentinel.
6. In Microsoft Sentinel, go to the **Data connectors** page, search for the new connector and then select the **Open connector page** button on it.



Sentinel.

Last data received

16.8.2022, 14:37:59

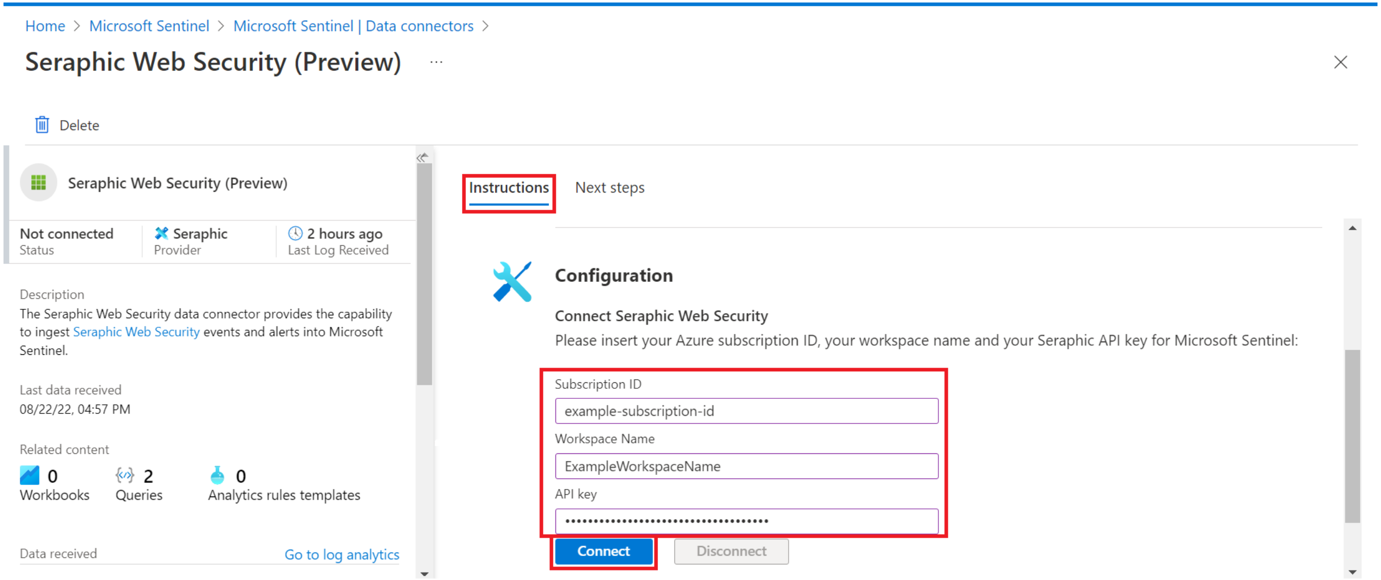
Related content

0 2 0

Configure the data connector to start ingesting data

Now, on the **Instructions** tab configure the connector:

1. Make sure you have read and write permissions to the **Workspace**.
2. Make sure you have **Seraphic API Key** for Microsoft Sentinel connected to your Seraphic Web Security tenant. Get this API Key from the Seraphic Web Security Admin Console and fill it in the **API key** text box. Also fill in your **Azure subscription ID** and your **workspace name** in the appropriate text boxes and select the **Connect** button.


Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >
Seraphic Web Security (Preview)
Delete
Seraphic Web Security (Preview)
Not connected Status
Seraphic Provider
2 hours ago Last Log Received
Instructions
Next steps
Configuration
Connect
Disconnect
Go to log analytics

Description

The Seraphic Web Security data connector provides the capability to ingest Seraphic Web Security events and alerts into Microsoft Sentinel.

Last data received

08/22/22, 04:57 PM

Related content

0 Workbooks

2 Queries

0 Analytics rules templates

Data received

Connect Seraphic Web Security

Please insert your Azure subscription ID, your workspace name and your Seraphic API key for Microsoft Sentinel:

Subscription ID: example-subscription-id

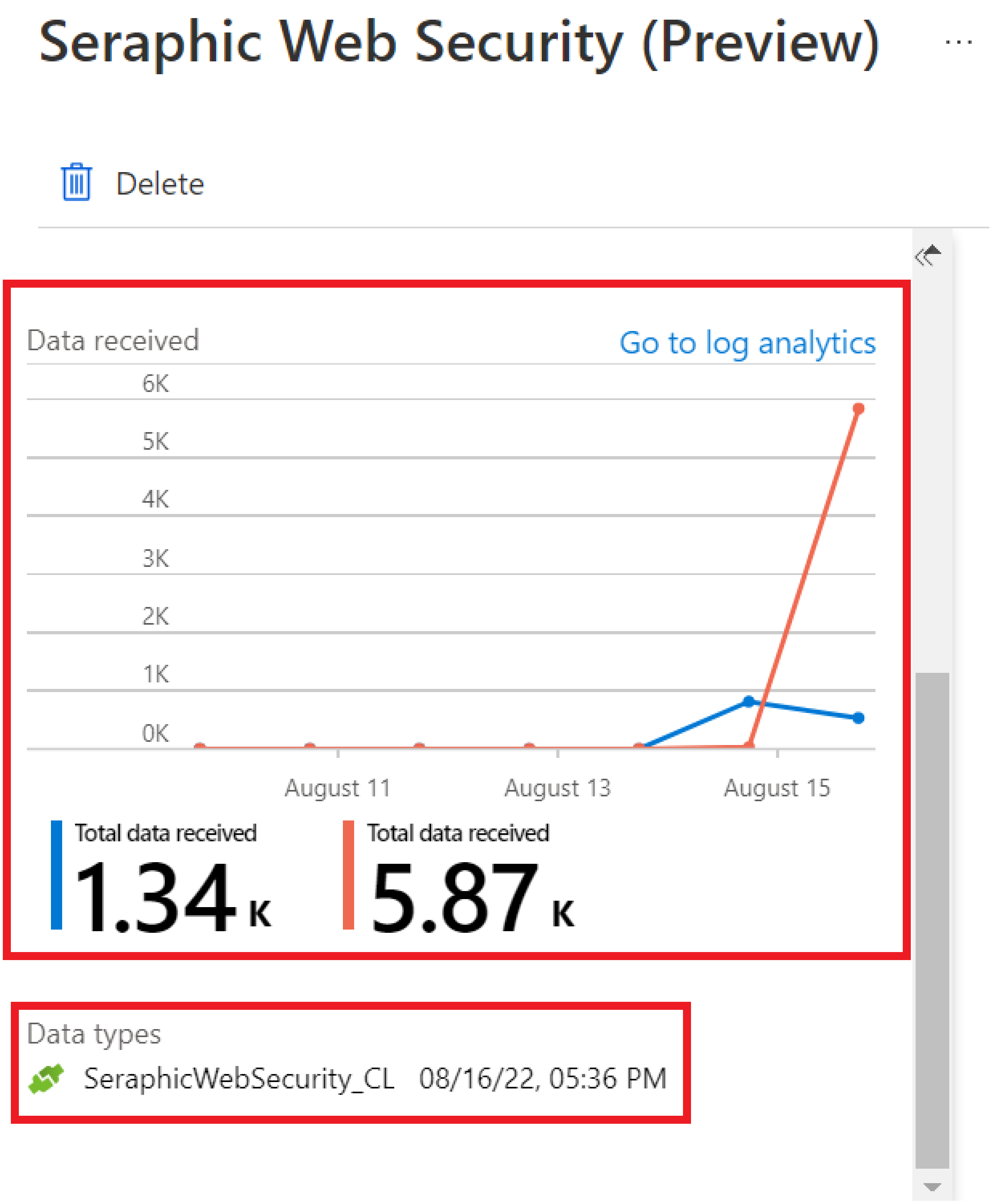
Workspace Name: ExampleWorkspaceName

API key: ••••••••••••••••••••••••••••••••••••••

Find your data

It may take up to 20 minutes before your logs start to appear in Log Analytics.

After a successful connection is established, you see a summary of the data in the Data received graph, and the connectivity status of the data type.



Seraphic Web Security (Preview)

Total data received 1.34K

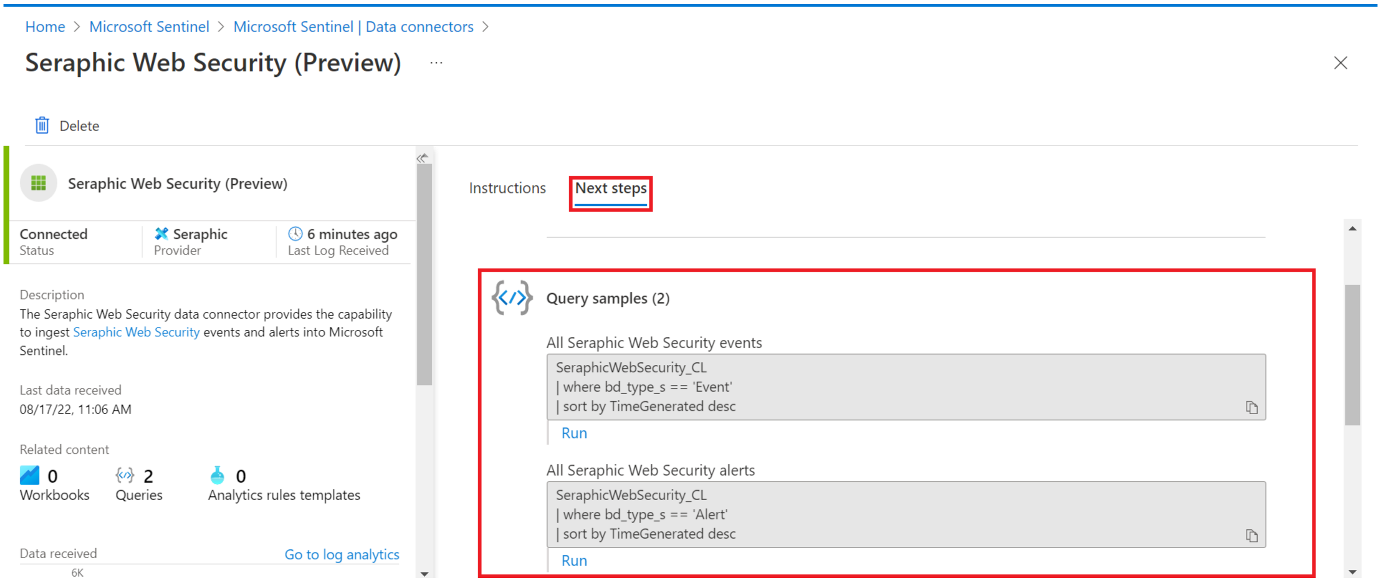
Total data received 5.87K

Data types

SeraphicWebSecurity_CL 08/16/22, 05:36 PM

The data appears in **Logs** under the **CustomLogs** section. The table name of the data is: `SeraphicWebSecurity_CL`. To query your Seraphic Web Security data, use this table name in your query. This table handles your Seraphic Web Security alerts and events together. In order to differentiate between them, there is a special field for both called `bd_type` (in the Microsoft Sentinel table it is called `bd_type_s`, because to identify the data type of a property, Azure adds a suffix to the property name. Read more information about it here), for events its value is **Event** and for alerts its value is **Alert**.

In the **Next steps** tab in the connector page, you'll see sample queries on your data.



Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >

Seraphic Web Security (Preview) ...

Delete

Seraphic Web Security (Preview)

Connected Status | Seraphic Provider | 6 minutes ago Last Log Received

Description
The Seraphic Web Security data connector provides the capability to ingest Seraphic Web Security events and alerts into Microsoft Sentinel.

Last data received
08/17/22, 11:06 AM

Related content
0 Workbooks | 2 Queries | 0 Analytics rules templates

Data received | Go to log analytics
6K

Instructions | Next steps

Query samples (2)

All Seraphic Web Security events

```
SeraphicWebSecurity_CL
| where bd_type_s == 'Event'
| sort by TimeGenerated desc
```

Run

All Seraphic Web Security alerts

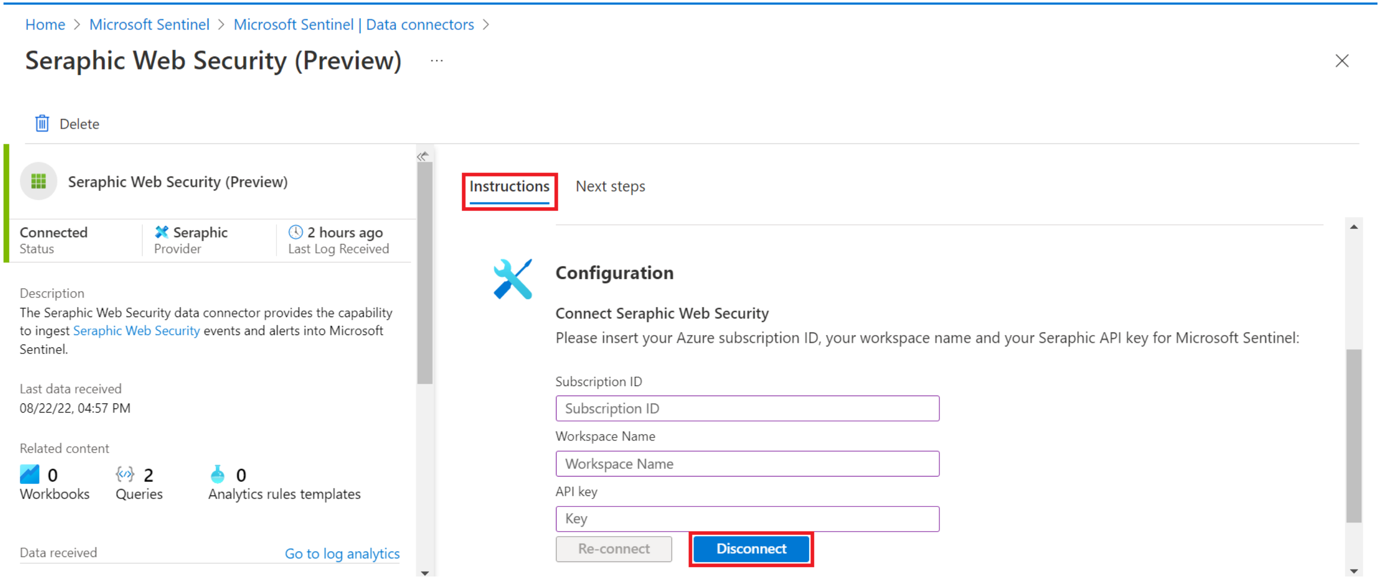
```
SeraphicWebSecurity_CL
| where bd_type_s == 'Alert'
| sort by TimeGenerated desc
```

Run

Disconnect the connector

If you no longer need the connector's data, disconnect the connector to stop the data flow:

In the data connector page in the Azure portal, select **Disconnect**.



Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >

Seraphic Web Security (Preview) ...

Delete

Seraphic Web Security (Preview)

Connected Status | Seraphic Provider | 2 hours ago Last Log Received

Description
The Seraphic Web Security data connector provides the capability to ingest Seraphic Web Security events and alerts into Microsoft Sentinel.

Last data received
08/22/22, 04:57 PM

Related content
0 Workbooks | 2 Queries | 0 Analytics rules templates

Data received | Go to log analytics

Instructions | Next steps

Configuration

Connect Seraphic Web Security
Please insert your Azure subscription ID, your workspace name and your Seraphic API key for Microsoft Sentinel:

Subscription ID: Subscription ID
Workspace Name: Workspace Name
API key: Key

Re-connect | Disconnect

Analytics rule

Our analytic rule sets Seraphic Web Security alerts to be Microsoft Sentinel alerts in the `SecurityAlert` table.

Configure the analytic rule

Import and deploy analytic rule from ARM template

1. Download the analytics rule ARM template JSON file from here.
2. From the Microsoft Sentinel navigation menu, select **Analytics**.
3. Click **Import** from the bar at the top of the screen. In the resulting dialog box, navigate to and select the above JSON file, and select **Oper**
.

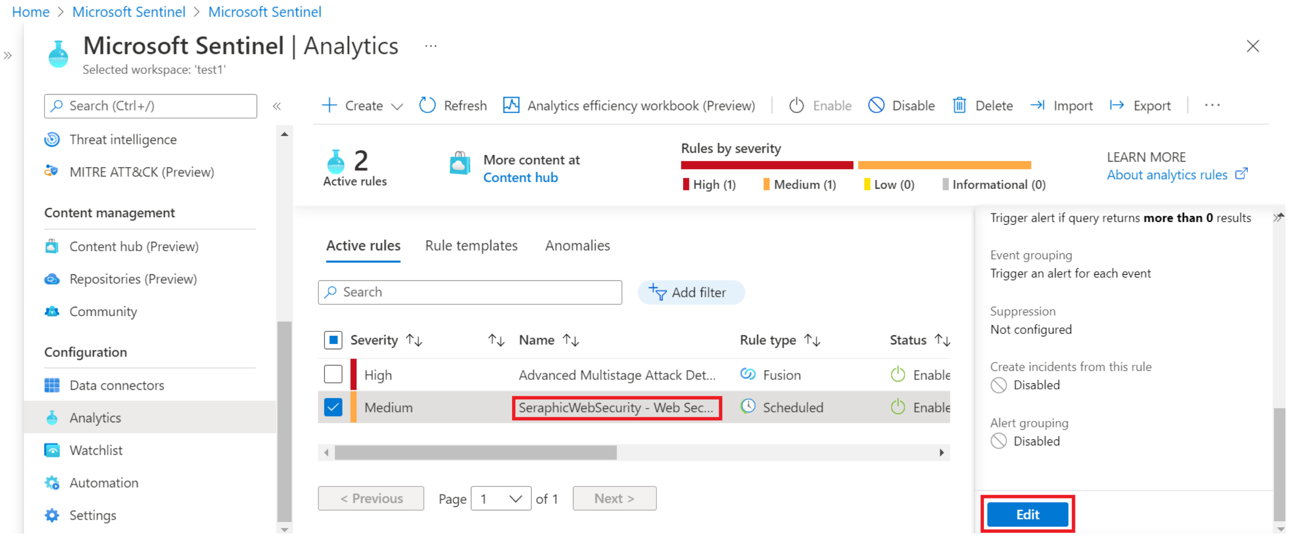
> You can also deploy the analytic rule ARM template in the **Deploy a custom template** service, like the data connector custom template deployment above.

Edit the analytic rule

After you've configured the analytic rule, you can edit it if you want to change some of the configuration. See the Microsoft's documentation for how to do this:

- **Entity mapping**: Map data fields to Microsoft Sentinel entities | Microsoft Docs
- **Custom details**: Surface custom details in Microsoft Sentinel alerts | Microsoft Docs
- **Alert details**: Customize alert details in Microsoft Sentinel | Microsoft Docs
- **Query scheduling**: you can also change the query scheduling from the default values:

1. Under **Active rules**, select the new scheduled query rule called **SeraphicWebSecurity - Web Security Alert** and click **Edit**.



Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'test1'

2 Active rules

More content at Content hub

Rules by severity: High (1) Medium (1) Low (0) Informational (0)

LEARN MORE About analytics rules

Active rules | Rule templates | Anomalies

Severity	Name	Rule type	Status
High	Advanced Multistage Attack Det...	Fusion	Enable
Medium	SeraphicWebSecurity - Web Sec...	Scheduled	Enable

Trigger alert if query returns **more than 0** results

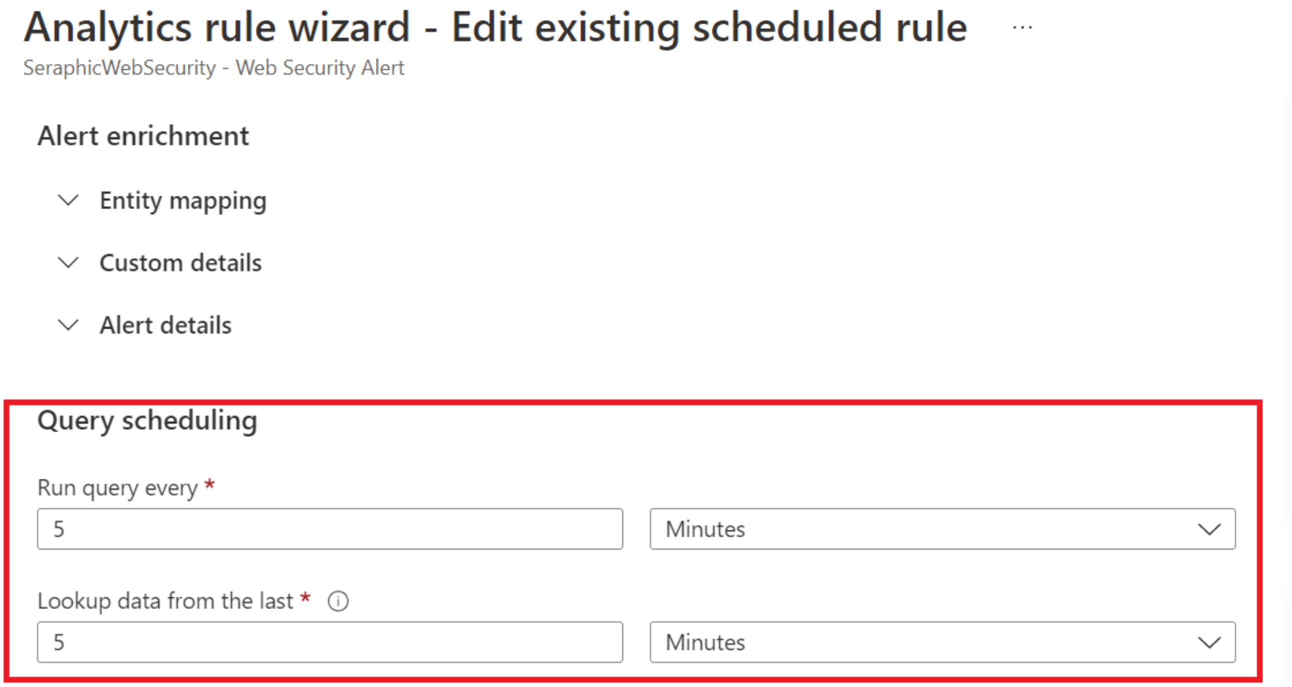
Event grouping: Trigger an alert for each event

Suppression: Not configured

Create incidents from this rule: Disabled

Alert grouping: Disabled

2. Click the **Set rule logic** tab.
3. In the **Query scheduling** section, you can change the **Run query every** to control how often the query is run - as frequently as every 5 minutes or as infrequently as once every 14 days, and the **Lookup data from the last** to determine the time period of the data covered by the query - for example, it can query the past 10 minutes of data, or the past 6 hours of data. The maximum is 14 days.



Analytics rule wizard - Edit existing scheduled rule

SeraphicWebSecurity - Web Security Alert

Alert enrichment

Entity mapping

Custom details

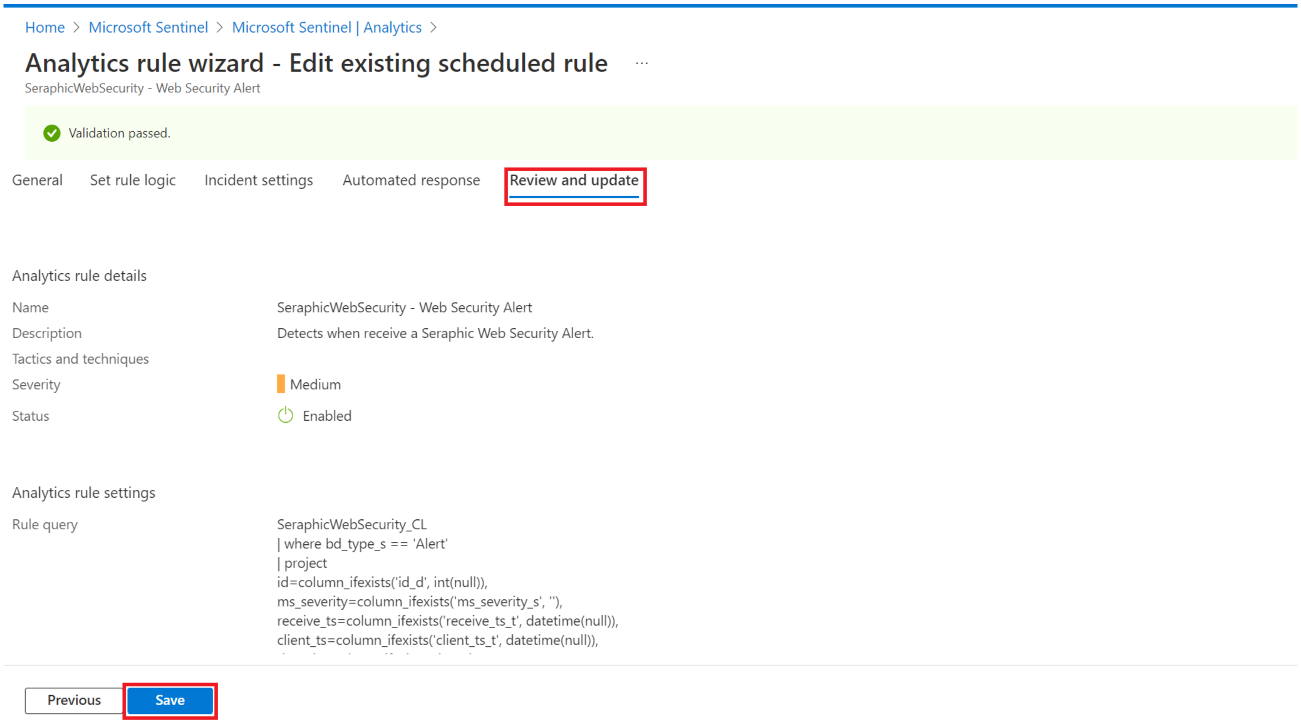
Alert details

Query scheduling

Run query every *: 5 Minutes

Lookup data from the last *: 5 Minutes

4. Select **Review and update** to review all the settings. When the "Validation passed" message appears, select **Save** to save your changes.


Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

Analytics rule wizard - Edit existing scheduled rule

SeraphicWebSecurity - Web Security Alert

✓ Validation passed.

Analytics rule details

Name	SeraphicWebSecurity - Web Security Alert
Description	Detects when receive a Seraphic Web Security Alert.
Tactics and techniques	
Severity	Medium
Status	Enabled

Analytics rule settings

Rule query

```
SeraphicWebSecurity_CL
| where bd_type_s == 'Alert'
| project
id=column_ifexists('id_d', int(null)),
ms_severity=column_ifexists('ms_severity_s', ''),
receive_ts=column_ifexists('receive_ts_t', datetime(null)),
client_ts=column_ifexists('client_ts_t', datetime(null)),
```