

# ReversingLabs content pack solution for Microsoft Sentinel

Last updated: 2023-03-30

[1. Solution Changelog](#)

[2. Overview](#)

[3. Prerequisites](#)

[4. Installing the solution](#)

[5. Installing the solution content](#)

[5.1. Workbook: ReversingLabs-CapabilitiesOverview](#)

[5.2. Playbook: ReversingLabs-CheckQuotas playbook](#)

[5.3. Playbook: ReversingLabs-EnrichFilehash](#)

[6. Managing the solution](#)

[6.1. Accessing the solution content manager](#)

[6.2. Updating the solution](#)

[6.3. Deleting solution content](#)

[6.4. Uninstalling the solution](#)

[7. Using the solution content](#)

[7.1. Using the ReversingLabs-CapabilitiesOverview workbook](#)

[7.2. Using the ReversingLabs-EnrichFileHash playbook](#)

[8. Support](#)

## 1. Solution Changelog

| Version | Changes  | Published  |
|---------|--|------------|
| 2.0.0   | Re-release of ReversingLabs File Enrichment Solution for Microsoft Sentinel  | 2022-10-26 |
| 2.0.1   | Fixes typos in workbook queries  | 2023-02-01 |
| 2.1.0   | Add API quota usage details to ReversingLabs-CapabilitiesOverview workbook, add ReversingLabs-CheckQuotas playbook | 2023-02-27 |
| 2.1.1   | Minor fix to workbook queries  | 2023-03-15 |

## 2. Overview

This document describes the ReversingLabs content pack solution for Microsoft Sentinel, including details on how to install and use the provided content. Please note that screenshots and examples used in this document are accurate at time of publication, however are subject to change due to the rapidly evolving nature of Microsoft Sentinel.

📌 **NEW:** Check out our YouTube video on how to install and configure the solution:  
▶ [How to install and configure the ReversingLabs Content Pack Solution for Microsoft Sentinel](#)

The ReversingLabs content pack solution for Microsoft Sentinel currently contains the following content:

| Name                               | Category | Description   |
|------------------------------------|----------|---|
| ReversingLabs-CapabilitiesOverview | Workbook | A workbook that provides insights into your threat intelligence implementation and overall impacts of ReversingLabs intelligence and automation on your operations. |
| ReversingLabs-CheckQuotas          | Playbook | A playbook that checks TitaniumCloud API usage.   |
| ReversingLabs-EnrichFileHash       | Playbook | A playbook that retrieves file hash reputation information from TitaniumCloud. Uses TCA-0101 and TCA-0104 APIs.   |

## 3. Prerequisites

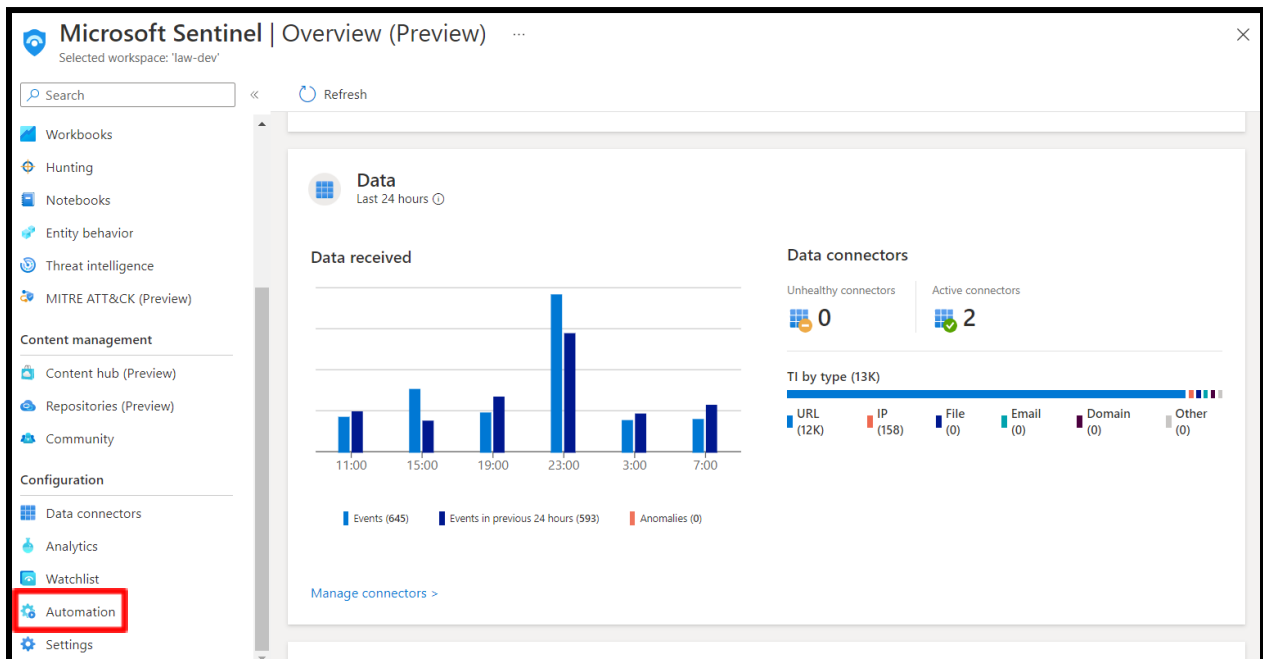
The ReversingLabs content pack solution for Microsoft Sentinel is a free to download collection of content for Microsoft Sentinel. Certain items included with the content pack are designed with the assumption that you already have a TitaniumCloud license.

📌 For more information about obtaining your TiCloud subscription information, see the **ReversingLabs Enrichment APIs For Sentinel Activation Instructions** at <https://reversinglabs-marketplace.azureedge.net/help/ReversingLabsEnrichmentAPIsForSentinelActivation.pdf>

## 4. Installing the solution

To begin using the provided content, you will need to first install the solution from the Microsoft Sentinel content hub, then enable the content.

The solution is made available in the Microsoft Sentinel content hub. The content hub is found under the “Content management” menu header in the Microsoft Sentinel resource blade:



To install the solution, enter “ReversingLabs” in the search box. You should see the “Reversinglabs content pack” solution. Click the solution, and in the solution information blade, click the “Install” button to start the installation:

282 Solutions   269 Standalone contents   5 Installed   1 Updates

reversinglabs   Status : All   Content type : All   Support : All

Content sources : All

Solutions (1)

**ReversingLabs Content Pack**  
ReversingLabs  
Security - Threat Intelligence  
[Playbook](#) [Workbook](#)

**ReversingLabs Content Pack**  
ReversingLabs Support   2.0.0 Version

Description

**OVERVIEW**

The ReversingLabs Content Pack solution for Microsoft Sentinel provides a collection of content for ReversingLabs users. The solution contains a sample playbook that will automatically enrich your incidents with file hash reputation information from TitaniumCloud, enabling faster and more accurate incident triage. The solution also includes a workbook that you can use to visualize the value provided by our Azure-focused products.

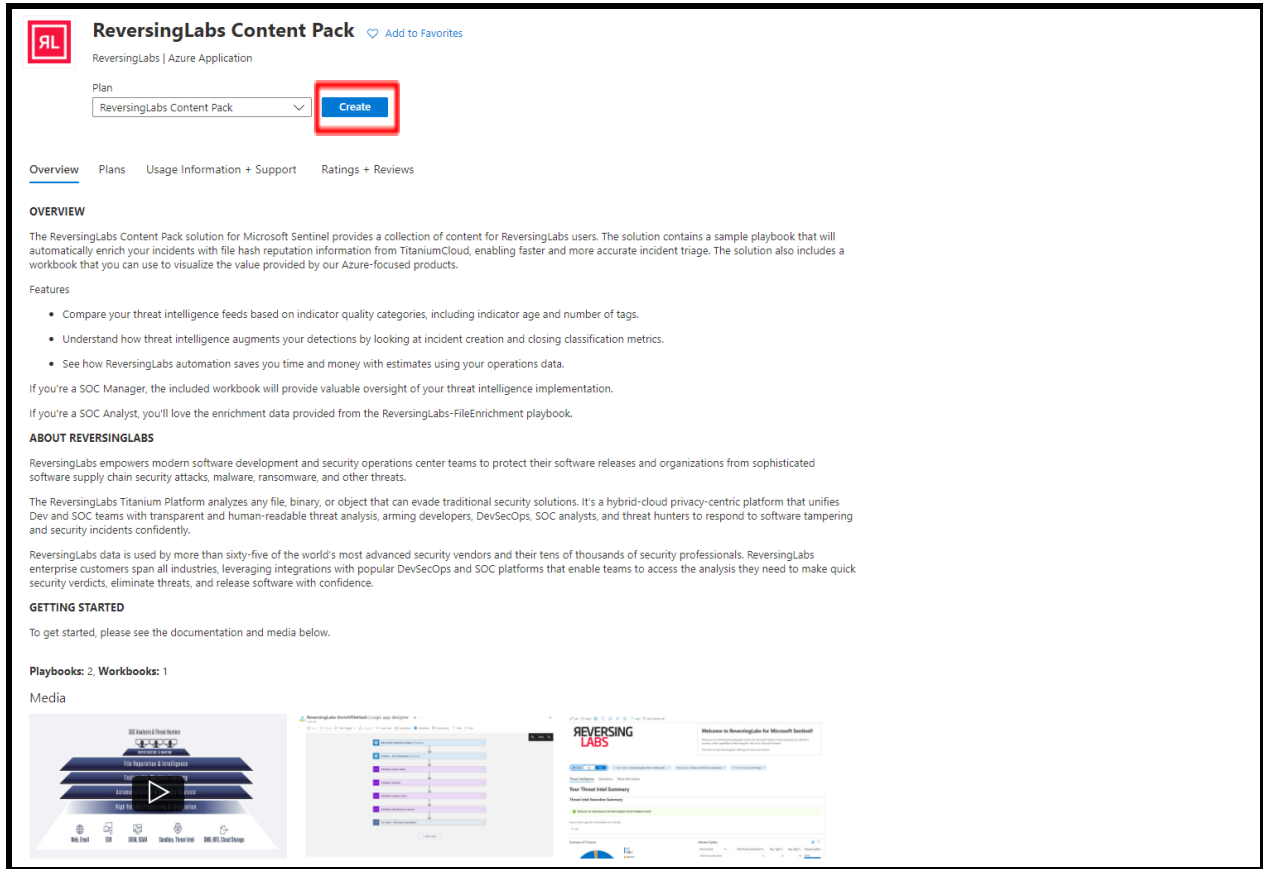
Features

- Compare your threat intelligence feeds based on indicator quality categories, including indicator age and number of tags.
- Understand how threat intelligence augments your detections by looking at incident creation and closing classification metrics.
- See how ReversingLabs automation saves you time and money with estimates using your operations data.

If you're a SOC Manager, the included workbook will provide valuable oversight of

**Install**

After clicking “Install”, you will be presented with the solution overview. Ensure the Plan drop-down menu is set to “ReversingLabs content pack”, then click “Create”:



After clicking “Create”, you will be presented with the deployment settings. Enter the following information:

- **Subscription:** this is the subscription where your Microsoft Sentinel instance is located
- **Resource group:** this is the resource group where your Microsoft Sentinel instance is located
- **Workspace:** this is the name your Microsoft Sentinel workspace

After filling in the information above, click “Review + create” to finalize the deployment.

Basics   Workbooks   Playbooks   Review + create

**REVERSING  
LABS**

**Note:** There may be [known issues](#) pertaining to this Solution, please refer to them before installing.

The ReversingLabs solution for Microsoft Sentinel includes a number of Sentinel resources designed to automate your security operations using the power of TitaniumCloud APIs and visualize your threat intelligence capabilities using included workbooks.

**Workbooks: 1, Playbooks: 1**

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Instance details**

Workspace \* ⓘ

**Review + create**   < Previous   Next : Workbooks >

After clicking “Review + create”, you will be presented with the deployment validation view. Ensure that validation has passed, and if necessary, provide the required contact information. Click “create” to deploy the solution.

## Create ReversingLabs Content Pack ...

✓ Validation Passed

Basics   Workbooks   Playbooks   Review + create

### PRODUCT DETAILS

ReversingLabs Content Pack  
by ReversingLabs  
[Terms of use](#) | [Privacy policy](#)

### TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Aaron Hoffmann

Preferred e-mail address

Preferred phone number

### Basics

Create

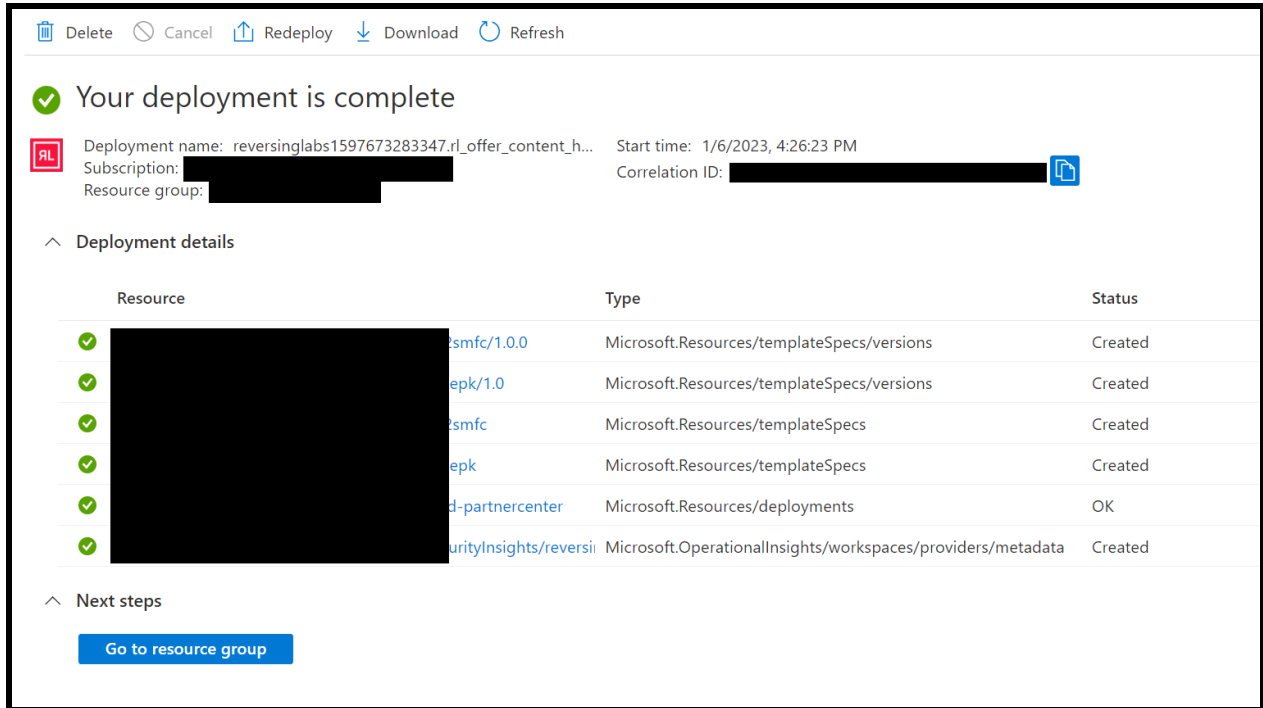
< Previous

Next

[Download a template for automation](#)

After clicking "create", you will be transferred to the deployment view. After a few seconds, the deployment should successfully complete. If there are any errors during deployment, please contact [support@reversinglabs.com](mailto:support@reversinglabs.com).

Once completed, you may now navigate back to Sentinel to install the included content.



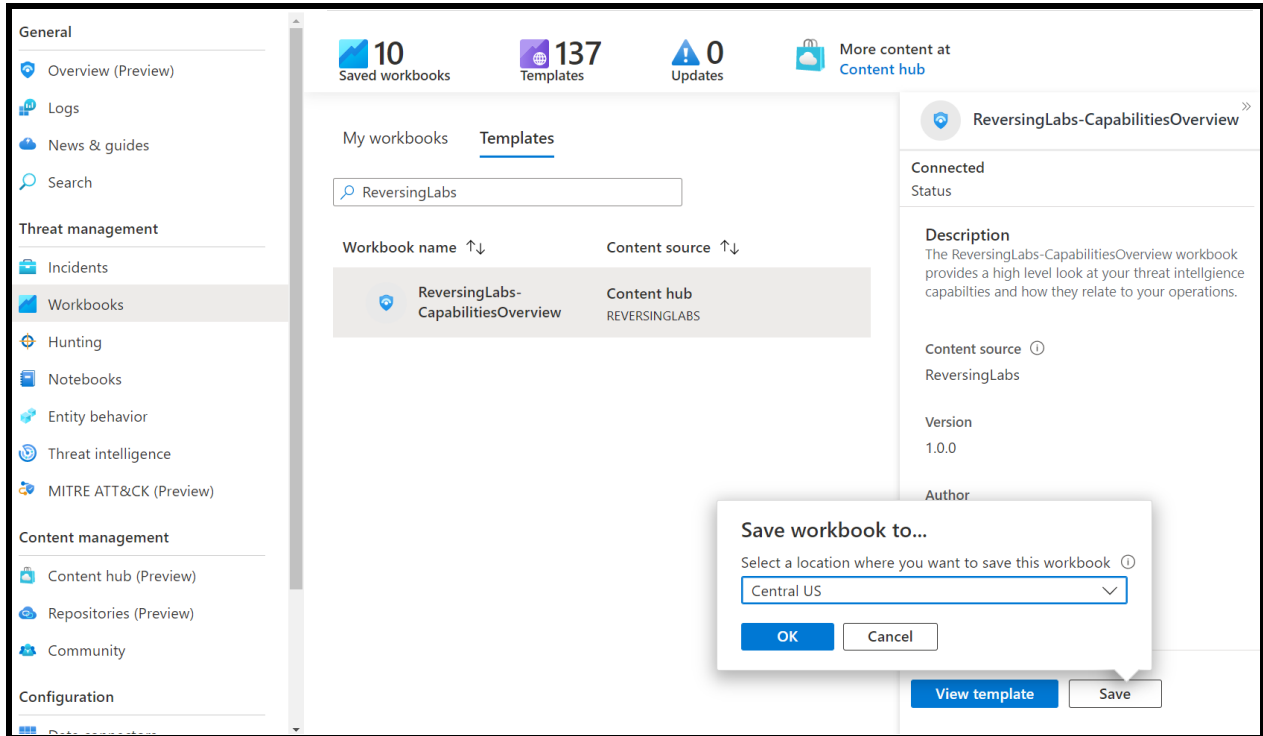
## 5. Installing the solution content

Once the solution has been installed, you will find the associated content is now available in their respective template sections.

### 5.1. Workbook: ReversingLabs-CapabilitiesOverview

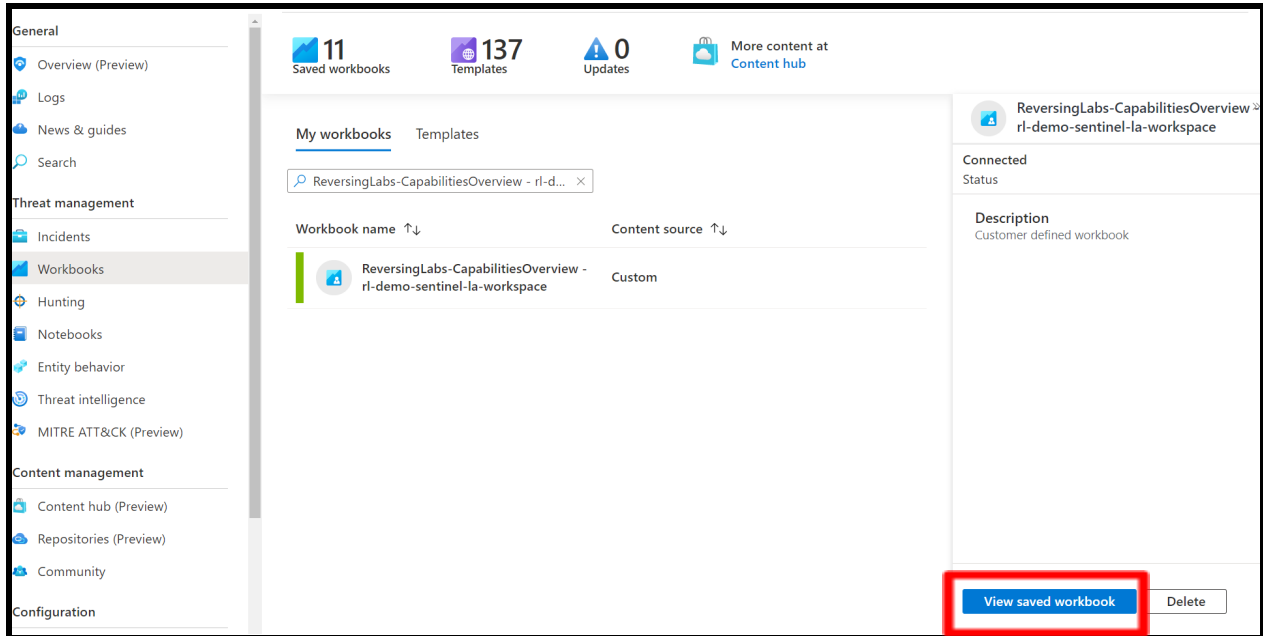
To install the workbook, navigate to Workbooks, then enter "ReversingLabs" in the search bar. You should see the "ReversingLabs-CapabilitiesOverview" workbook with content source "Content hub / ReversingLabs" in the results list. Click "Save", then select the region of your Sentinel workspace and click "OK".




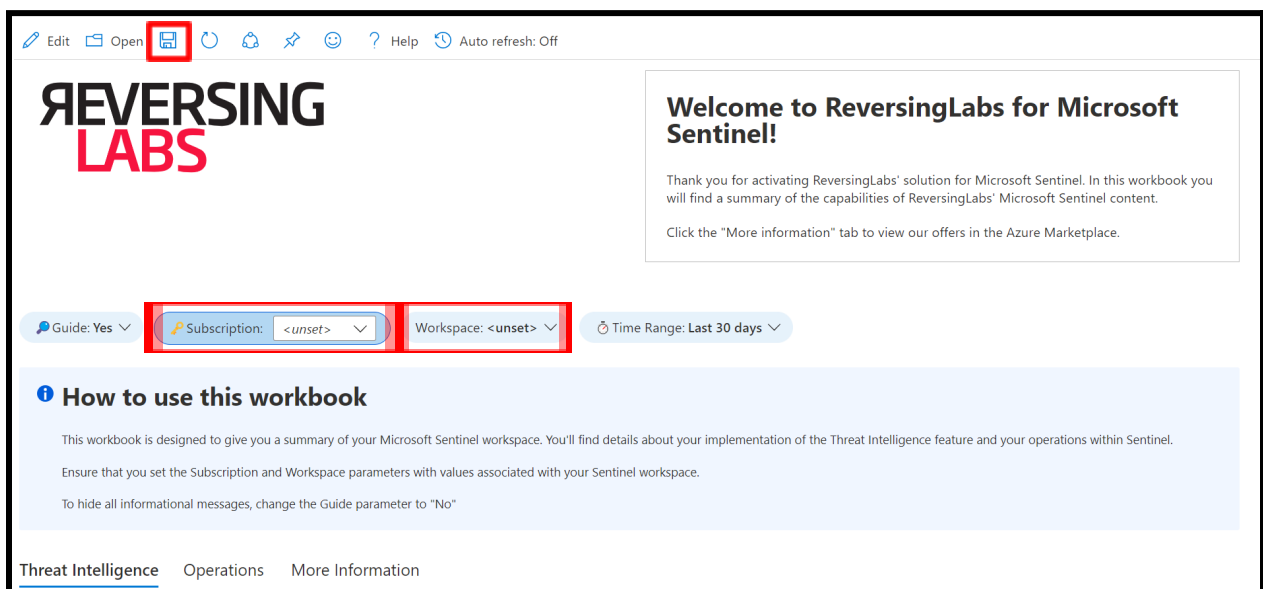


**⚠️ NOTE:** You may see an error in your notifications after clicking 'OK', as shown below. You can ignore this, and the workbook should still deploy normally. If the workbook doesn't appear in your 'My workbooks' list after a few minutes, please contact us.

After the workbook has been saved, click "My workbooks" and you should see the new workbook name with the resource group name appended:



Next, you will need to configure the workbook to query data in your Sentinel workspace. Click “View saved workbook” to open the workbook. Click the “Subscription” parameter bubble and select the subscription containing the Sentinel workspace, then click the “Workspace” parameter bubble and select your Sentinel workspace. You should see the workbook refresh and show data if available. Click the “Save” icon (  ) to save the workbook with these updated settings; the workbook has now been fully deployed.



If you have a TitaniumCloud license, or have subscribed to the Azure Marketplace offer ReversingLabs File Enrichment APIs, you can configure the workbook to monitor your API quotas and view API usage. This requires installation and configuration of the ReversingLabs-CheckQuota playbook, included in version 2.1.0 of the ReversingLabs content pack solution for Microsoft Sentinel - see the previous section for details.

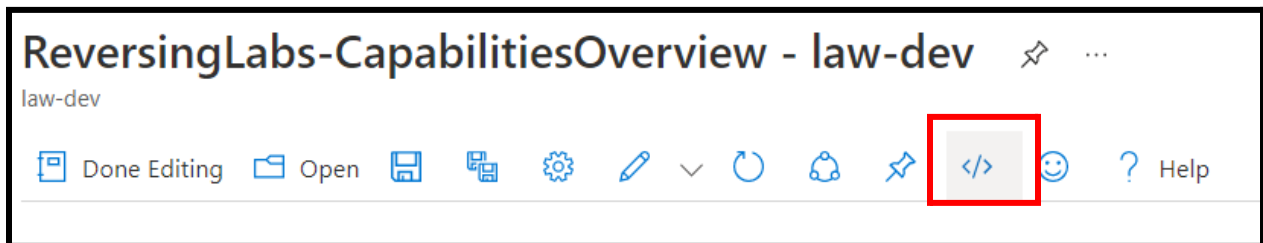
Click the “API Usage” tab. If this is your first time setting up the workbook and/or using the ReversingLabs API, you will be presented with the panel below.

**NOTE:** Ensure you have configured the ReversingLabs-CheckQuotas playbook prior to continuing!

You will need to edit the workbook and provide the path to the ReversingLabs-CheckQuotas playbook. To do this, copy the ArmAction path of the playbook using the following format, replacing the highlighted values with your subscription ID and resource group name:

```
/subscriptions/<subscription_id>/resourceGroups/<resource_group_name>/providers/Microsoft.Logic/workflows/ReversingLabs-CheckQuota/triggers/manual/run?api-version=2016-06-01
```

With the path copied, click the “edit” button in the workbook, then click the advanced editor button:



In the advanced editor, press Control + F on your keyboard to open the search prompt. Enter the ID: b9059e5f-55bb-4e6d-9745-f7fe6497824d

There will be two ArmAction objects with empty path items as shown below. Paste the ArmAction path previously mentioned here:

```
{
  "type": 11,
  "content": {
    "version": "LinkItem/1.0",
    "style": "list",
    "links": [
      {
        "id": "b9059e5f-55bb-4e6d-9745-f7fe6497824d",
        "linkTarget": "ArmAction",
        "linkLabel": "✔ Check quotas",
        "style": "primary",
        "linkIsContextBlade": true,
        "armActionContext": {
          "path": "",
          "httpMethod": "POST",
          "title": "Check quota",
          "description": "# ✔ Check ReversingLabs TitaniumCloud API quotas\n\n## T",
          "actionName": "Check RL TiCloud API Quotas"
        }
      }
    ]
  }
},
```

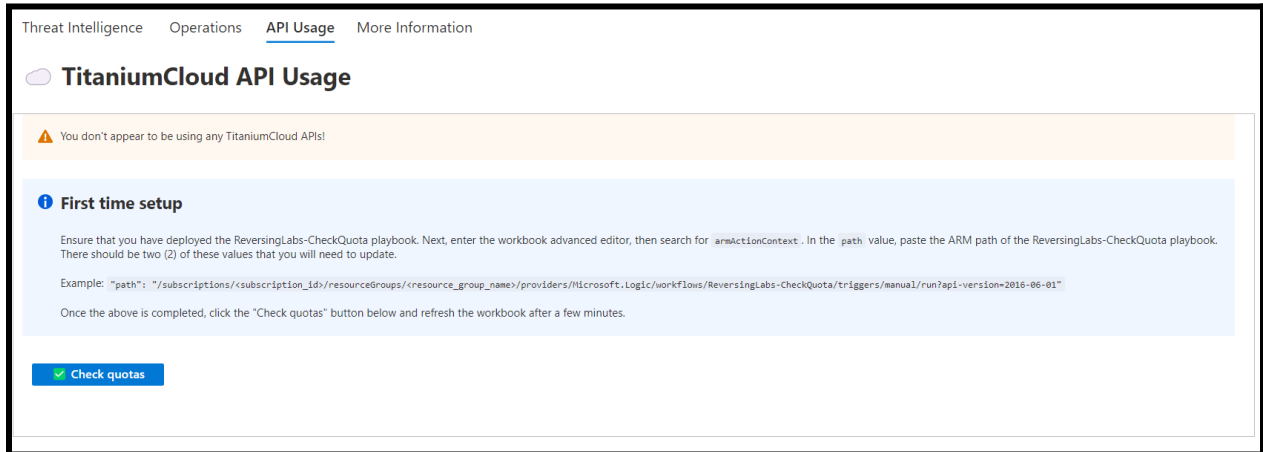
After pasting the ArmAction path:

```
"content": {
  "version": "LinkItem/1.0",
  "style": "list",
  "links": [
    {
      "id": "b9059e5f-55bb-4e6d-9745-f7fe6497824d",
      "linkTarget": "ArmAction",
      "linkLabel": "✔ Check quotas",
      "style": "primary",
      "linkIsContextBlade": true,
      "armActionContext": {
        "path": "/subscriptions/506[REDACTED]/resourceGroups/sentinel-dev/providers/",
        "httpMethod": "POST",
        "title": "Check quota",
        "description": "# ✔ Check ReversingLabs TitaniumCloud API quotas\n\n## This action will execute a",
        "actionName": "Check RL TiCloud API Quotas"
      }
    }
  ]
}
```

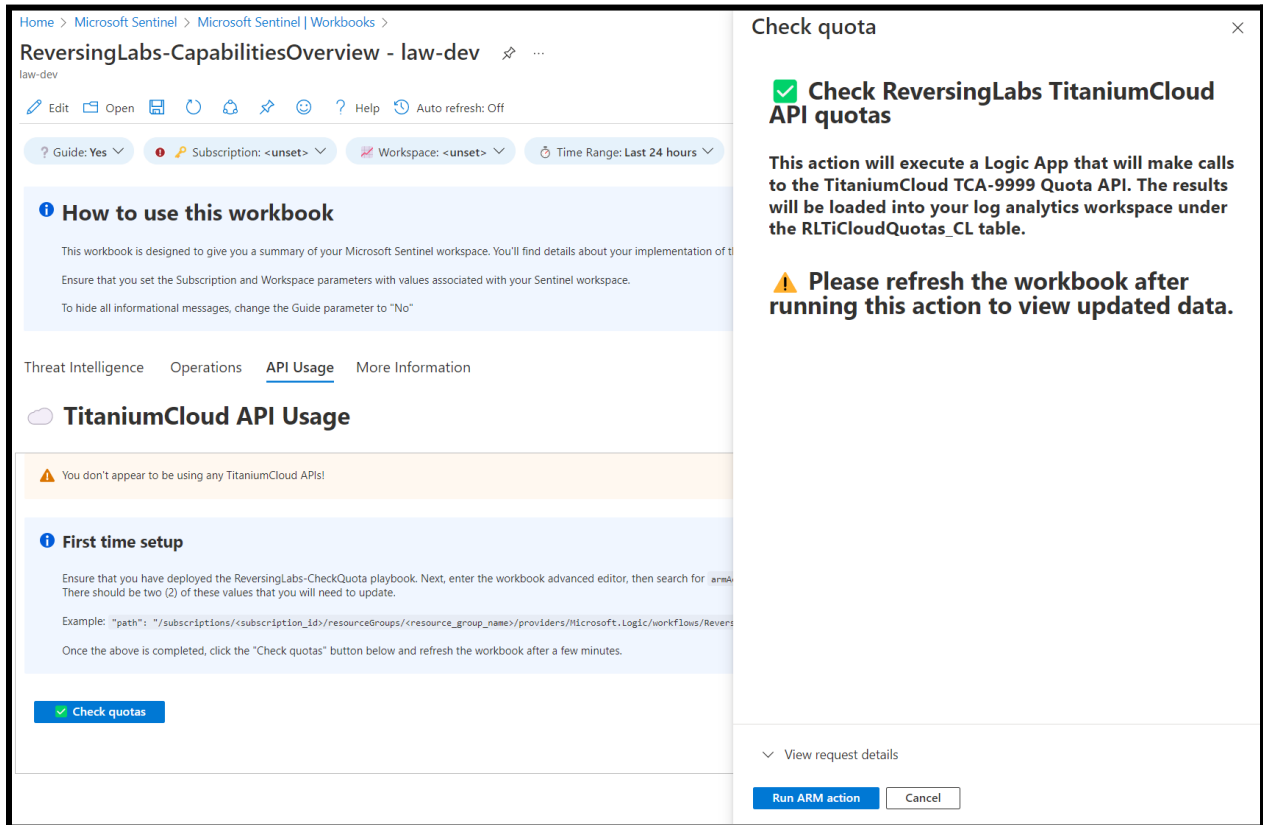
After providing the path value, click the “Apply” button and then save the workbook.


### Checking connectivity and API usage

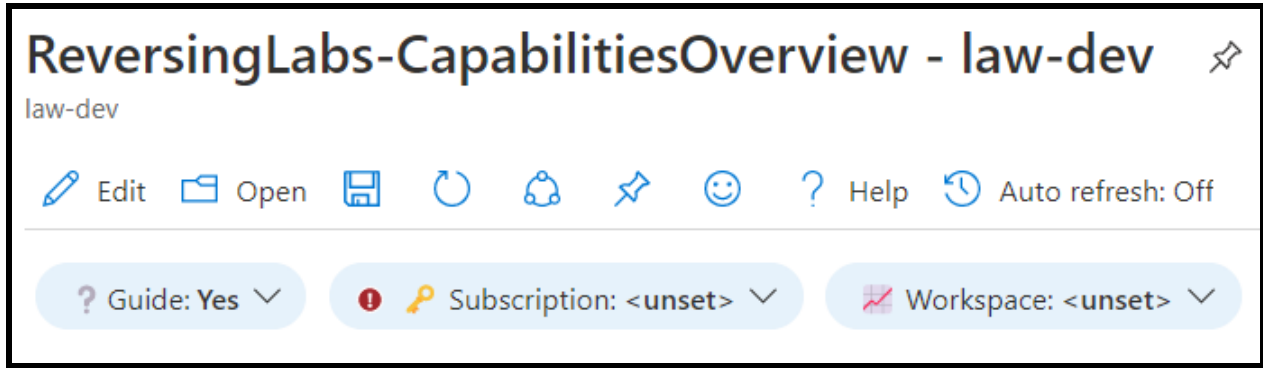
To test connectivity, click the “Check quotas” button.



An ARM action blade will slide out from the right side of the screen. Click the “Run ARM Action” button to continue:

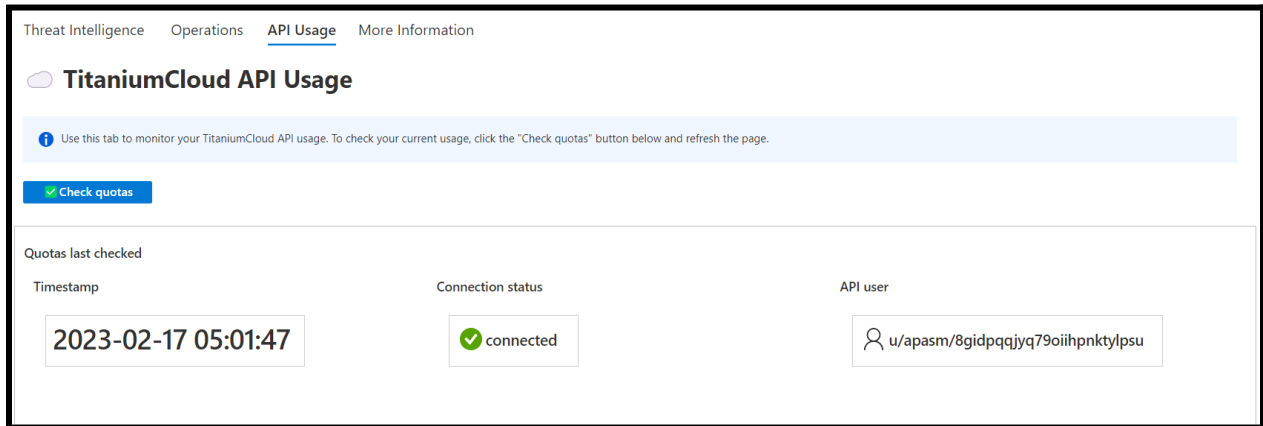


Wait a few minutes, then refresh the workbook by clicking the refresh button (  ):



At minimum, you should see the panel change and present the following information:

- **Timestamp:** UTC timestamp of the last ReversingLabs-CheckQuota playbook run
- **Connection status:** shows 'connected' for successful connection to the TitaniumCloud API or 'error'
- **API User:** the TitaniumCloud user configured in the ReversingLabs-CheckQuota playbook



## 5.2. Playbook: ReversingLabs-CheckQuotas playbook

To install the playbook, from the Microsoft Sentinel menu blade navigate to "Automation", then click "Playbook templates". Use the search box to query "ReversingLabs-CheckQuota". Click "Create playbook" to start the deployment.

Automation rules 0 Enabled rules 0 Enabled playbooks 29 More content at Content hub

Automation rules Active playbooks **Playbook templates (Preview)**

ReversingLabs-CheckQuota Trigger: All More (4)

| Name ↑↓                  | Trigger ↑↓ | Logic Apps Connect... | Entitie |
|--------------------------|------------|-----------------------|---------|
| ReversingLabs-CheckQuota | Other      | Azure Key Vault +1    |         |

**ReversingLabs-CheckQuota**

Other Trigger type Content ... Content source 2/21/202... Last update ti...

**Description**  
This playbook will check your ReversingLabs TitaniumCloud API quota and provide usage details. To be used in conjunction with the ReversingLabs-CapabilitiesOverview workbook.

**Connectors in use**  
 Azure Key Vault Azure Log Analytics Data Collector

**Prerequisites**  
 ReversingLabs TitaniumCloud license  
 ReversingLabs TitaniumCloud username and password

|               |         |
|---------------|---------|
| Source name   | Version |
| ReversingLabs | 1.0     |

Supported by: ReversingLabs | Author: ReversingLabs  
 Email

**Create playbook**

< Previous Page 1 of 1 Next >

In the next window, you will be presented with the deployment settings. Enter the following information:

- **Subscription:** this is the subscription where your Microsoft Sentinel instance is located
- **Resource group:** this is the resource group where your Microsoft Sentinel instance is located
- **Playbook name:** customize the playbook name, if necessary. We recommend that you leave this as the default value.
- **Enable diagnostics logs in Log Analytics:** this option enables diagnostics logs for the logic app, including events such as failures and runtime metrics. We recommend enabling this option. If you enable this option, select your log analytics workspace from the dropdown below.
- **Associate with integration service environment:** enable this only if you wish to associate the logic app with an integration service environment.

After filling in the settings, click “Next: Parameters” to move to the next configuration page.

## Create playbook ...

1 Basics 2 Parameters 3 Connections 4 Review and create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  [Create new](#)

Region \*

Playbook name \*

Enable diagnostics logs in Log Analytics ⓘ

Log Analytics workspace

Associate with integration service environment ⓘ

Integration service environment

In the parameters configuration page, enter your TitaniumCloud username and password. Your TiCloud password will be added as a secret to an Azure Key Vault, which is deployed with the playbook. Click "Next: Connections":

## Create playbook ...

1 Basics 2 Parameters 3 Connections 4 Review and create

RLPAPIPassword \* ⓘ

✘ The value must not be empty.

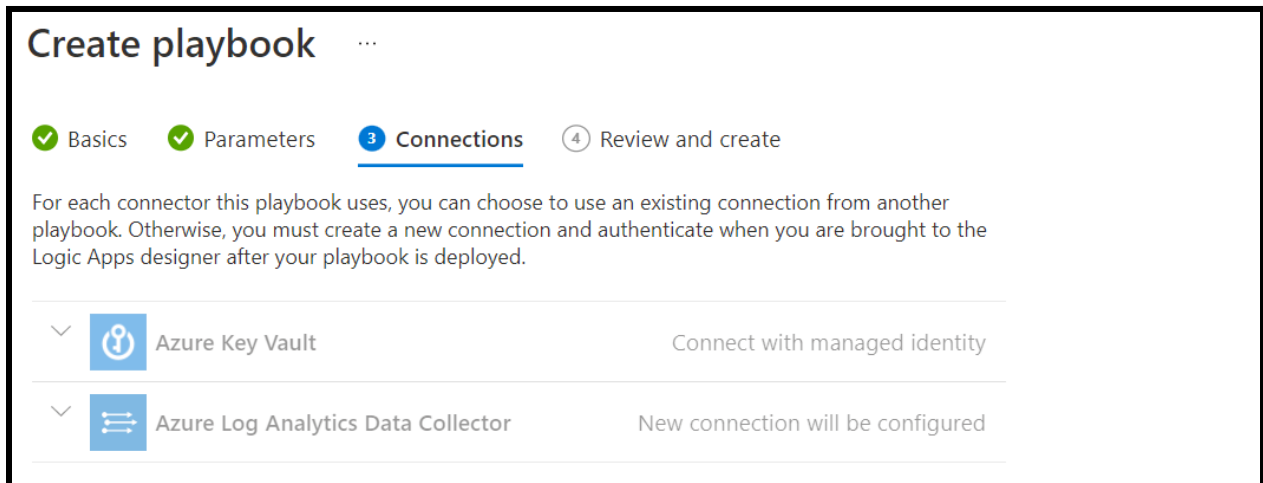
RLPAPIUsername \* ⓘ

✘ The value must not be empty.

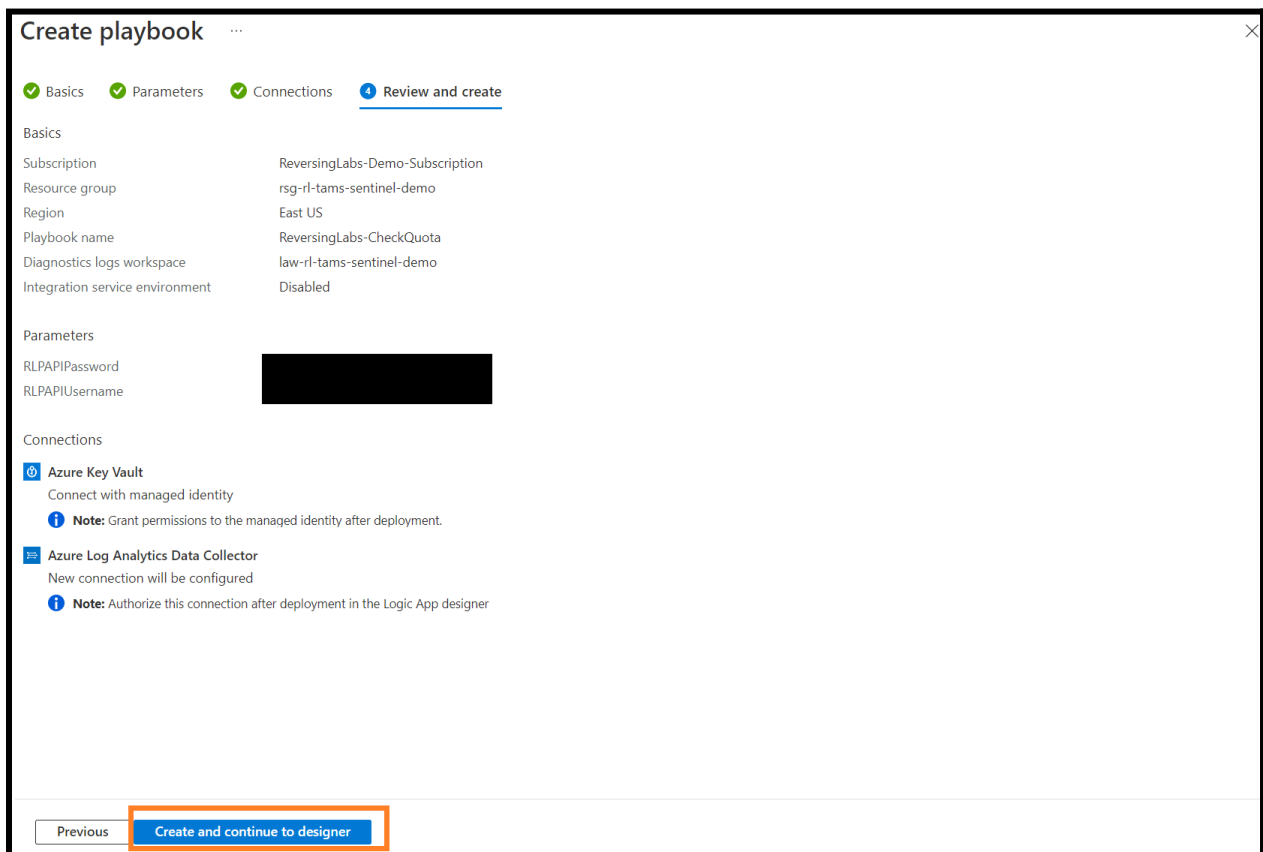
In the connections page, there should be two connections displayed. The first connection for Azure Key Vault will be a new connection deployed with the playbook. The second connection for Azure Log Analytics Data Collector can either be configured with an existing connection, or



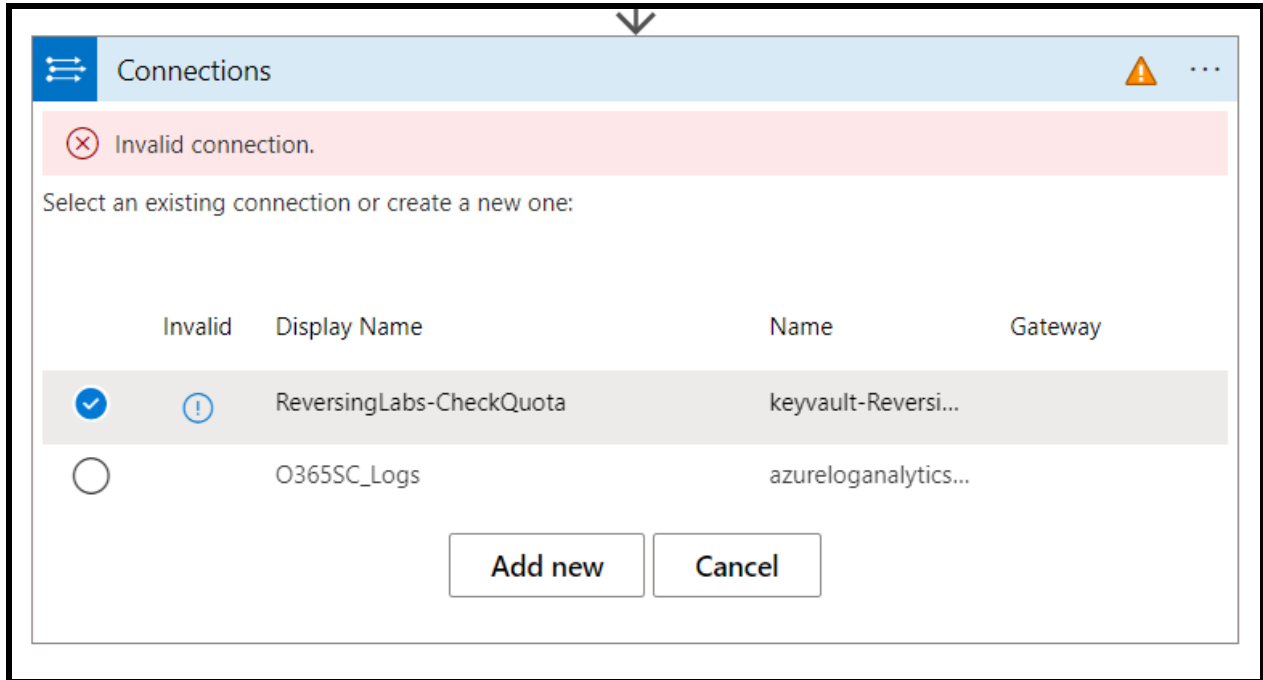
configured with a new connection later. Click “Next: Review and create” to finalize the deployment.



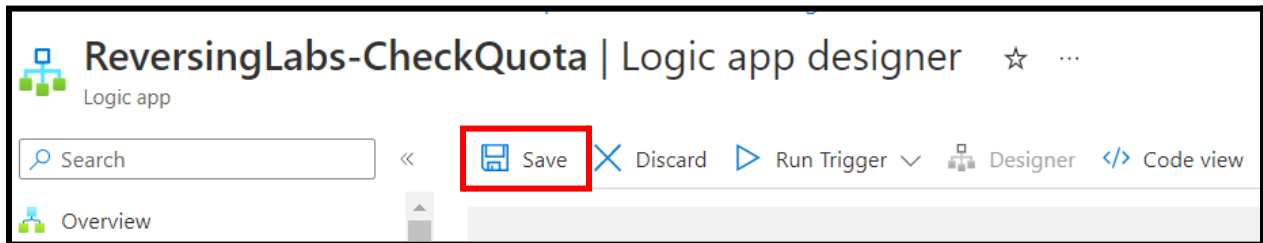
Finally, click “Create and continue to designer” to deploy the playbook:



After the playbook deployment completes, you will need to update the connections for several steps in the playbook. Go through the playbook and look for any steps identified by the yellow “caution” symbol (⚠️). At this time, there should be seven (7) steps that need updating.

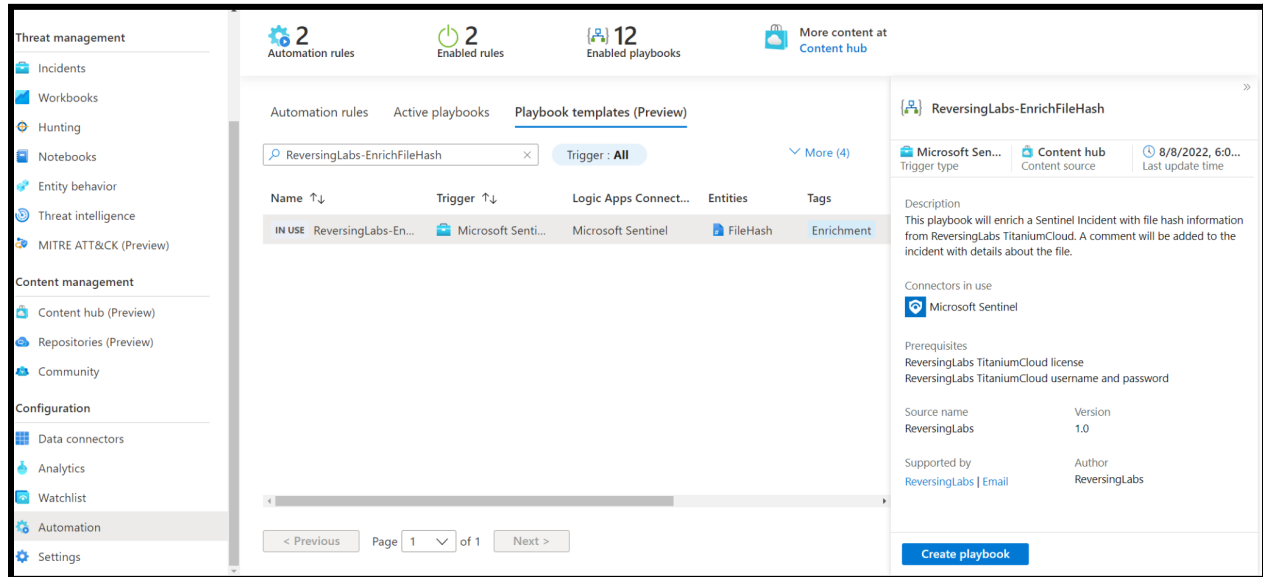


After verifying all API connections have been updated, click "Save" to update the playbook:



## 5.3. Playbook: ReversingLabs-EnrichFilehash

To install the playbook, from the Microsoft Sentinel menu blade navigate to “Automation”, then click “Playbook templates”. Use the search box to query “ReversingLabs-EnrichFileHash”. Click “Create playbook” to start the deployment.



In the next window, you will be presented with the deployment settings. Enter the following information:

- **Subscription:** this is the subscription where your Microsoft Sentinel instance is located
- **Resource group:** this is the resource group where your Microsoft Sentinel instance is located
- **Playbook name:** customize the playbook name, if necessary. We recommend that you leave this as the default value.
- **Enable diagnostics logs in Log Analytics:** this option enables diagnostics logs for the logic app, including events such as failures and runtime metrics. We recommend enabling this option. If you enable this option, select your log analytics workspace from the dropdown below.
- **Associate with integration service environment:** enable this only if you wish to associate the logic app with an integration service environment.

After filling in the settings, click “Next: Connections” to move to the next configuring page.

## Create playbook ⋮

1 Basics 2 Connections 3 Review and create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  [Create new](#)

Region \*

Playbook name \*

Enable diagnostics logs in Log Analytics ⓘ

Log Analytics workspace

Associate with integration service environment ⓘ

Integration service environment


On the connections page, you will be asked to select any existing API connections to be used by the playbook. If you don't have any existing API connections, you can configure those after the playbook has been deployed. Click "Next: Review and create".

## Create playbook ⋮

1 Basics 2 Connections 3 Review and create

For each connector this playbook uses, you can choose to use an existing connection from another playbook. Otherwise, you must create a new connection and authenticate when you are brought to the Logic Apps designer after your playbook is deployed.

---


^  **Microsoft Sentinel** New connection will be configured

New connection will be configured

---

rl-sentinel-demo-sp

---

^  **Microsoft Sentinel** New connection will be configured

New connection will be configured

On the final page, you will be presented with a summary of the deployment settings. Click “Create and continue to designer” to finalize the playbook deployment.


## Create playbook ...


✓ Basics    ✓ Connections    **3** Review and create


### Basics


|                                 |                                 |
|---------------------------------|---------------------------------|
| Subscription                    | ReversingLabs-Demo-Subscription |
| Resource group                  | rsg-rl-demo-sentinel            |
| Region                          | Central US                      |
| Playbook name                   | ReversingLabs-EnrichFileHash    |
| Diagnostics logs workspace      | rl-demo-sentinel-la-workspace   |
| Integration service environment | Disabled                        |

### Connections

 **Microsoft Sentinel**  
New connection will be configured

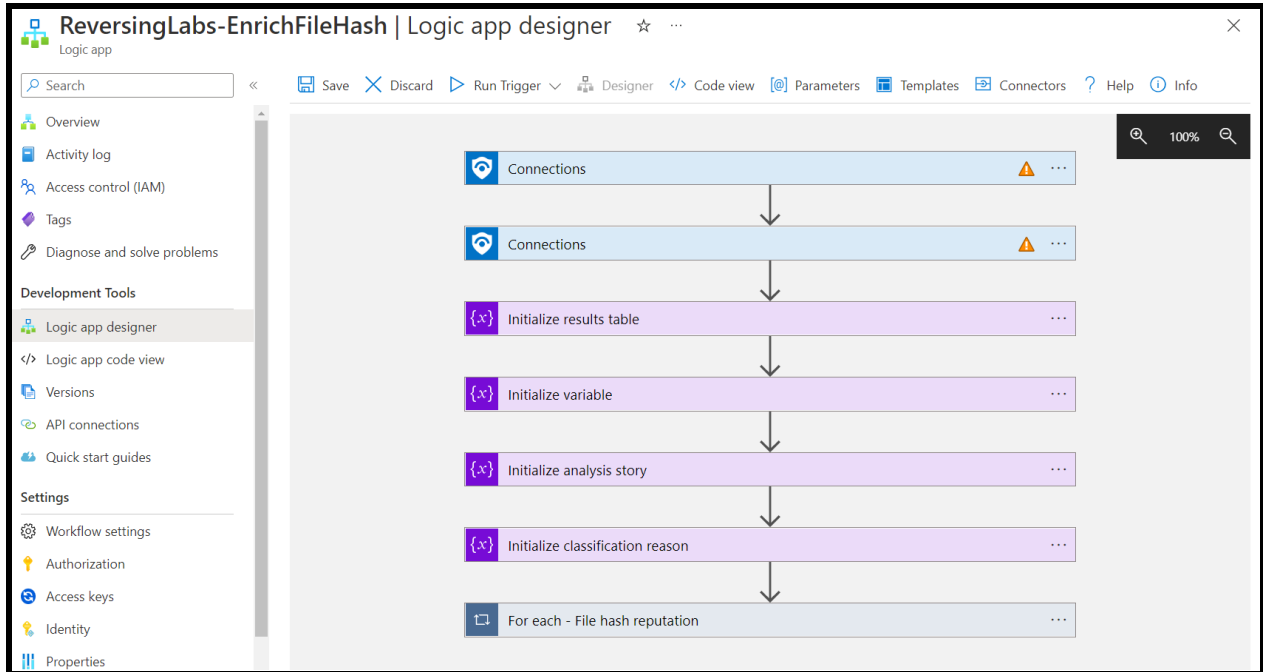
 **Note:** Authorize this connection after deployment in the Logic App designer

 **Microsoft Sentinel**  
New connection will be configured

 **Note:** Authorize this connection after deployment in the Logic App designer

[Previous](#) [Create and continue to designer](#)

If the deployment was successful, you will be dropped into the logic app designer view.



If you did not select any existing API connections during the playbook deployment, you will need to configure the missing connections. These are identified by the yellow “caution” symbol (⚠).

There are five (5) steps that require an API connection. The connectors used are:

- Microsoft Sentinel
- ReversingLabs Intelligence

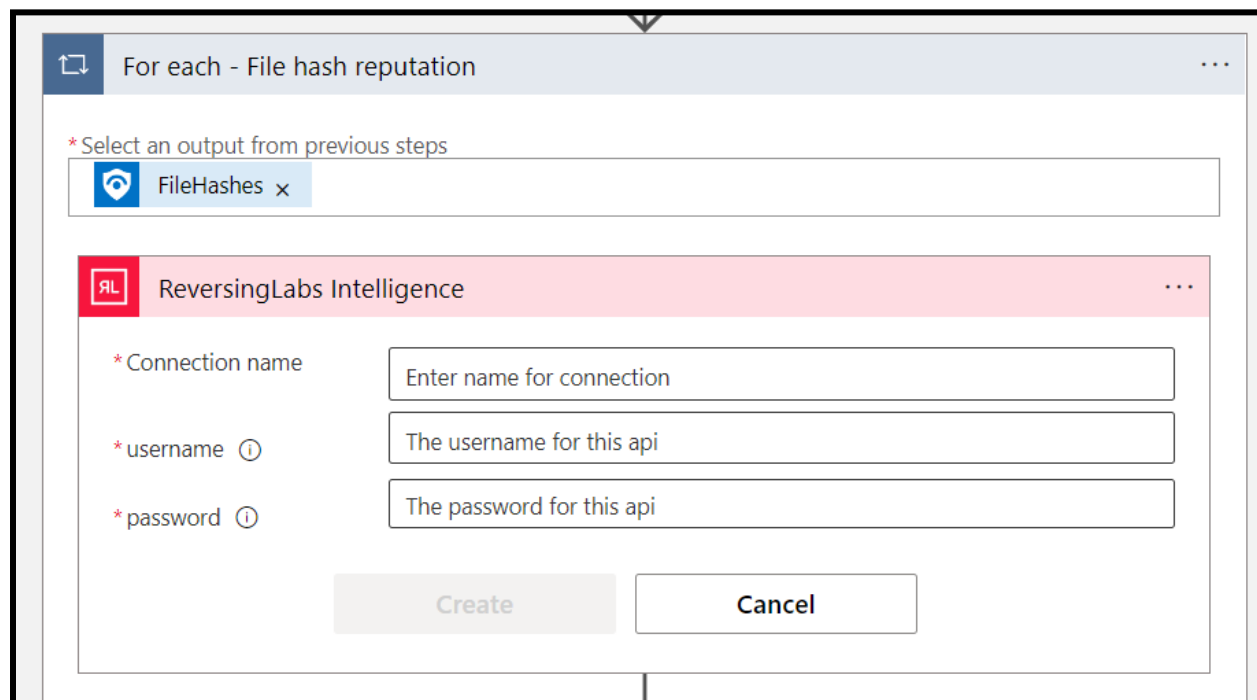
Setting up the API connection for the Microsoft Sentinel connector for the first time is out of scope for this document. Please refer to the following Microsoft documentation for recommendations on authenticating playbooks to Microsoft Sentinel:

<https://learn.microsoft.com/en-us/azure/sentinel/authenticate-playbooks-to-sentinel>

To configure the ReversingLabs connector, click the “For each - File hash reputation” step to expand. Click the first “ReversingLabs Intelligence” step, then add a new connection. Enter the following details:

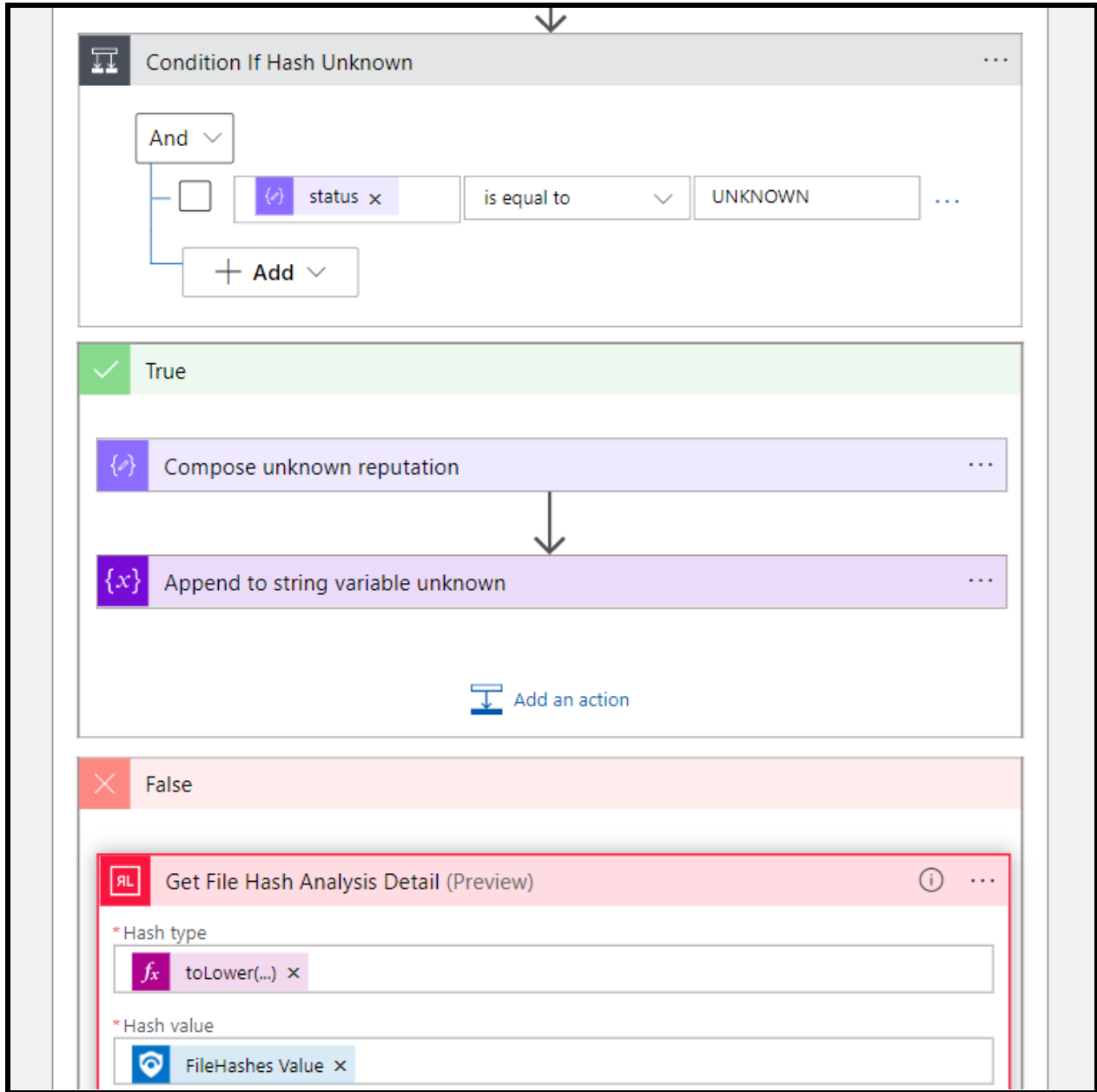
- **Connection name:** friendly name for the connection
- **Username:** your TitaniumCloud username
- **Password:** your TitaniumCloud password

Click “Create” to save the new API connection.

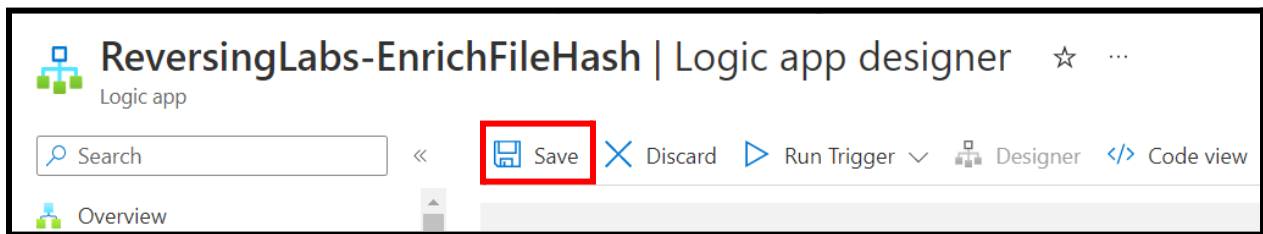


The screenshot shows a configuration window titled "For each - File hash reputation". At the top, there is a dropdown menu showing "FileHashes" with a close button. Below this, there is a section for "ReversingLabs Intelligence" with a red header. This section contains three input fields: "Connection name" with the placeholder "Enter name for connection", "username" with the placeholder "The username for this api", and "password" with the placeholder "The password for this api". At the bottom of this section are two buttons: "Create" and "Cancel".

Click the “Condition If Hash Unknown” step, expand the “False” path if necessary, then select the final “ReversingLabs Intelligence” step. Select the API connection you created previously.



After verifying all API connections have been updated, click "Save" to update the playbook:



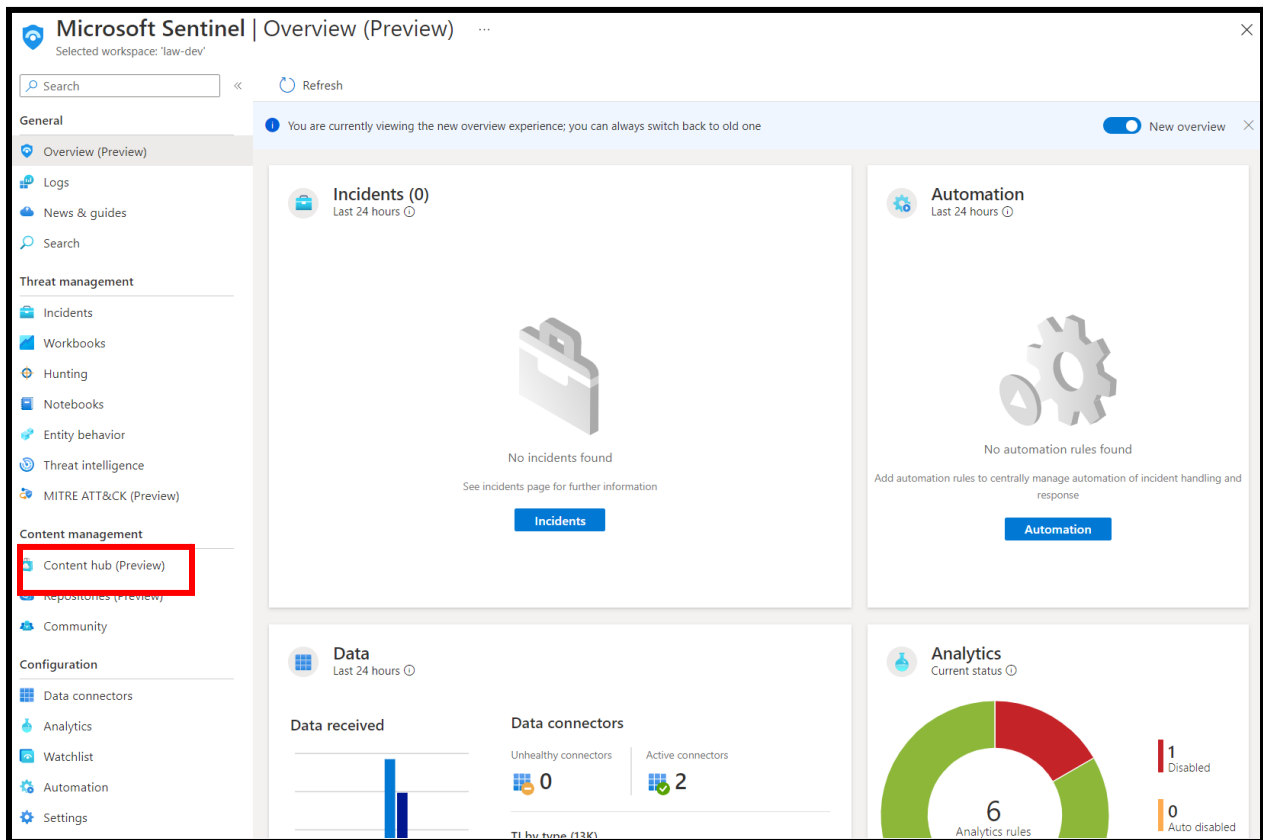


## 6. Managing the solution

This section describes how to manage the solution content, including reinstallation and removal.

### 6.1. Accessing the solution content manager

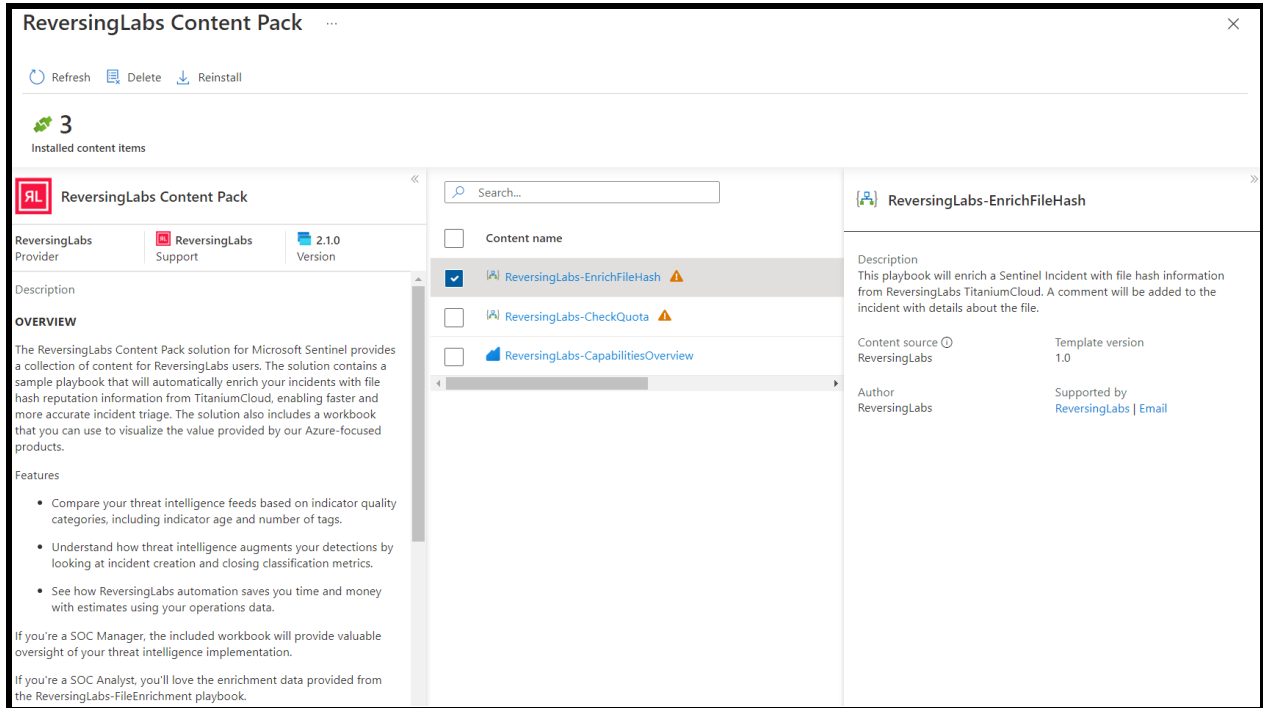
Microsoft Sentinel provides a simple management interface for each solution's content. To access the content manager, navigate to the Content Hub from the Sentinel menu blade.



Next, search for the ReversingLabs solution. Click "Manage" to open the content manager.

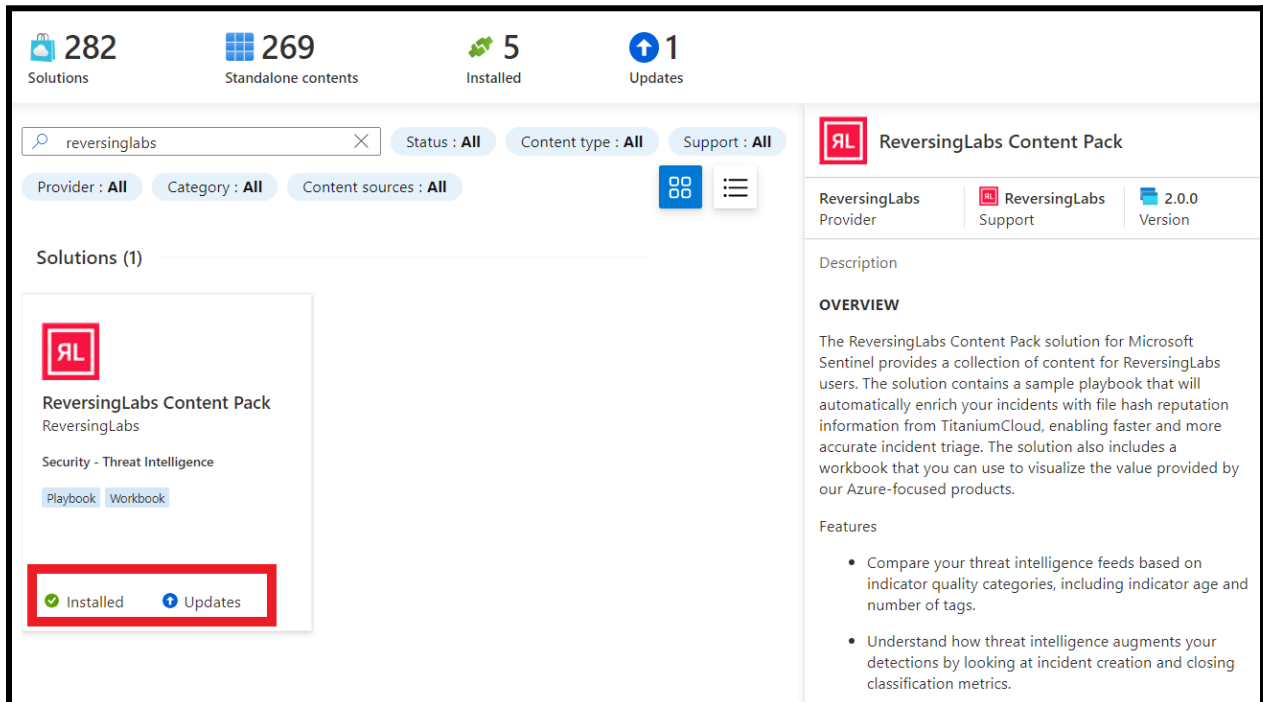
The screenshot shows a web interface for managing content. At the top, there is a search bar with 'reversinglabs' and several filter buttons: 'Status: All', 'Content type: All', 'Support: All', 'Provider: All', 'Category: All', and 'Content sources: All'. A 'Solutions (1)' section displays a card for 'ReversingLabs Content Pack' by 'ReversingLabs', categorized under 'Security - Threat Intelligence'. The card lists 'Playbook (2)' and 'Workbook' as content items and shows a green checkmark indicating it is 'Installed'. To the right, a detailed view of the 'ReversingLabs Content Pack' is shown, including its provider (ReversingLabs), support (ReversingLabs Support), and version (2.1.0). The description explains that the solution provides content for Microsoft Sentinel users, including a sample playbook for enrichment and a workbook for visualization. A list of features includes comparing threat intelligence feeds, understanding how threat intelligence augments detections, and seeing how automation saves time and money. The interface also includes a 'Manage' button (highlighted with a red box), an 'Actions' dropdown menu, and a 'View details' link.

In the content manager, you'll see the solution details, and a list of each content item included with the solution.

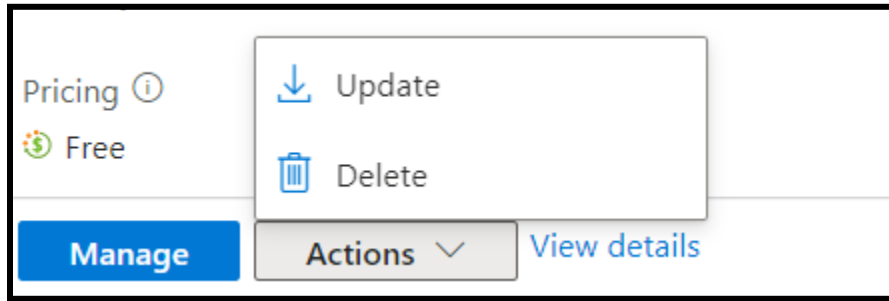


## 6.2. Updating the solution

When a new update is available for the solution, the content hub will indicate as such:



To install the update, click the “Actions” button, then click “Update”:

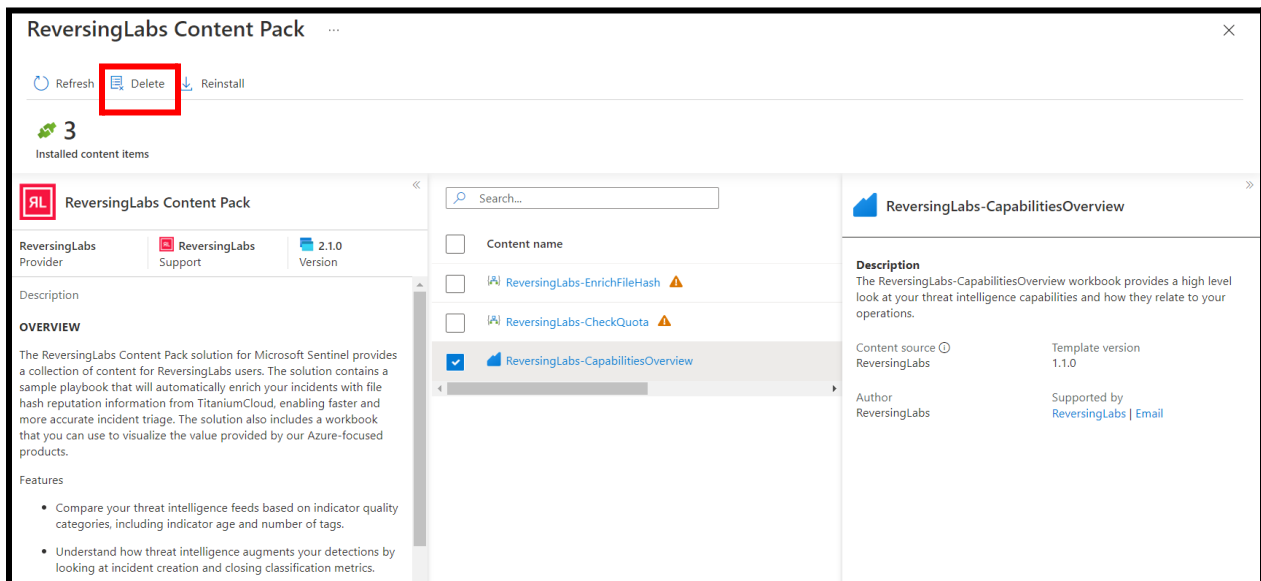


Note that this will not automatically update any installed content items - you will need to manually re-deploy them.

### 6.3. Deleting solution content

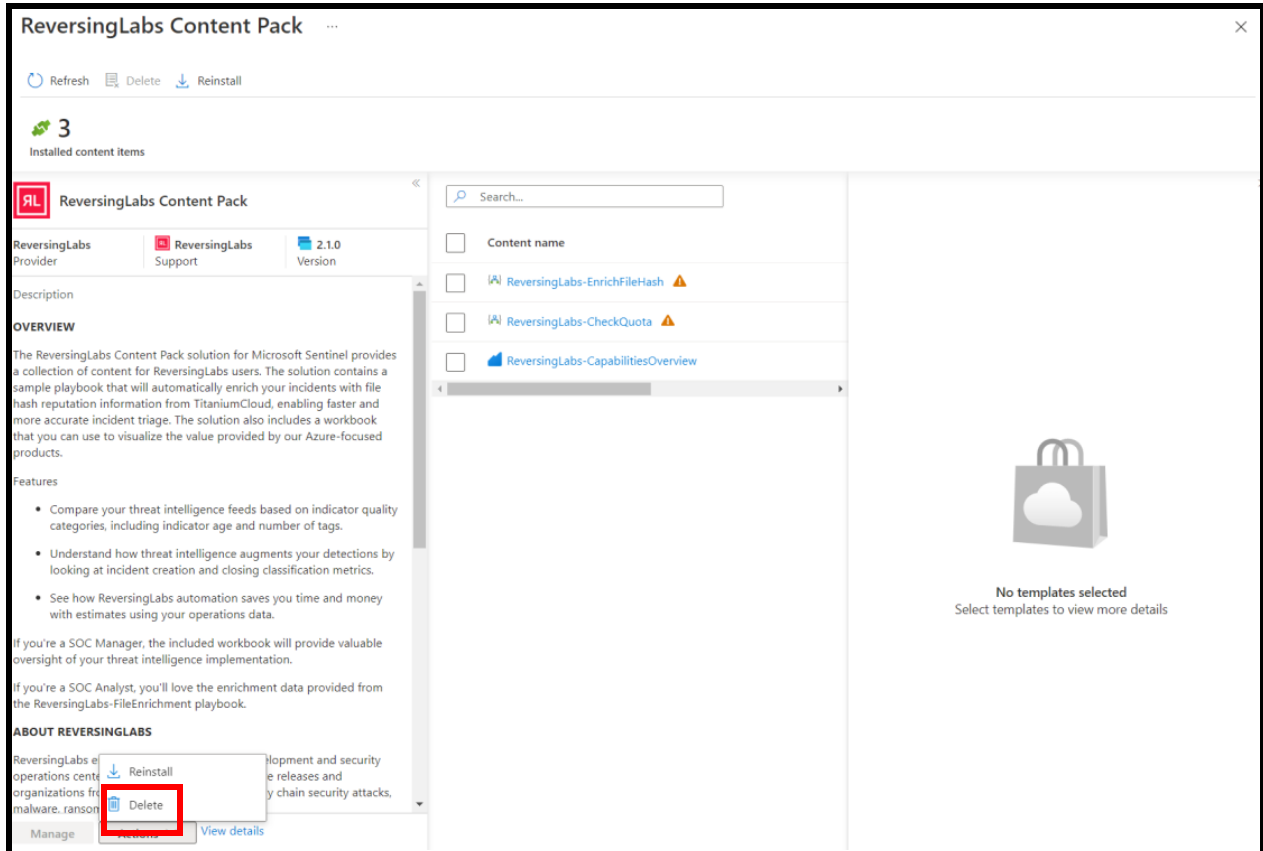
To delete any deployed content, you can either delete the content item from the solution content manager, or from the content items respective menu within Microsoft Sentinel.

To delete a content item from the solution content manager, select the box next to the item you wish to delete, then click the “Delete” button:



### 6.4. Uninstalling the solution

To uninstall the solution, simply click the “Actions” button, then select “Delete”. Note that this will not delete any of the installed content items already deployed in your Microsoft Sentinel environment. To delete the installed content items, see the previous section.



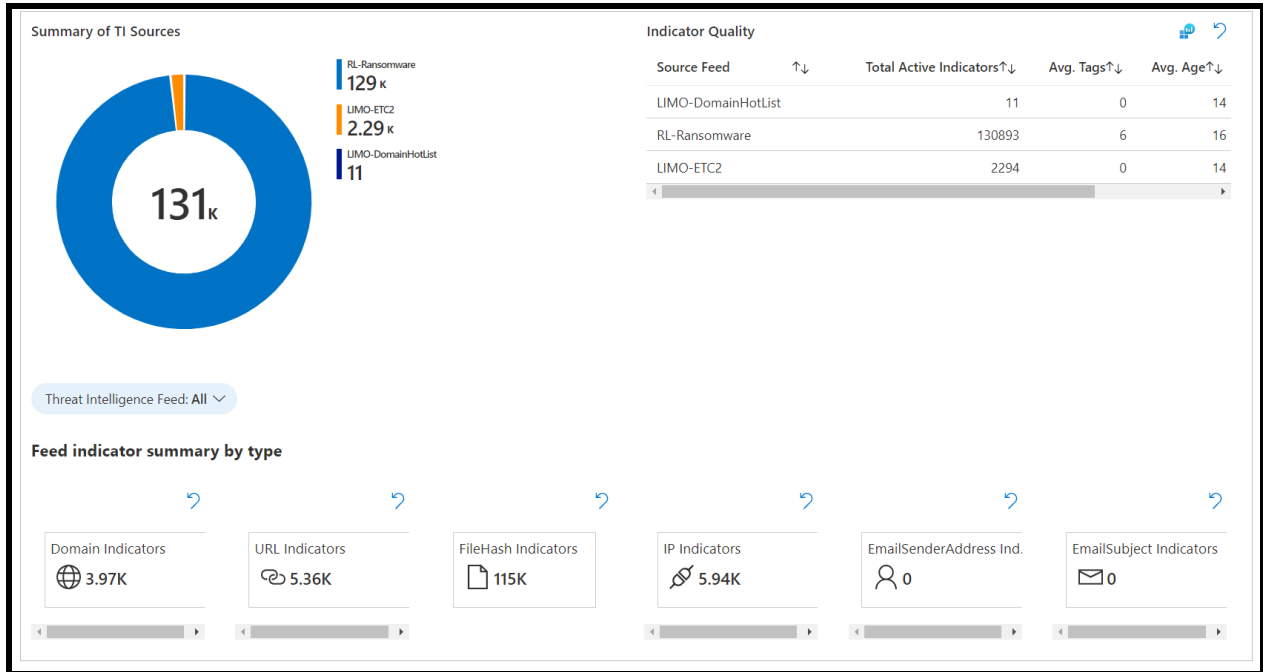
## 7. Using the solution content

This section describes how to use the content provided in the Reversing content pack solution.

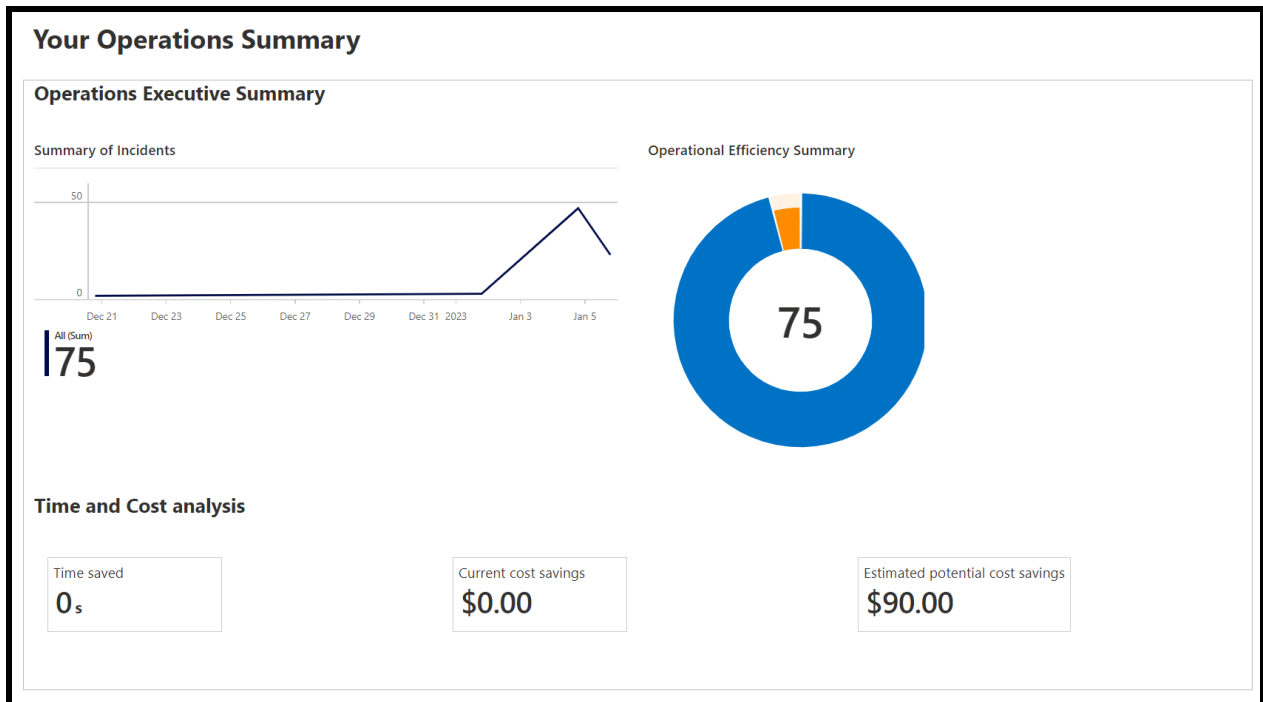
### 7.1. Using the ReversingLabs-CapabilitiesOverview workbook

The workbook is designed to provide an overview of your threat intelligence implementation within Microsoft Sentinel. The workbook contains a few helpful tips on how to interpret the data, which can also be hidden using the “Guide” parameter at the top of the workbook.

The “Threat Intelligence” tab provides some useful metrics for your threat intelligence feeds, including a breakdown of number of indicators, tags, average age, and indicator uniqueness. You will also find details on incidents created from each threat intelligence feed, as well as the overall number of true vs. false positive outcomes for each feed.



The operations tab provides an overview of how ReversingLabs threat intelligence and automation impact your Sentinel environment. Here you can see the total number of incidents and a breakdown of the number of incidents being automated by playbook types. Finally, a time and cost savings analysis is provided to show your estimated savings using ReversingLabs threat intelligence and automation playbooks.



## 7.2. Using the ReversingLabs-EnrichFileHash playbook

The ReversingLabs-EnrichFileHash playbook can be run manually or automatically with an automation rule. To manually run the playbook, first select an incident containing file hash entities. Click “Actions”, then “Run playbook”:

The screenshot displays the Microsoft Sentinel interface. At the top, there are summary cards for 'Open incidents' (73), 'New incidents' (73), and 'Active incidents' (0). A bar chart shows 'Open incidents by severity' with categories: High (1), Medium (67), Low (4), and Informational (1). Below this is a search bar with 'all' and a filter for 'Severity: All'. A table lists incidents, with one selected: 'Informational' severity, Incident ID '1184', Title 'DEMO-008: All hash types', and 1 alert. The right-hand pane shows details for this incident, including 'Alert product names' (Microsoft Sentinel), 'Tasks (Preview)' (0/2 completed), 'Evidence' (3 Events, 1 Alerts, 0 Bookmarks), and 'Entities (3)'. A context menu is open over the entities, with 'Run playbook (Preview)' highlighted.

Search “ReversingLabs-EnrichFileHash”, then click “Run”:

The screenshot shows the 'Playbooks' page in Microsoft Sentinel. It includes a search bar with 'ReversingLabs-EnrichFileHash' and a subscription filter for 'ReversingLabs-Demo-Subscription'. Below is a table of playbooks:

| ↑↓ Name ↑↓                     | Subscription ↑↓   | Resource group ↑↓ | Plan ↑↓     |     |
|--------------------------------|-------------------|-------------------|-------------|-----|
| ☆ ReversingLabs-EnrichFileHash | ReversingLabs-... | rsg-rl-demo-se... | Consumption | Run |

Wait a few seconds, then open up the incident and navigate to the comments. You should see the file hash reputation results from TitaniumCloud:

The screenshot displays a security incident response dashboard. On the left, a sidebar for incident 'DEMO-008: All hash types' (ID: 1184) shows details like 'Unassigned Owner', 'Alert product names' (Microsoft Sentinel), and 'Evidence' (3 Events, 1 Alerts, 0 Bookmarks). The main area shows a 'Comments (6)' tab. A comment from 'ReversingLabs - Enrich File Hash' (dated 01/09/23, 10:25 PM) is visible, containing a table of reputation results:

|                    |   |
|--------------------|---|
| Hash (SHA256)      | 2ac4f0fc16f41a4e9cf031d81e06534e0a668ecff484d05c171ac4b7d9c89e6   |
| Status             | <b>MALICIOUS</b>  |
| Status Description | The sample was classified as malicious by ReversingLabs proprietary algorithms. This classification is reserved for high-accuracy heuristics and named threats, such as Emotet, Dridex and WannaCry. Threat severity is expressed through the threat level value on a scale of 1-5. The higher the value, the more severe the threat. |
| Threat Name        | ByteCode-MSIL.Trojan.RedLine  |
| Threat Level       | 5   |

The results will include the following information:

- **Hash:** the submitted file hash
- **Status:** the malware presence status designation of the file hash (malicious/known/suspicious/unknown)
- **Status Description:** further describes the status designation
- **Threat Name:** if available, the given threat name for the sample
- **Threat Level:** Threat level value for the requested sample (0 indicates no threat; 1 is the lowest threat value - lowest severity, such as Adware; 5 is the highest threat value, e.g, Trojan)
- **Trust factor** (known files only): value of the sample's sources (0 is the most trusted; 5 is the least trusted)
- **Reason:** clarifies the reason why a sample received a particular classification status.
- **File Details:** contains a summarized natural language description of the file's behavior and properties.
- **Scanner Detection:** Number of AV scanners that detected malware in the last scan



## 8. Support

If you have any questions, please contact ReversingLabs support at [support@reversinglabs.com](mailto:support@reversinglabs.com).