

QRadar Integration

Cyble Infosec Pvt Ltd

Introduction:

Cyble Threat Intel, an advanced cybersecurity workflow based on QRadar's Universal REST API Protocol, built for QRadar platform, enables users to monitor events/alerts efficiently. This application allows users to actively prevent potential threats and gain valuable insights for immediate action. By adopting Cyble Threat Intel, organizations can enhance their security operations and confidently safeguard their digital assets. Users can leverage the data obtained through Cyble's modular input via APIs. This input can customize their dashboard, establish alerts, and generate reports.

The Cyble Threat Intel QRadar integration has 2 components: Workflow and DSM.

Workflow is a uREST Protocol based configuration which, after configuration, allows user to fetch events/alerts from Cyble Vision platform. The workflow and parameter file can be downloaded from <https://github.com/IBM/IBM-QRadar-Universal-Cloud-REST-API/tree/master/Community%20Developed/Cyble%20Threat%20Intel>. Detailed steps for configuration are given later in this document.

DSM is an application which helps the user to properly parse and clearly display the data fields in QRadar log activity table. The integration will work without DSM as well. But since data will not be parse properly, the user will see the raw data. Nevertheless, the workflow will work with or without DSM.

Pre-requisite:

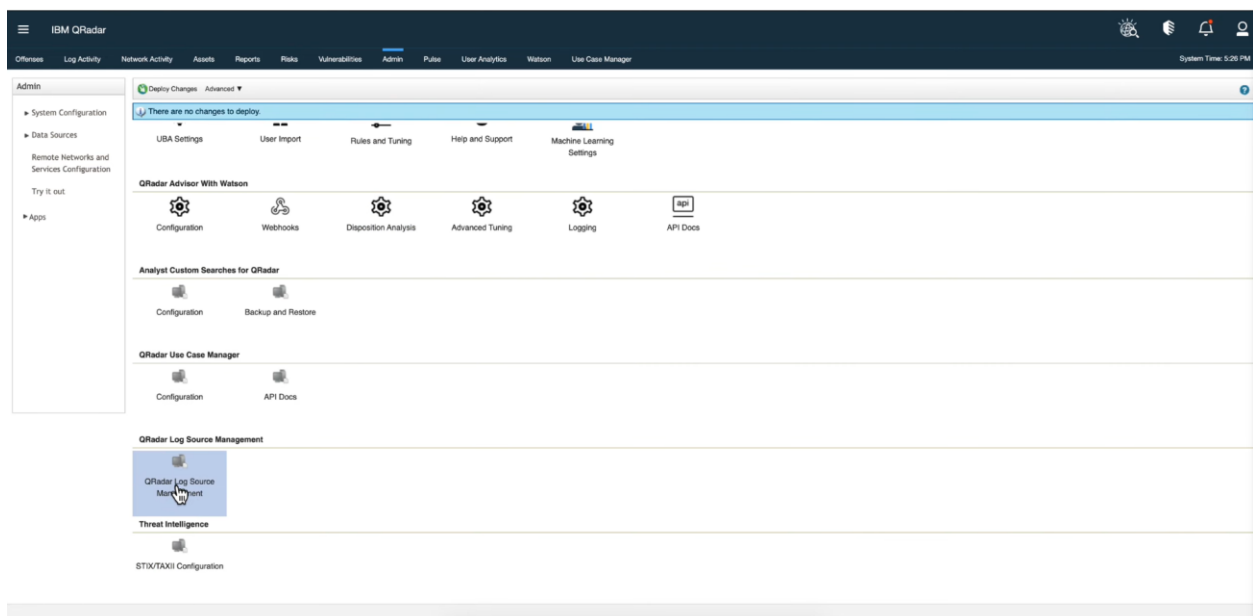
1. The user must have the Cyble Vision API Key with them. They can obtain this key from our Vision platform or by contacting CSM.
2. Install the 'Cyble Threat Intel DSM' Extension from the IBM App Exchange. If you don't, you won't find 'Cyble Threat Intel (DSM)' in the Log Source Types and will not be able to correctly parse the events.

Note: DSM might not be available as it is still in review. You may skip this step for now.

Procedure to configure QRadar:

Step 1:

Login to your QRadar instance and navigate to the Admin tab. In the Admin tab, click on 'QRadar Log Source Management' app. If you don't see this app, contact your QRadar instance manager to install it from IBM App Exchange.

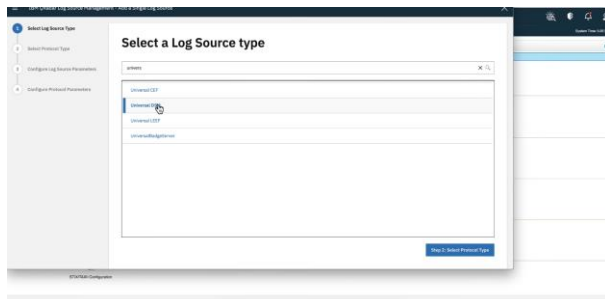
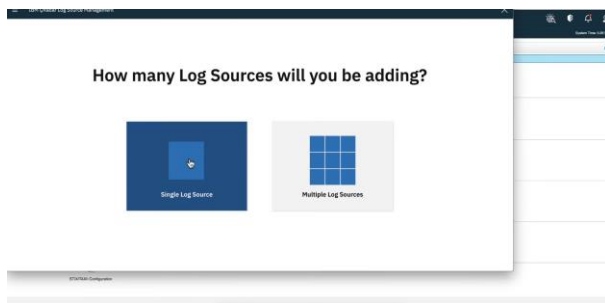
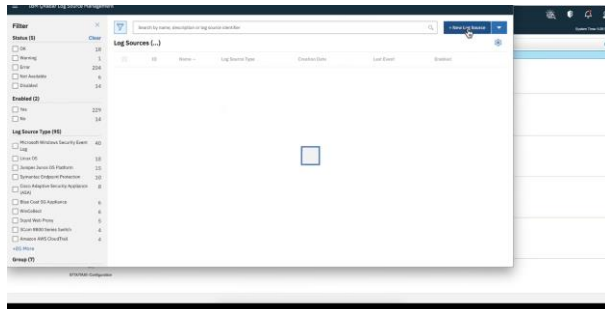
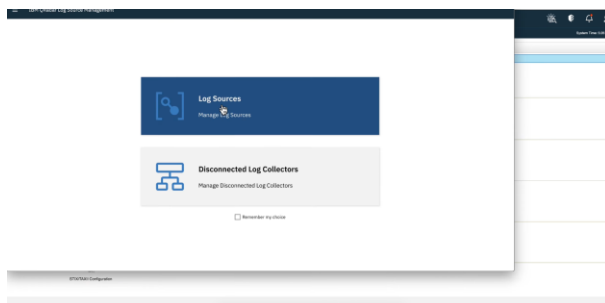


Step 2:

Log Source > New Log Source > Single Log Source > Select a Log Source Type

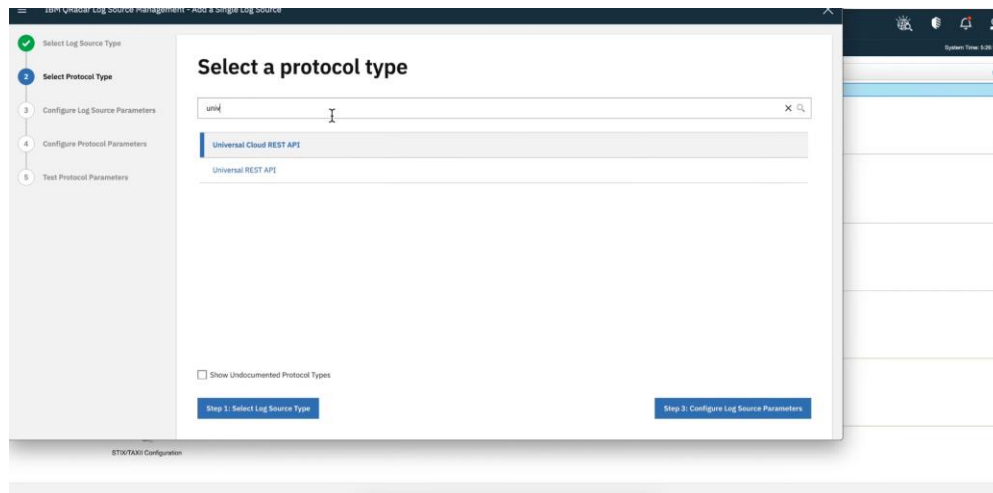
On the Select Log Source Type page, select Cyble Threat Intel (DSM)

If you have not installed Cyble Threat Intel DSM, then select 'Universal DSM' and click on 'Select Protocol Type'



Step 3:

On the Select a Protocol Type page, select "Universal Cloud REST API" and click Configure Log Source Parameters.

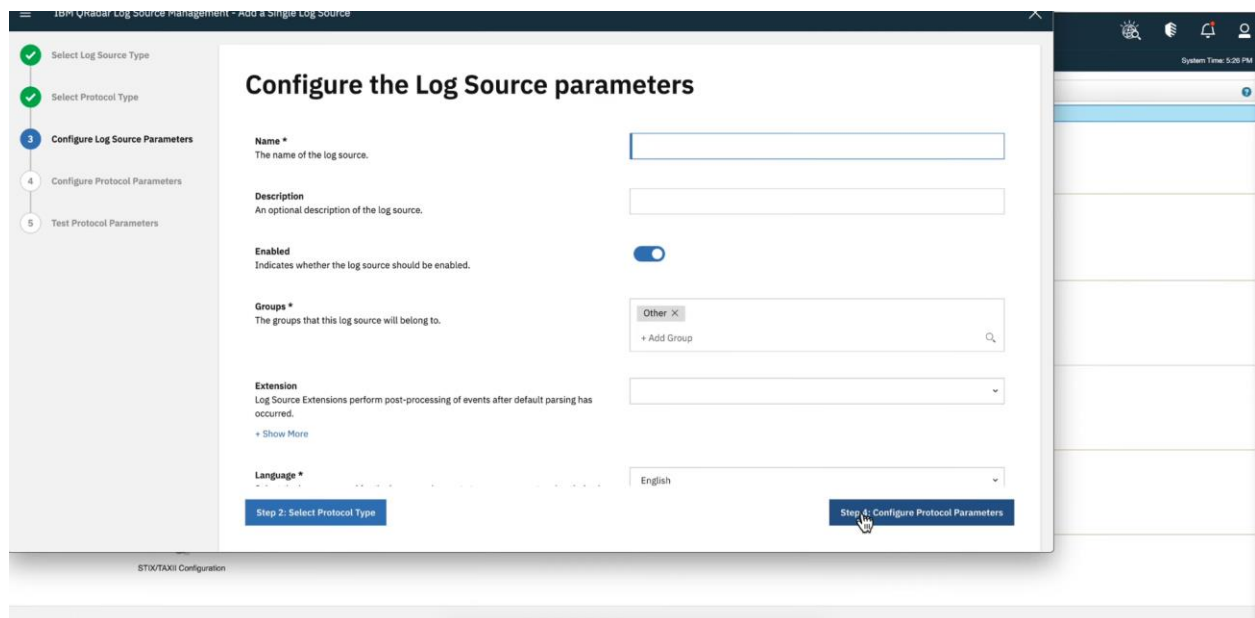


Step 4:

On the Configure the Log Source parameters page, configure the log source parameters:

- Insert a name for this log source (Cyble Threat Intel)

Leave the other fields as default.



Step 5:

On the Configure the Protocol Parameters page, configure:

- Insert a log source identifier (Cyble Threat Intel)

Configure the protocol parameters

Log Source Identifier *

Workflow *

Workflow Parameter Values

Use Proxy
Select this check box if the API is accessed by using a proxy.
+ Show More

Recurrence *
The time interval between each execution of the workflow.
+ Show More

EPS Throttle *

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

- Copy the Workflow XML you downloaded from <https://github.com/IBM/IBM-QRadar-Universal-Cloud-REST-API/tree/master/Community%20Developed/Cyble%20Threat%20Intel> and paste it into the Workflow field

The top screenshot shows the GitHub repository page for 'IBM-Qradar-Universal-Cloud-REST-API'. The file 'Cyble-Threat-Intel-Workflow.xml' is selected in the 'Cyble-Threat-Intel' directory. The file's content is displayed, showing the 'Workflow Parameter Description' section with the following details:

- Author Name: Cyble Inc
- Maintainer Name: developers@cyble.com
- Version Number: 1.0
- Endpoint Documentation: This workflow can be used to pull alerts/events from Cyble Vision.
- Detailed documentation can be found at: <https://cyble.ai/centers/help-center>
- Event Types Currently Supported by the workflow: Cyble Threat Intel Alerts

The bottom screenshot shows the 'Cyble-Threat-Intel-Workflow.xml' file open in the code editor. The XML code is displayed, showing the 'Workflow Parameter Description' section with the following details:

- Author Name: Cyble Inc
- Maintainer Name: developers@cyble.com
- Version Number: 1.0
- Endpoint Documentation: This workflow can be used to pull alerts/events from Cyble Vision.
- Detailed documentation can be found at: <https://cyble.ai/centers/help-center>
- Event Types Currently Supported by the workflow: Cyble Threat Intel Alerts

- Copy the Workflow Params (make sure your hostname, api_key and fetch_since are populated within the quotes) into the Workflow Parameters Values field

hostname: api.cyble.ai

api_key: <obtained_above>

fetch_since: data of how many previous days user wishes to fetch. Maximum value is 30 days.

The top screenshot shows the GitHub repository page for 'IBM-QRadar-Universal-Cloud-REST-API'. The left sidebar shows the file structure, with 'Cyble Threat Intel' selected. The main content area shows a table of recent commits:

Name	Last commit message	Last commit date
..		
Cyble-Threat-Intel-Workflow-Parameter-Values.xml	Implemented Review Changes	4 days ago
Cyble-Threat-Intel-Workflow.xml	Implemented Review Changes	4 days ago
README.md	Review changes	4 days ago

The bottom screenshot shows the 'Cyble-Threat-Intel-Workflow-Parameter-Values.xml' file. The XML content is as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<WorkflowParameterValues xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/WorkflowParameterValues/v1">
  <Value name="hostname" value="" />
  <Value name="api_key" value="" />
  <Value name="fetch_since" value="" />
</WorkflowParameterValues>
```

- Set 30M as the Recurrence

Click on Test Protocol Parameters

Step 6:

- In the Test protocol parameters window, click Start Test. All tests should pass.
- To fix any errors, click Configure Protocol Parameters. Configure the parameters and click Test Protocol Parameters.

- Click Finish

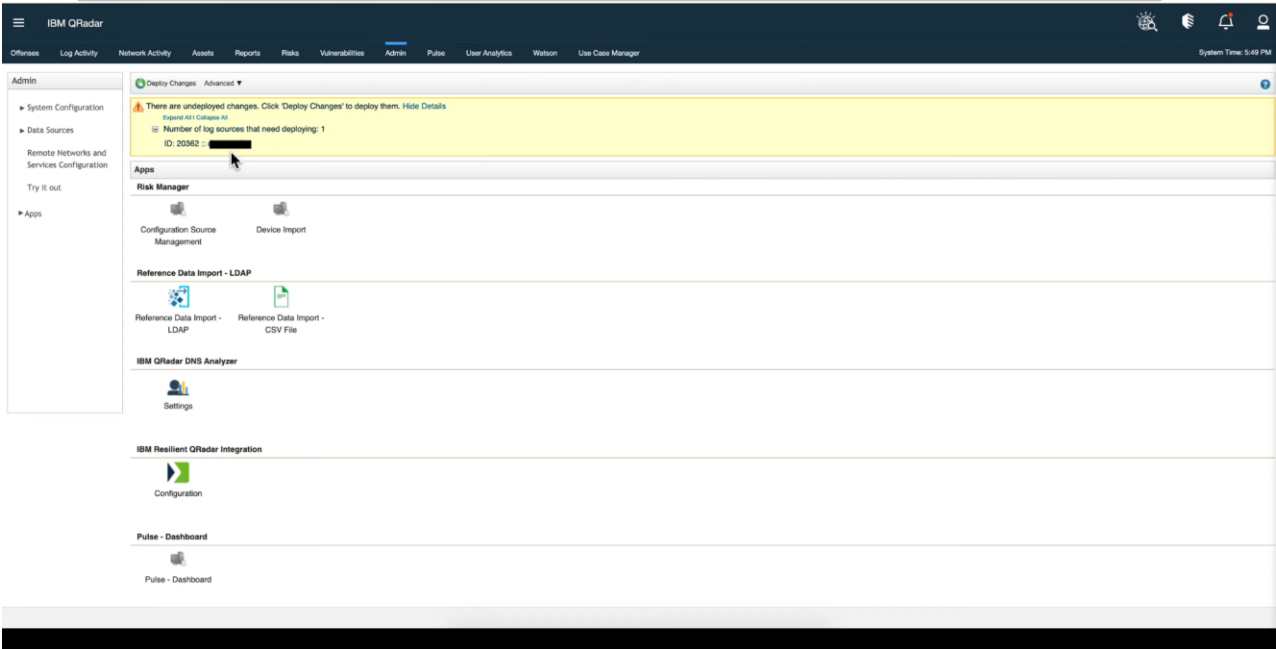
The image displays two screenshots of the IBM QRadar Log Source Management interface, specifically the 'Test Protocol Parameters' step in the 'Add a Single Log Source' workflow.

Top Screenshot: This view shows the initial state of the 'Test Protocol Parameters' step. The left sidebar indicates the progress: 'Select Log Source Type', 'Select Protocol Type', 'Configure Log Source Parameters', and 'Configure Protocol Parameters' are completed (green checkmarks), while 'Test Protocol Parameters' is the current step (blue circle with '5'). The main content area has the title 'Test Protocol Parameters' and a sub-header 'Test this log source configuration to ensure that the parameters are correct.' Below this, explanatory text states: 'The test runs from the host specified by the Target Event Collector parameter. If there is high network latency between the console and this host, it may take a moment for the results to appear.' and 'The test collects sample event data from the target system. This feature can be disabled in the settings.' A large blue button with a checkmark icon and the text 'Start Test' is centered. At the bottom, there are two buttons: 'Step 4: Configure Protocol Parameters' on the left and 'Skip Test and Finish' on the right, which is being clicked by a mouse cursor.

Bottom Screenshot: This view shows the results of the test. The 'Test Protocol Parameters' step is now complete, indicated by a green checkmark and the word 'Restart' below it. The 'Results (3):' section lists three successful tests: 'Testing DNS resolution of [redacted]', 'Testing TCP connection to [redacted]', and 'Testing SSL connection to [redacted]'. Below this, the 'Events (5):' section displays a table of log events. The table has two columns: 'Log Source Identifier' and 'Payload ~'. The first event shows an 'admin_self_activate' action with a phone number. The second event shows an 'admin_login' action with a username and device ID. At the bottom, there are two buttons: 'Step 4: Configure Protocol Parameters' on the left and 'Finish' on the right, which is being clicked by a mouse cursor.

Step 7:

Do a full configuration deploy (Deploy Changes -> Advanced -> Deploy Full Configuration)



Step 8:

User shall see the logs in Log Activity tab

