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.

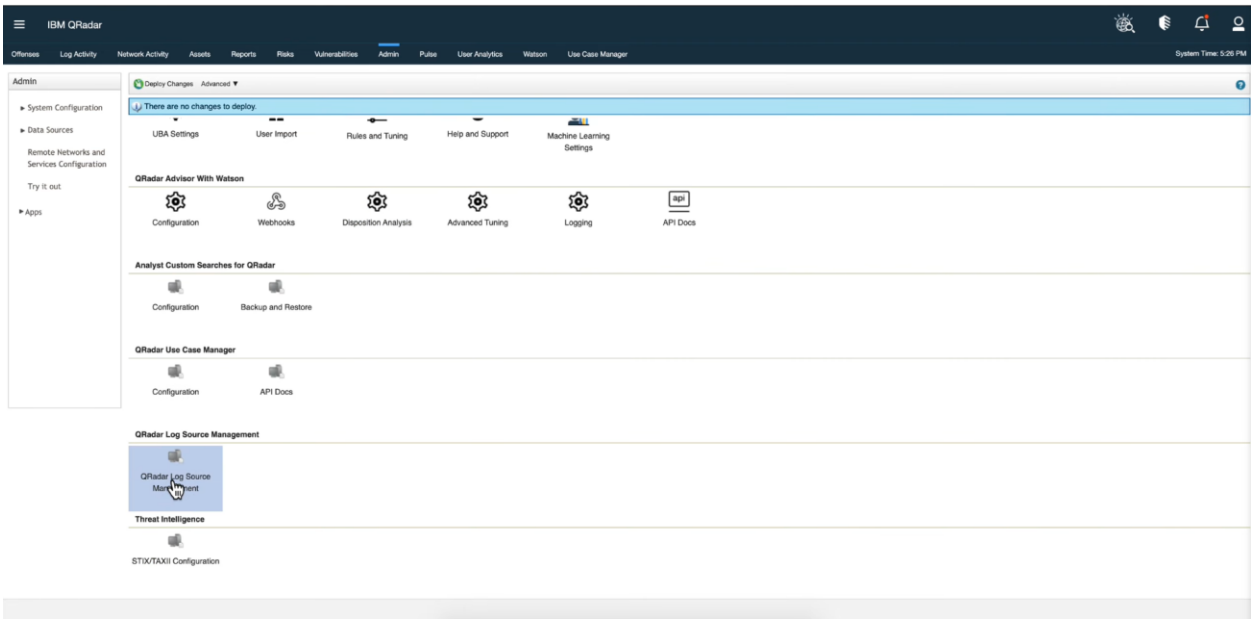
Pre-requisite:

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.

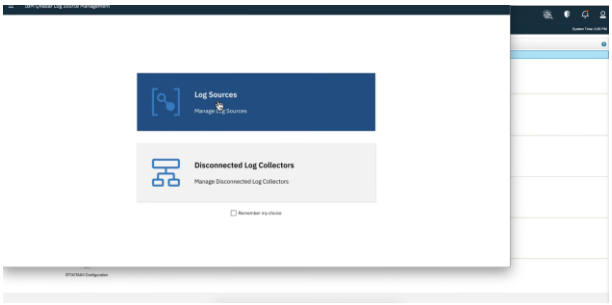


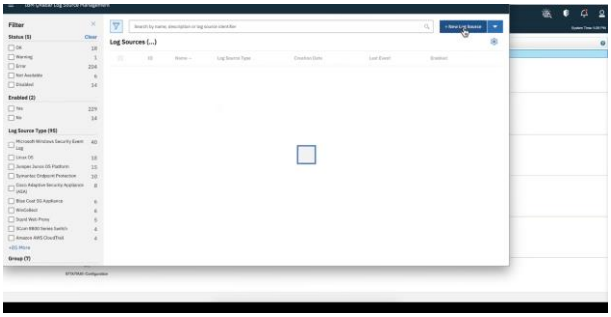
Step 2:

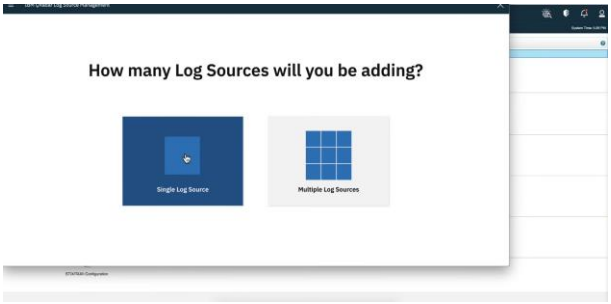
Log Source > New Log Source > Single Log Source > Select a Log Source Type

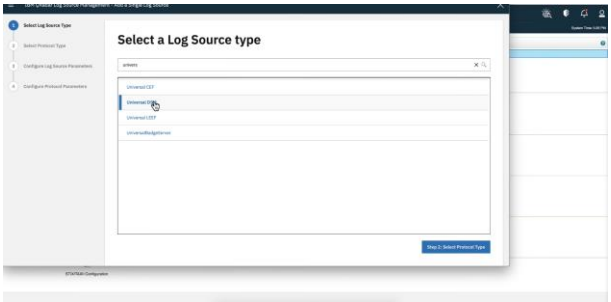
On the Select Log Source Type page, select Cyble Threat Intel (DSM)

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



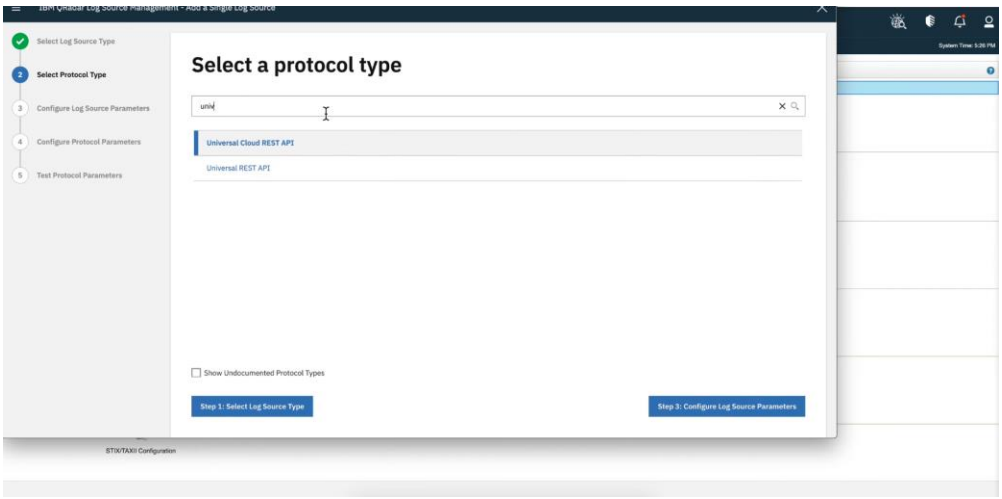






Step 3:

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

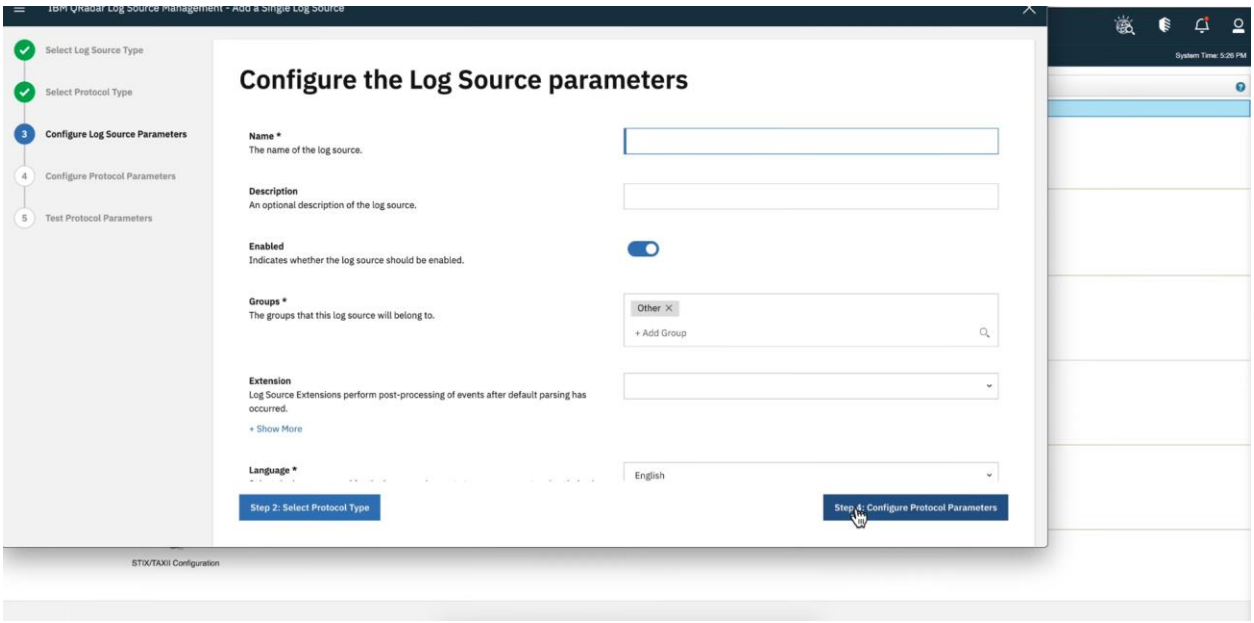


Step 4:

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

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

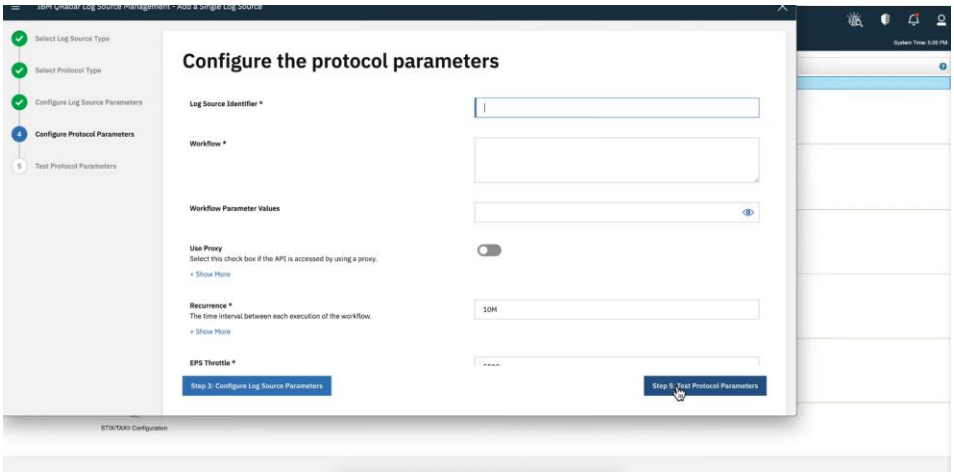
Leave the other fields as default.



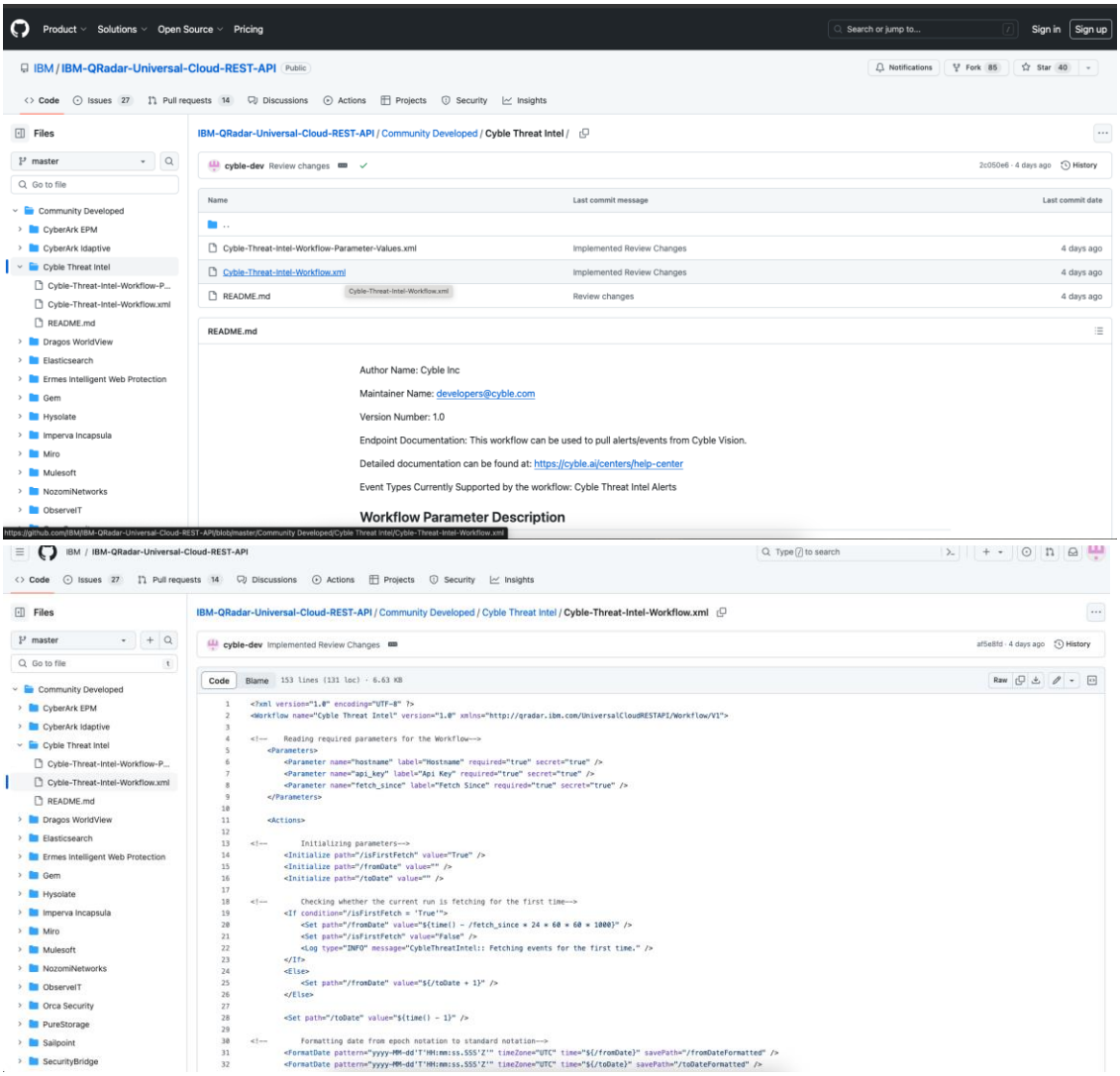
Step 5:

On the Configure the Protocol Parameters page, configure:

- Insert a log source identifier (Cyble Threat Intel)

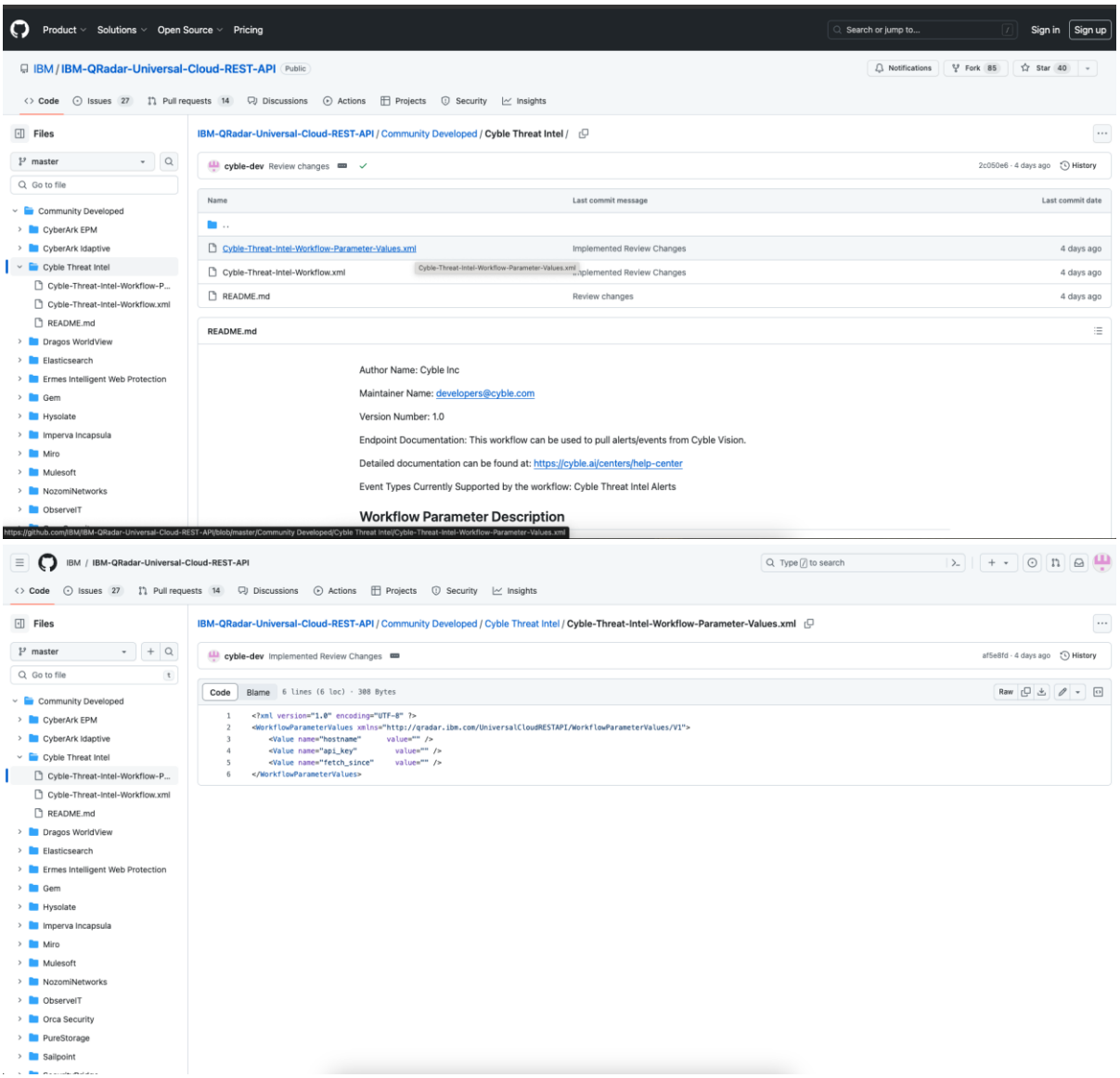


- Copy the Workflow XML you downloaded from https://github.com/IBM/IBM-QRadar-Universal-Cloud-REST-API/tree/master/Community%20Developed/Cyble%20Threat%20Intel and paste it into the Workflow field



- 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.



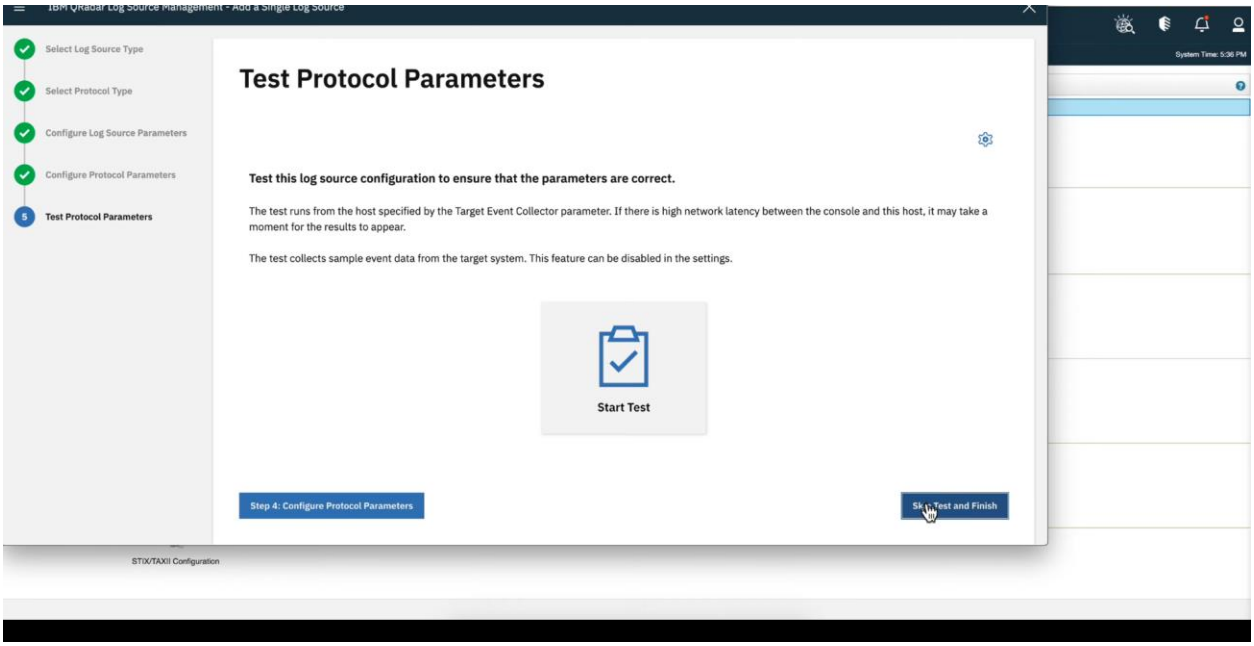
- Set 30M as the Recurrence

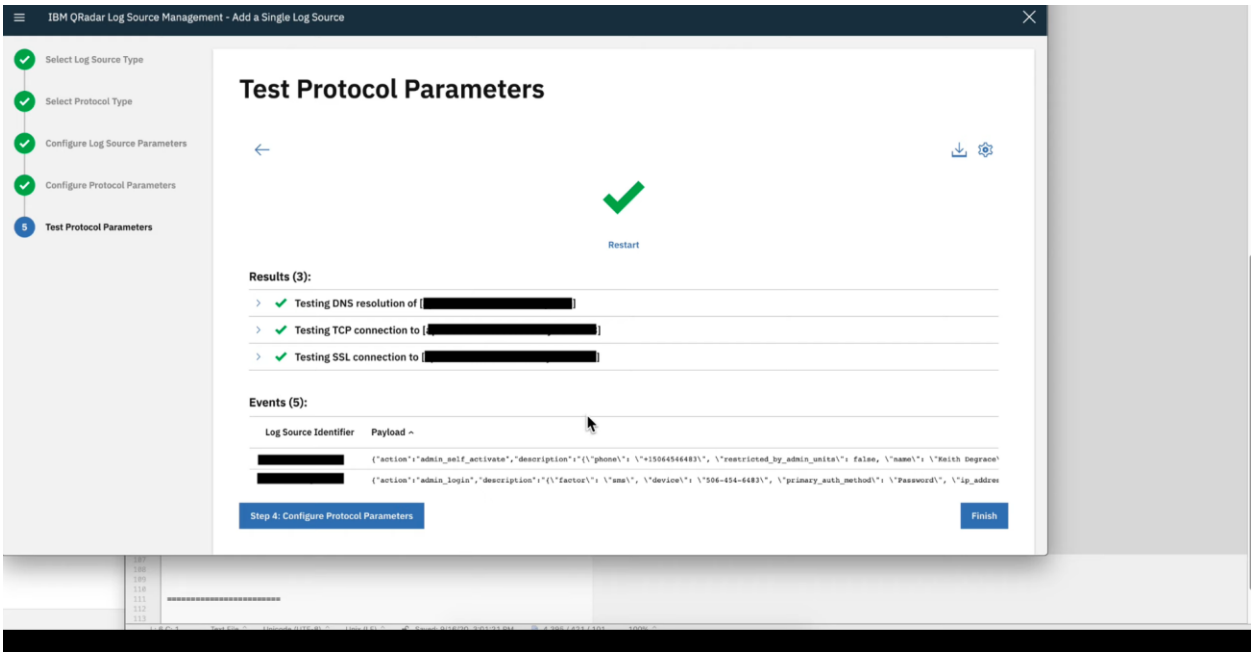
Click on Test Protocol Parameters

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.

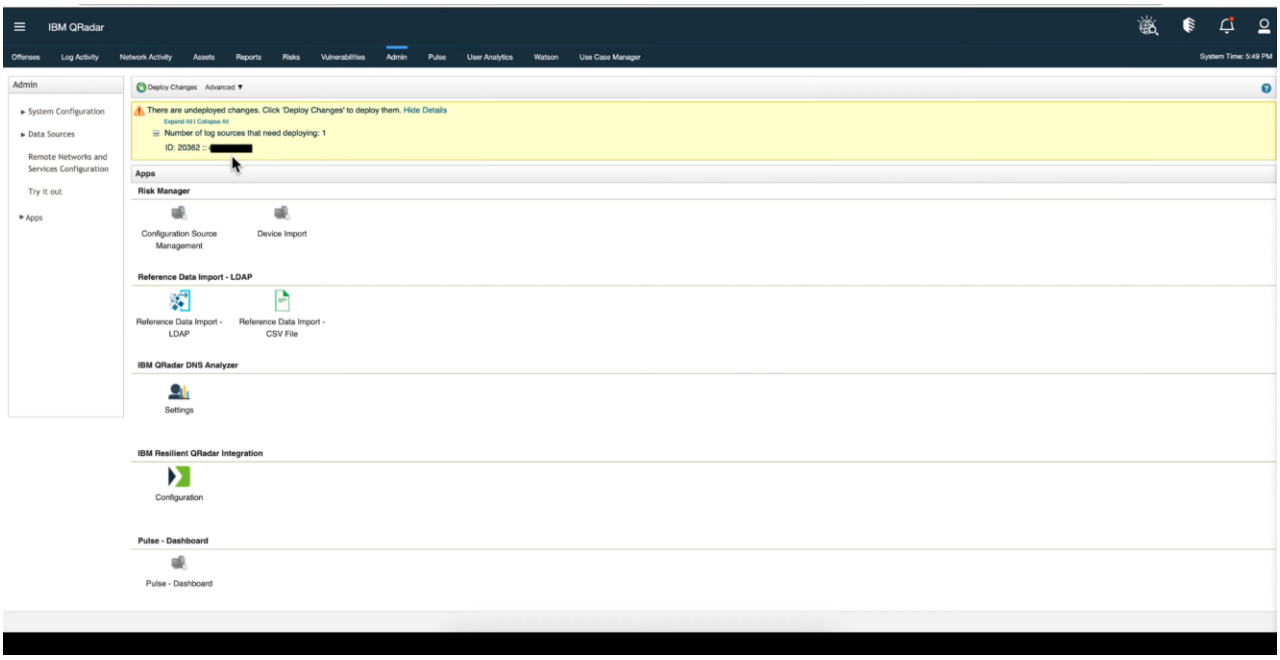
- Click Finish





Step 7:

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



Step 8:

User shall see the logs in Log Activity tab