Integrate XDR with Umbrella

Contents

Introduction

This document describes how to integrate XDR with Umbrella.

Prerequisites

- XDR Admin account
- Umbrella Admin account
- Umbrella Investigate API
- Umbrella Enforcement API
- Umbrella Reporting API

Requirements

Components Used

XDR Console.

Umbrella Console.

Configure

In XDR, navigate to Administration > Integrations.

Under Cisco Integrations, search for Umbrella, click on Get Started.

Give your integration a Name.

In order to obtain the Organization ID, navigate to Umbrella, log in and, look at the URL, the Org ID will come next to the umbrella.com domain.

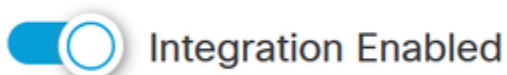Copy it and paste it in the approprite field in XDR.

To obtain Investigate API, navigate to Umbrella > Investigate > API keys.

Create a new token, copy the Access Token in the Investigate API field of XDR.

To obtain the Enforcement URL, navigate to Umbrella > Policies > Integrations settings .

Add an integration, give it a name and ensure the Integration is enabled.

Under the Integration Enabled option, you can find the Integration URL, copy it and paste it on the appropriate field in XDR.

To obtain the Reporting APi key and APi secret, navigate to Umbrella > Admin > Api Keys.

If you have to create an API and Secret, navigate to Legacy keys > Umbrella Reporting.

Click on Generate Token.

Copy the Key and the Secret, ensure to keep them safe as the Secret cannot be retrieved and you will need to refresh your API keys if you lose it.

Paste them in the appropriate field in XDR.

For the Request Timeframe days, you can leave it blank or configure 30 days

Click on Add.

> **Note**: At the top of the page, you have to see a Healthcheck saying: This integration module has no issues.

Verify

Navigate to Administration > Integrations.

Expand the My Integrations panel.

Search for the Integration name you have just created.

Troubleshoot

The Integration did not succeeded unknown API key.

If you face this issue, ensure the API key and API secret of Reporting API are correct, if the API key does not match with the information from Umbrella, you have to refresh the API key and paste the new values.

Events are not Populating XDR Dashboard.

Ensure the events are populating the Umbrella Dashboard.

Bear in mind that Umbrella tiles in XDR are subjected to a cache of 5 minutes, so you have to wait around 5 minutes to start seeing data in XDR.