Integrate Umbrella Logs with Azure Sentinel Using REST API

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Overview

Procedure

Introduction

This document describes how to ingest Umbrella logs into Azure Sentinel via REST API.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

If you use Azure Sentinel as a SIEM, you can ingest Umbrella logs into it. This article describes the process required to complete the integration.

Procedure

To ingest Umbrella logs into Azure Sentinel by using the REST API, complete these steps:

1. Access the documentation for integrating Umbrella with Azure Sentinel.

2. Adhere to all detailed instructions for configuration in the Microsoft documentation.

Read more in the Microsoft integration guide.