# Understand Data Management with Log Exports or Reporting API

## Contents

## Introduction

This document describes how to manage data with log exports or the Reporting API in Cisco Umbrella.

## 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

Umbrella is a powerful tool that gives you a lot of information about your internet traffic. Here is a simple guide to help you decide how to best consume your data:

| Use Case | Granularity / Type | Recommendation | Considerations |
|---|---|---|---|
| Compliance/Long term event retention | Export and store all events | S3: Customer-owned bucket | It is possible to use Cisco Managed Bucket but information is only retained up to 30 days. |
| SIEM: Event Correlation | Export all events | S3: Cisco-managed bucket | Information is only retained up to 30 days; offloading needs to be handled. |
| Dashboard KPI/Widgets | Activity Search/Aggregations | Reporting API | Query must be well tuned as a broad query can result in timeouts. |

| | | | |
|---|---|---|---|
| Generate Reports | Aggregations | Reporting API | |
| SOAR Workflow: Trigger | Activity Search | Reporting API | Query must be well tuned as a broad query can result in timeouts. |

## Additional Information

- Instructions on how to manage your logs: Umbrella documentation-Manage Your Logs
- Instructions on how to manage your APIs: Cisco DevNet-Cisco Cloud Security API