

# Configuring Sumo Logic HTTP Collector

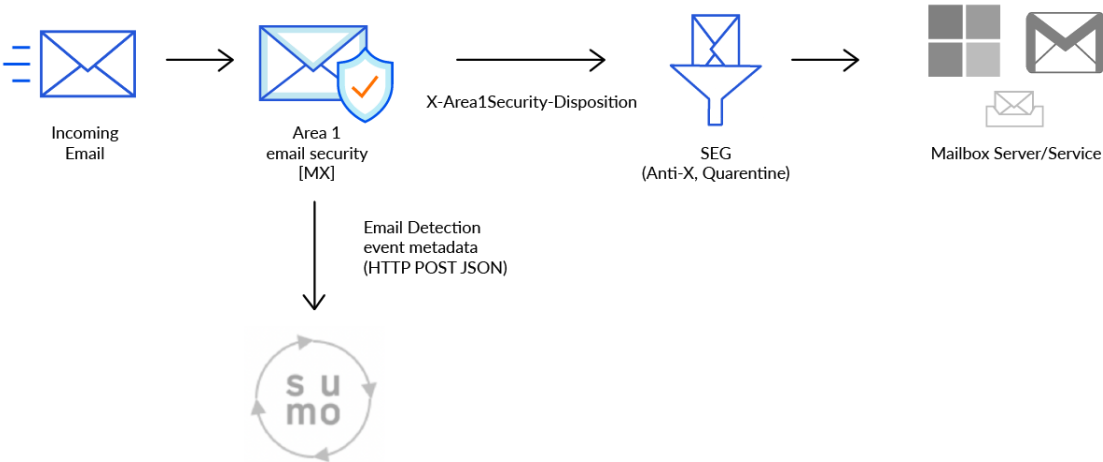
## Cloudflare Area 1 Overview

Phishing is the root cause of upwards of 90% of security breaches that lead to financial loss and brand damage. Cloudflare Area 1 is a cloud-native service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors and comprehensive attack analytics, Cloudflare Area 1 proactively identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Area 1 email security allows customers to take preemptive action against these targeted phishing attacks across all vectors - email, web and network; either at the edge or in the cloud.

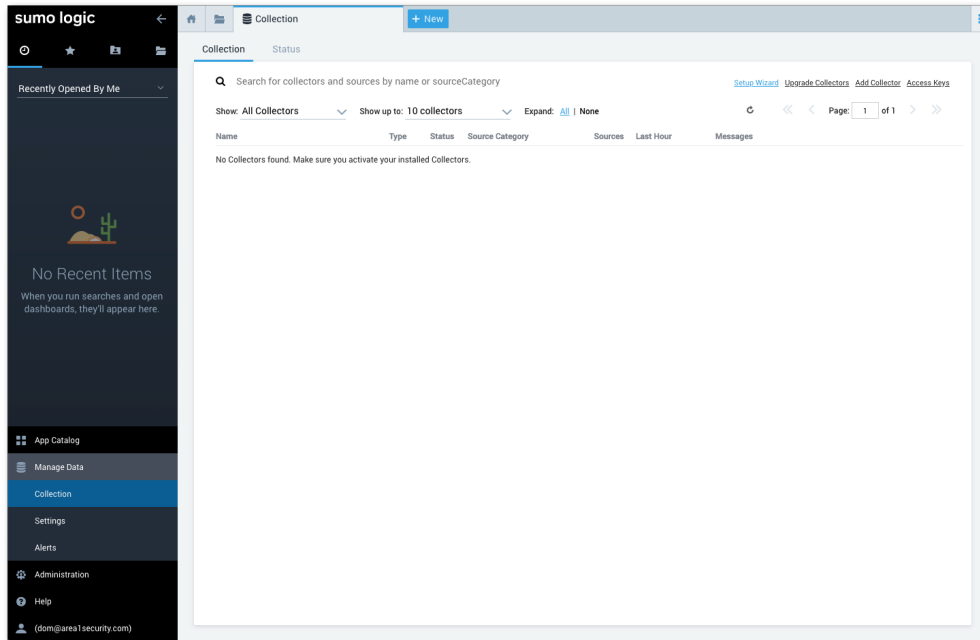
# Cloudflare Area 1 Email Protection

When Area 1 detects a phishing email, the metadata of the detection can be sent directly into your instance of Sumo Logic. This document outlines the steps required to integrate Area 1 with Sumo Logic.

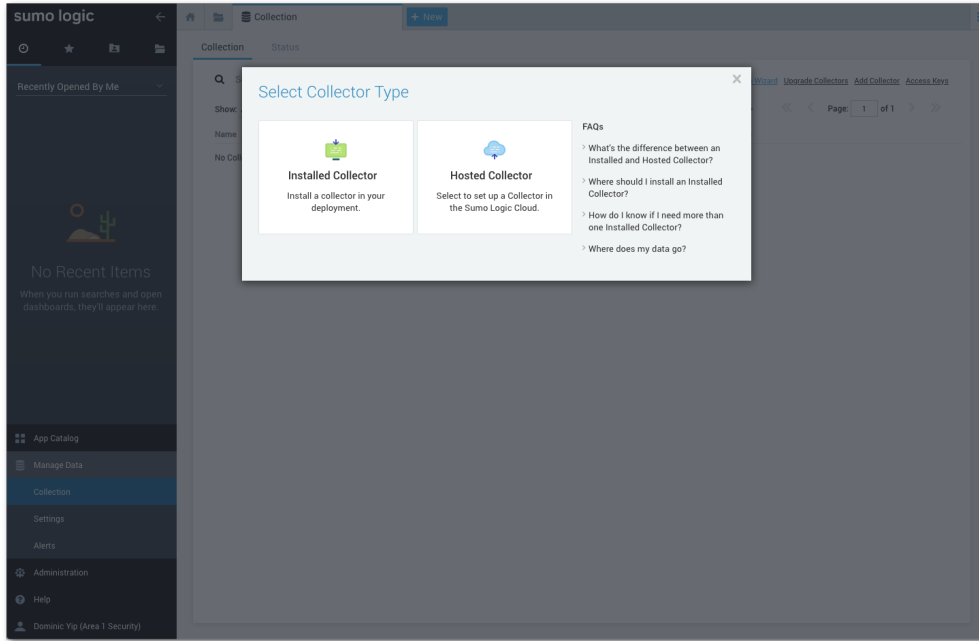


# Configure the Sumologic Collector

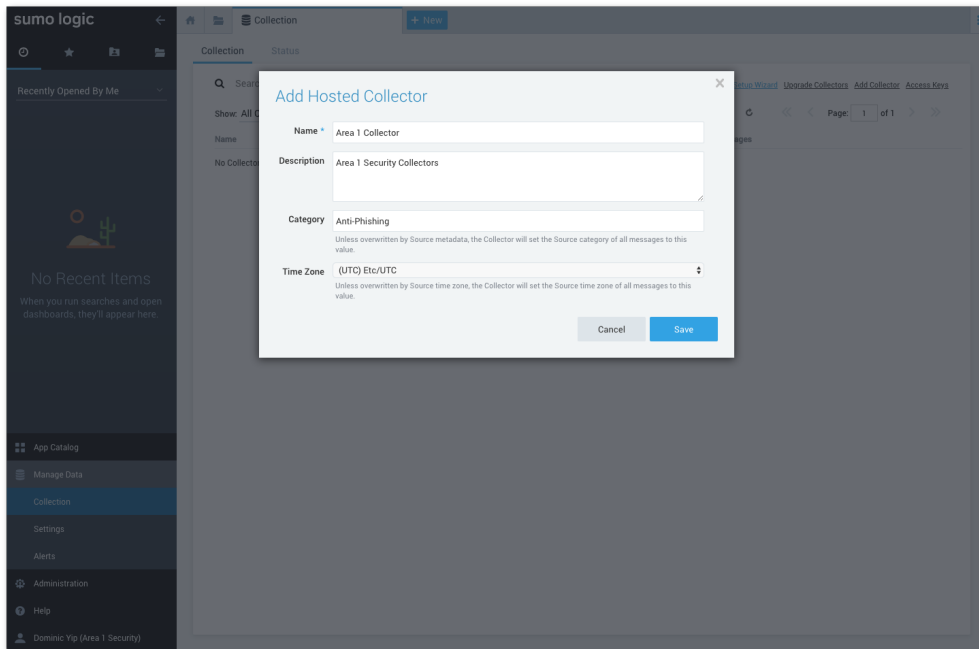
Log into your instance of Sumologic as an administrator and navigate to the collector configuration pane under **Manage Data >> Collection**, located in the left navigation bar. Click on the **Add Collector** option in the top corner of the Collector configuration pane to configure the Collector:



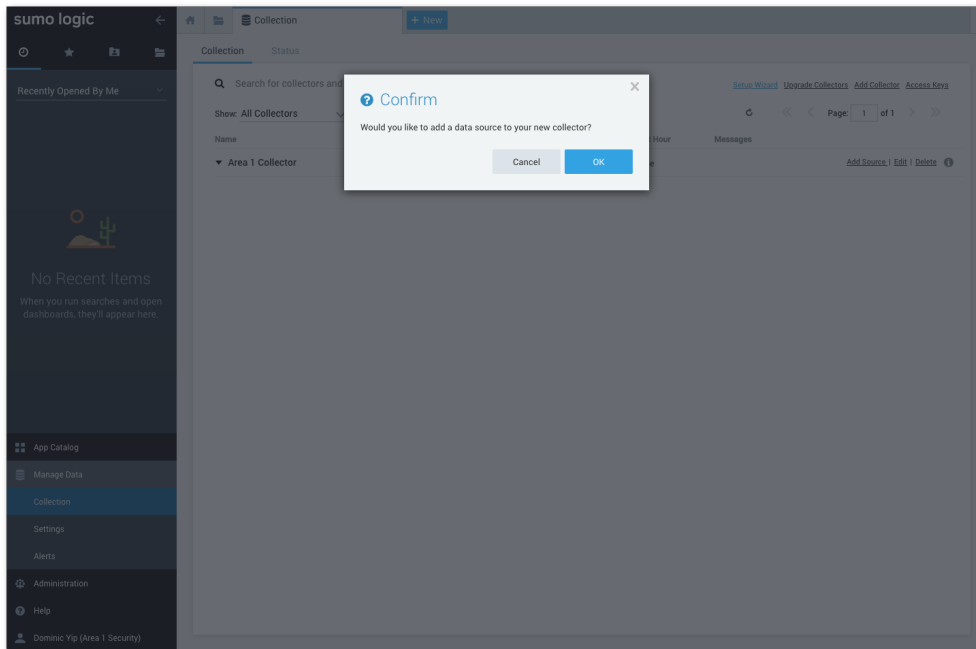
Select **Hosted Collector** as the collector type to start the configuration:



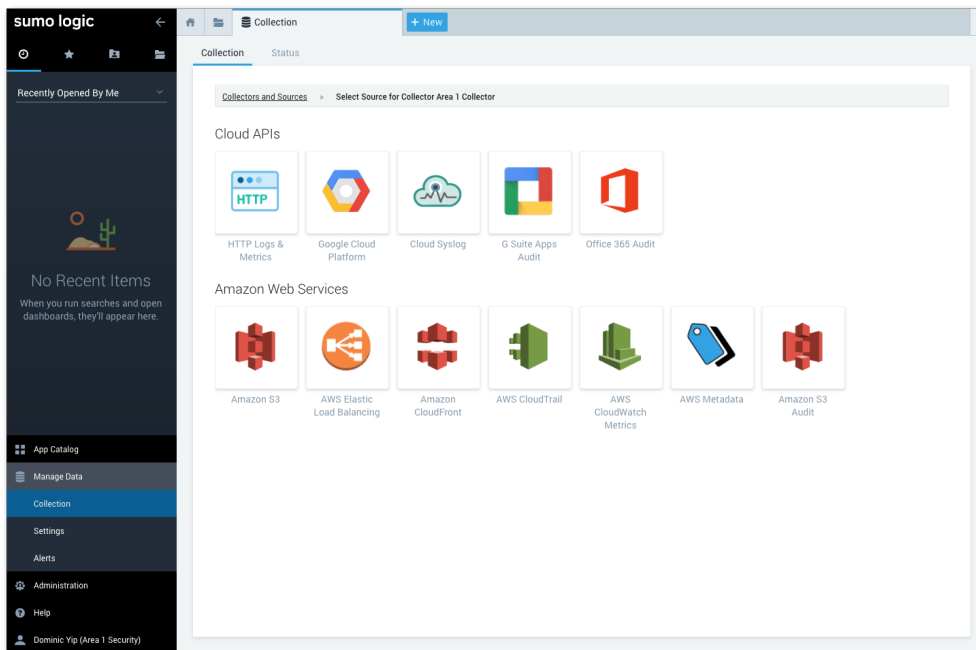
Enter the appropriate details to the Collector configuration. Click **Save** to save the configuration:



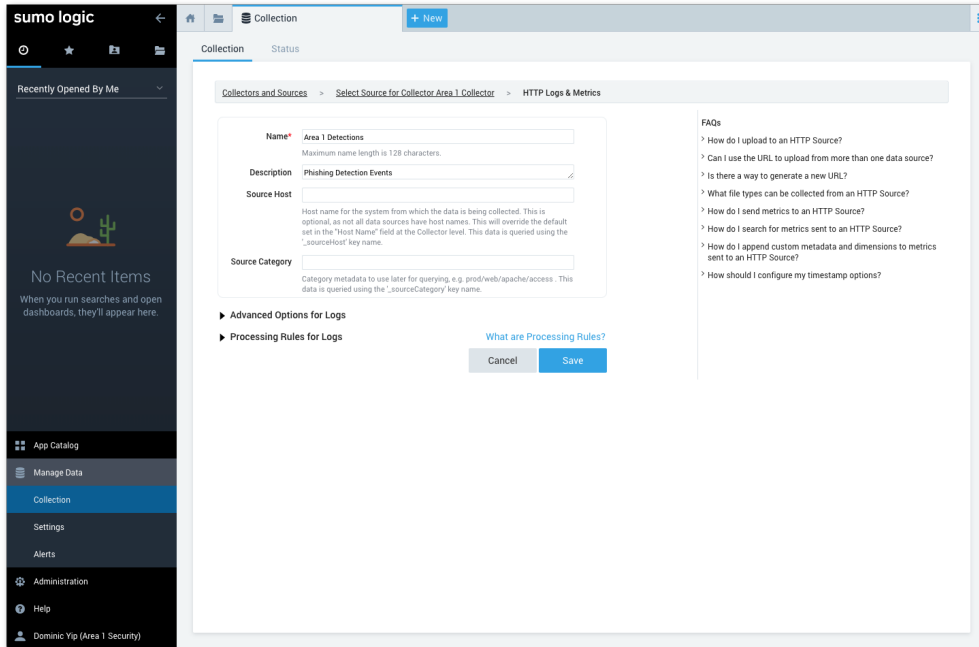
Click **OK** to confirm the addition of the new Collector in the confirmation dialog:



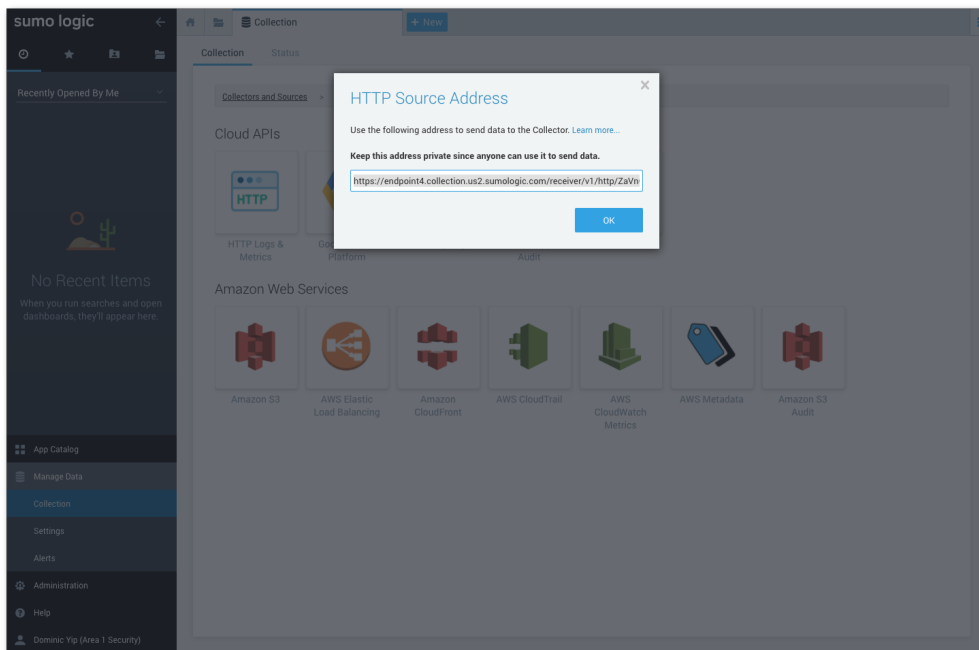
In the following dialog, under the **Cloud APIs** section, click the **HTTP Logs and Metrics** icon to start the configuration of the data source:



Configure the input with the appropriate details and click **Save** to save the configuration:




The following dialog will provide you with the HTTP Endpoint required for the Area 1 configuration:

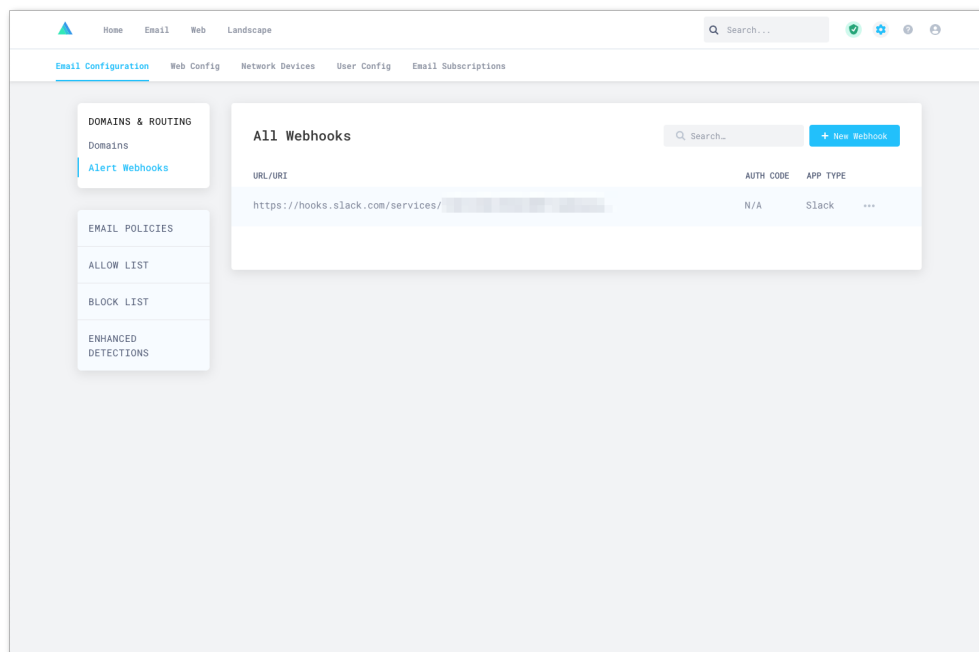


# Configure Area 1 to push the Email Detection Events to the Sumologic HTTP Collector

Login to the Area 1 Configuration portal (<https://horizon.area1security.com>) and navigate to the

**Alert Webhooks** configuration section (located under the configuration  icon >> Email Configuration >> Alert Webhooks)

Click the **New Webhook** button, located in the top right corner, to configure the Sumologic HTTP Collector:

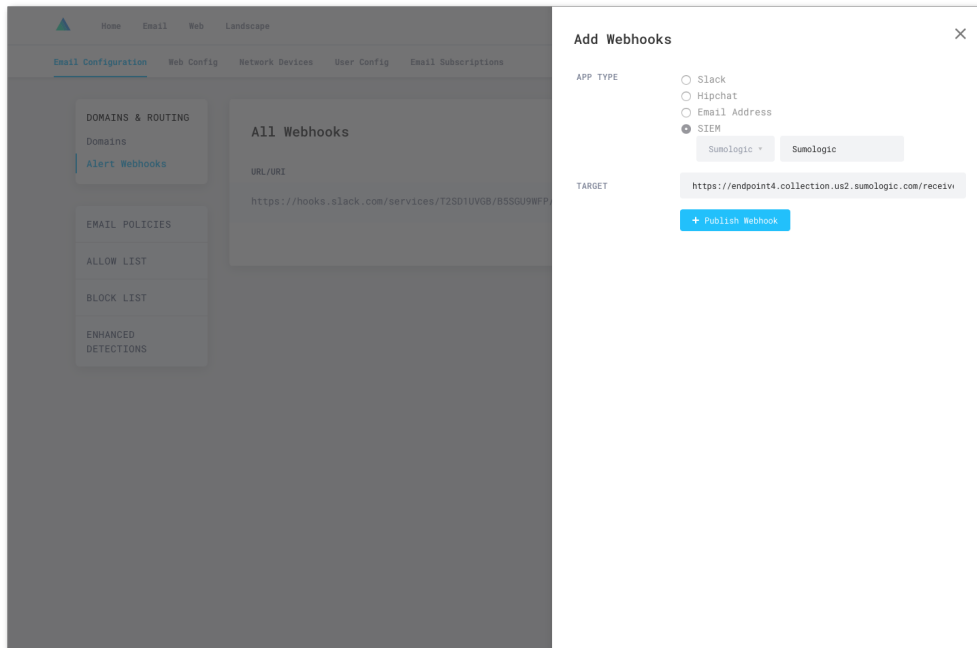


Configure the Webhook with the appropriate details

Select **SIEM >> Sumologic**

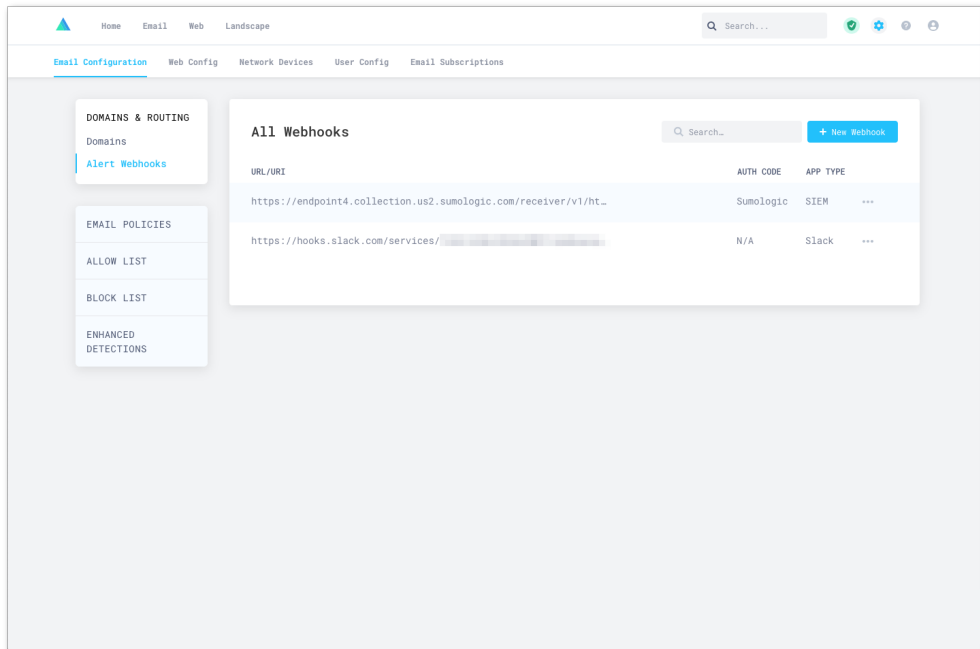
Enter the string **Sumologic** in the **Auth Code** field

Enter the Target URI of the Sumologic Collector (generated above)

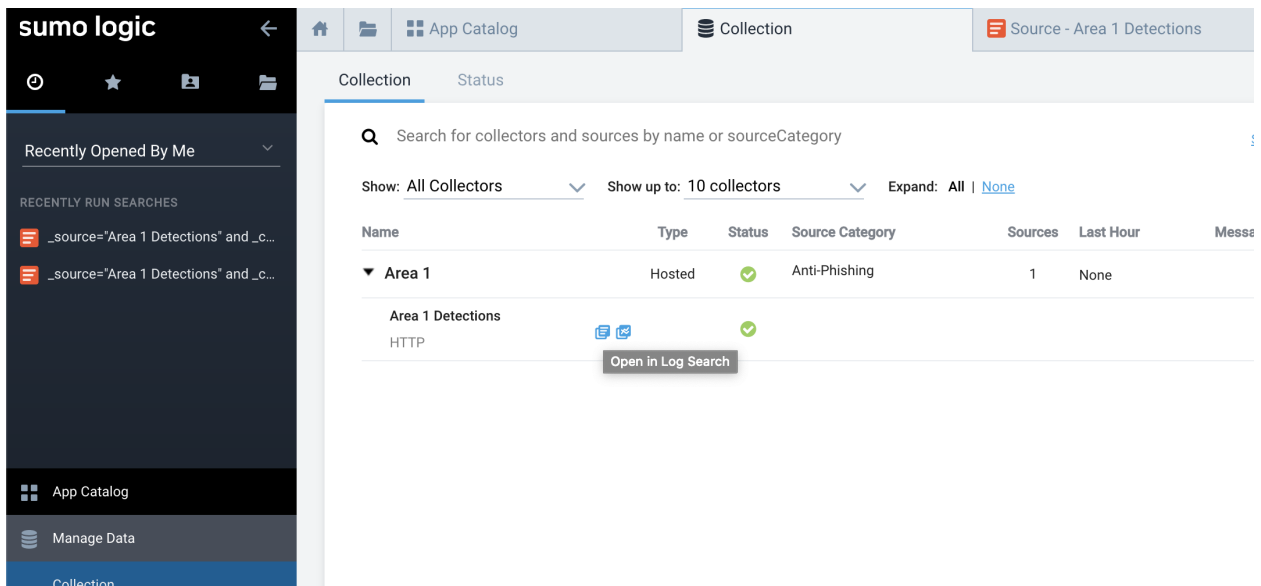




The Sumologic integration will now show up in the **All Webhooks** panel



**Note:** It will take about 10 minutes or so for the configuration to fully propagate through Area 1's infrastructure and for events to start to appear in your searches. Once the configuration is propagated, event will start to appear in your instance of Sumologic. To view logs, simply hover your mouse over the Area 1 Collector and click *Open in Log Search*:



Once events start to flow, you will be able to search for the detection events:

