Configuring Splunk Cloud HTTP Event Collector

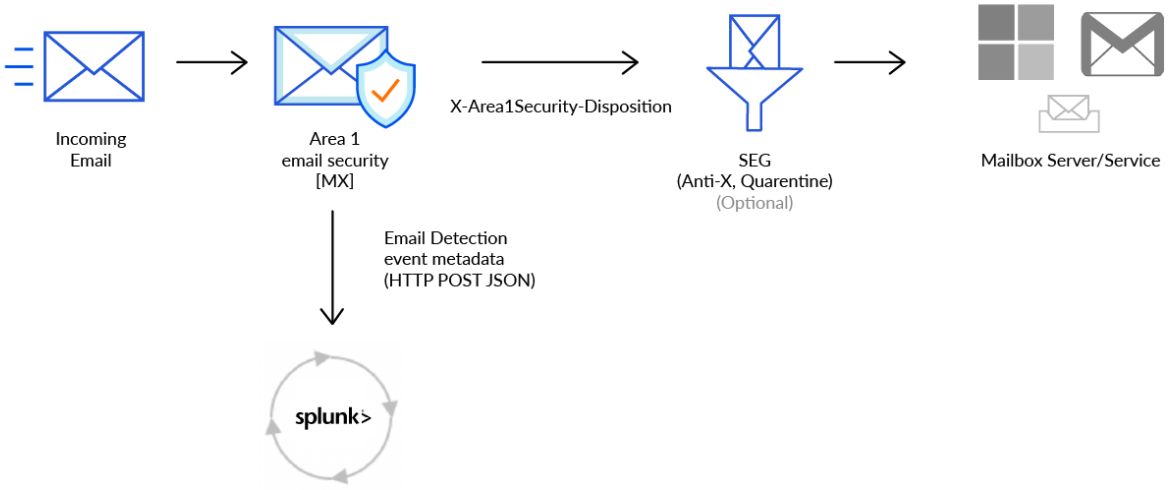
Cloudflare Area 1 Overview

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, Area 1 email security 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 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.

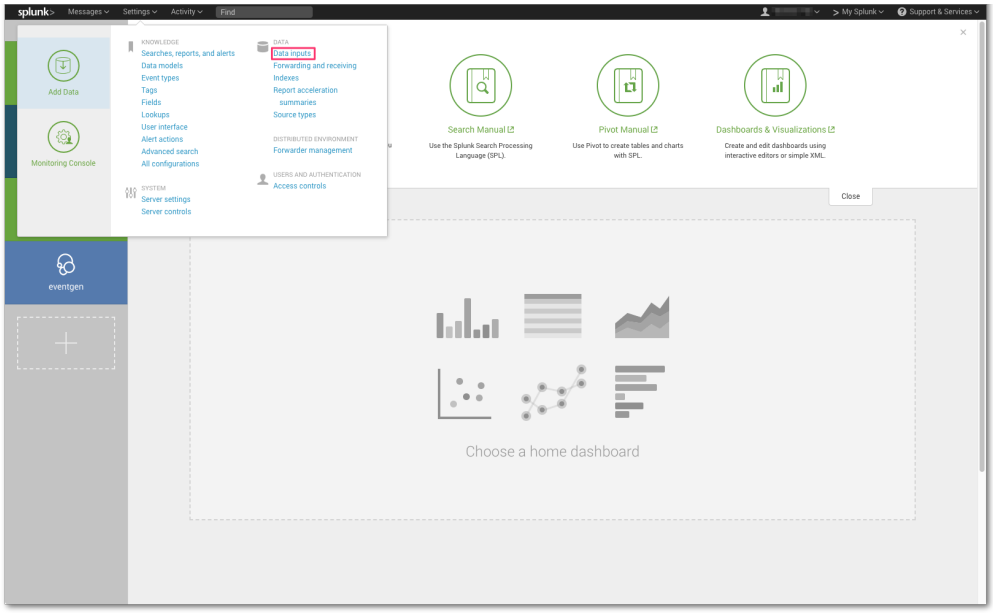
Area 1 Email Protection

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

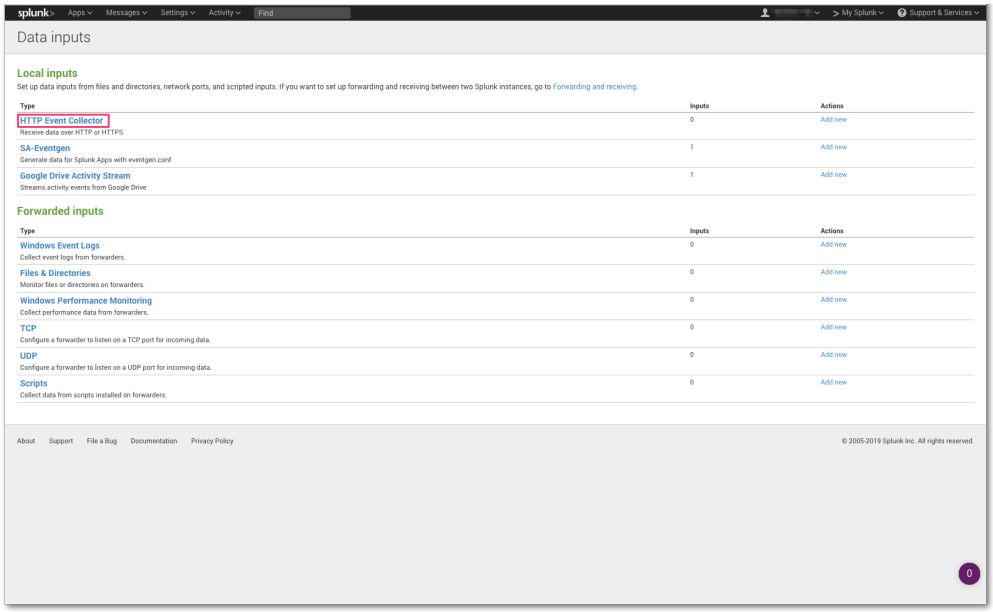


Configure the Splunk HTTP Event Collector

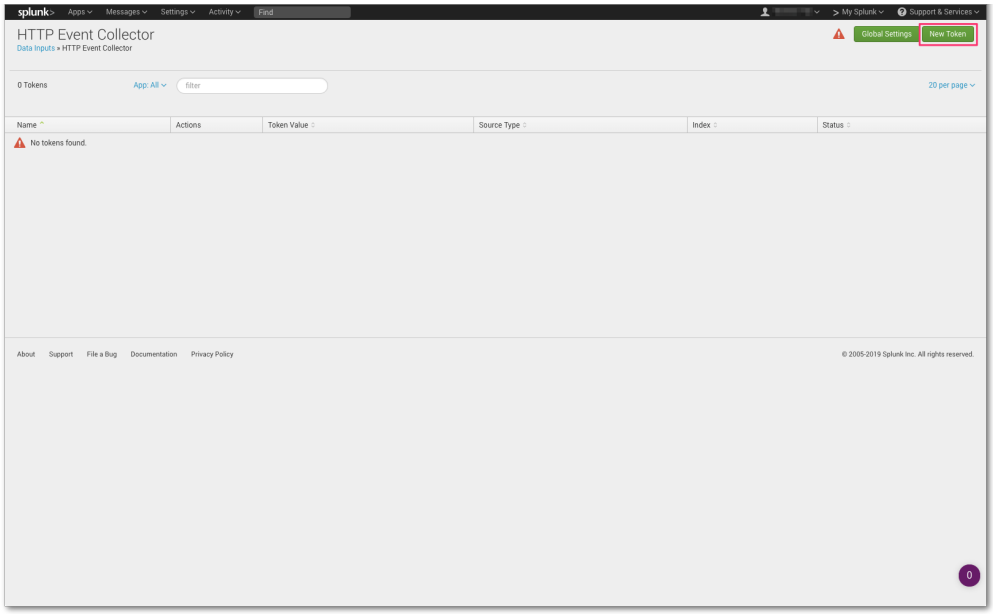
Log into Splunk as an administrator and go to **Settings >> Data inputs**, to configure the data inputs.



Click on the **HTTP Event Collector** type to access this configuration to create a new collector

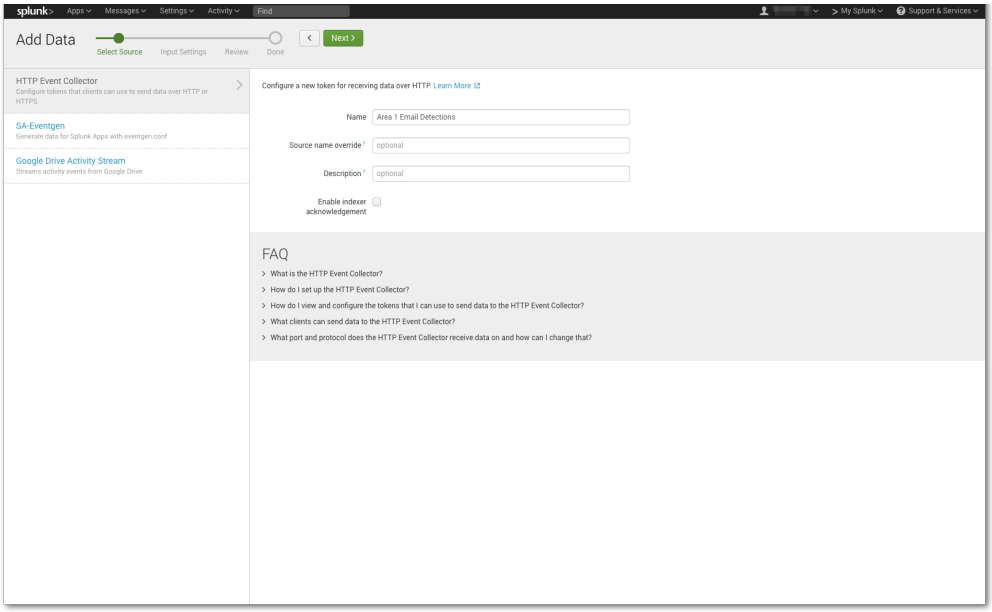


Click the **New Token** button to start the configuration

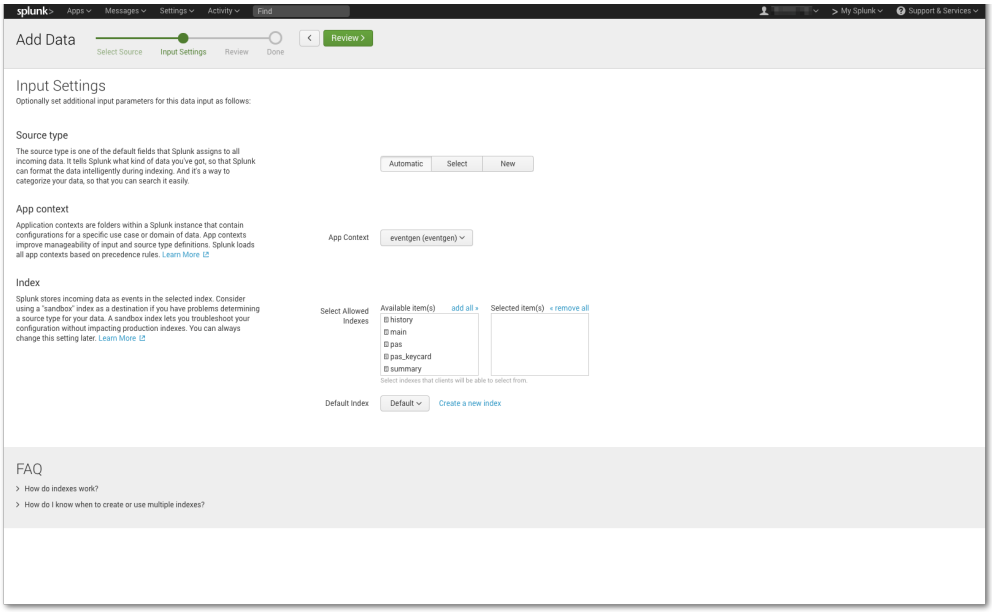


Provide a name for the Area 1 Token (e.g: Area 1 Email Detections)

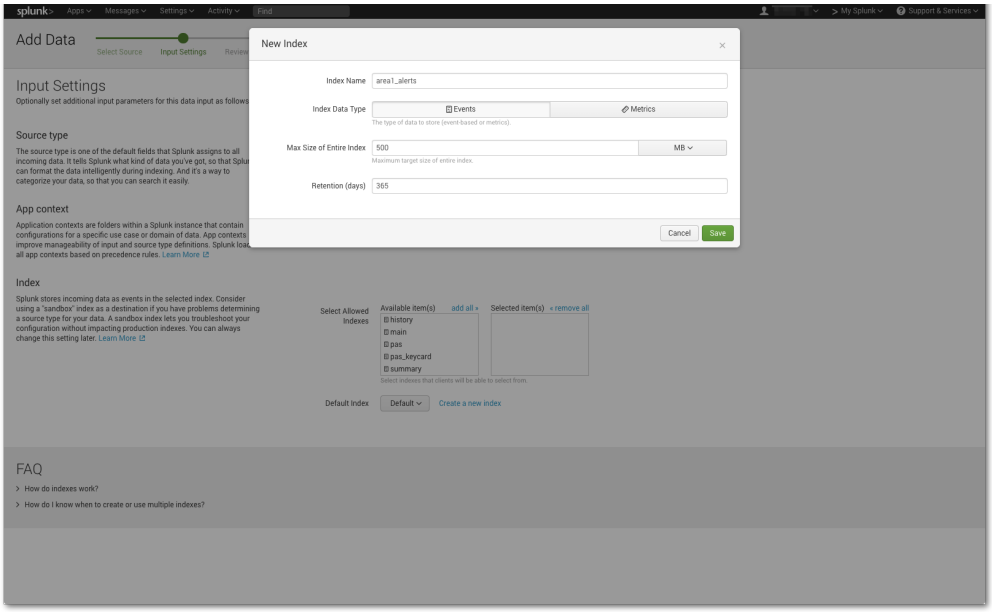
Leave the "Enable indexer acknowledgement" unchecked
Click **Next** to continue



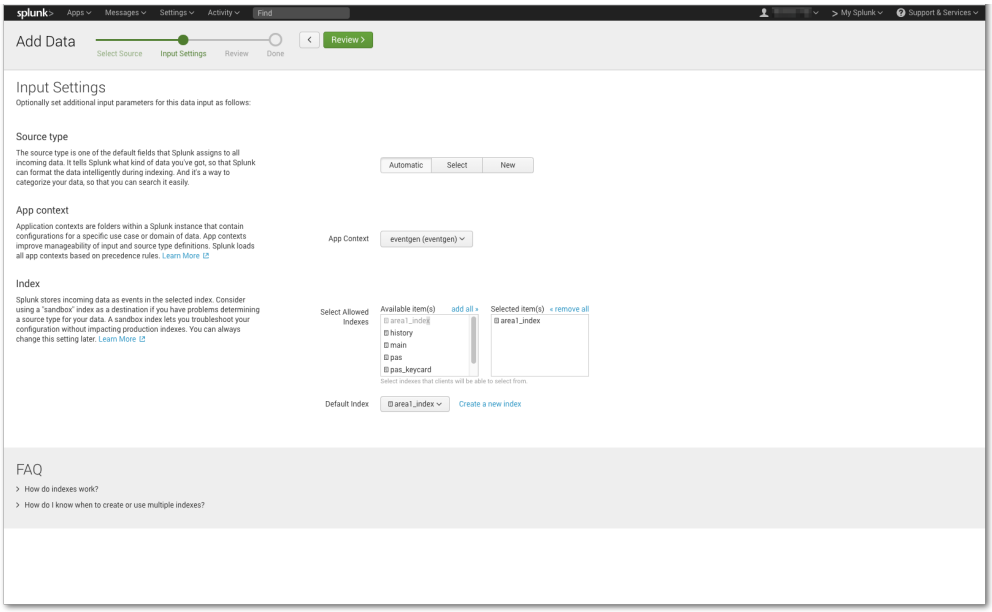
Configure the Input Settings for the HTTP Event Collector based on your environment.



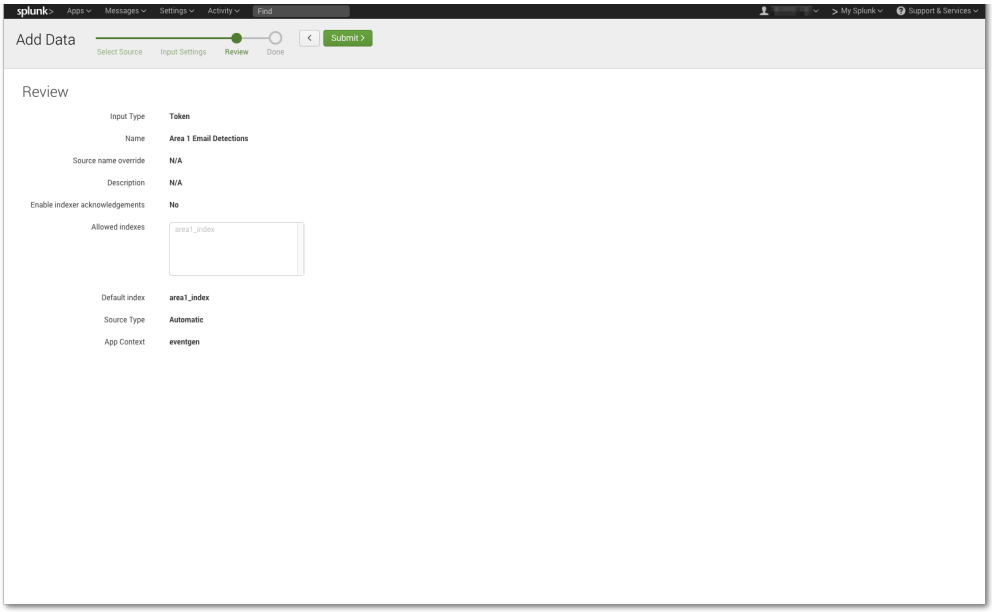
You may also create a new index for the Area 1 events with the **Max Size** and **Retention days** that fits your environment.



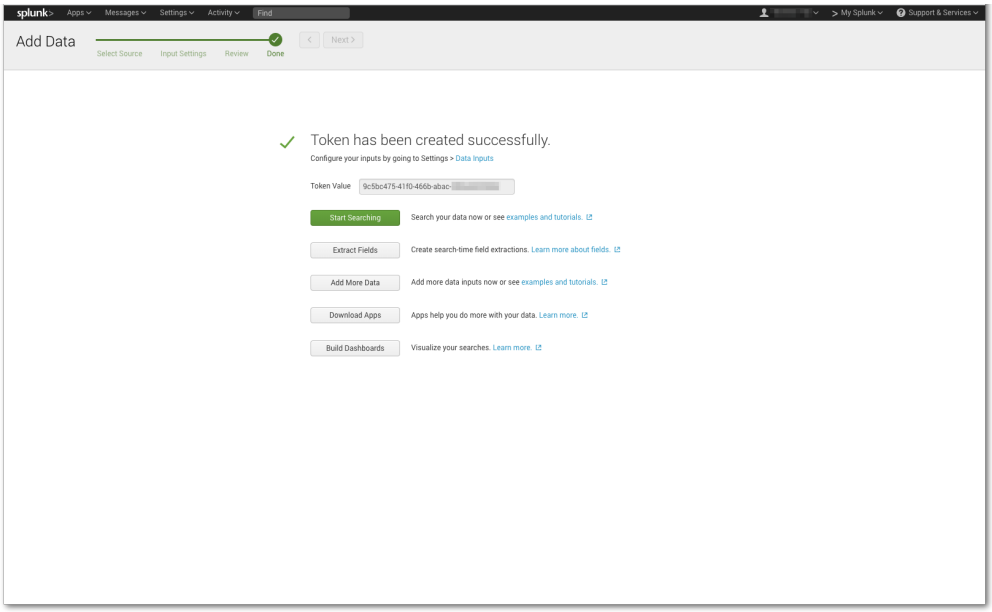
Add the newly created “area1_index” index to the configuration. Click **Review**.



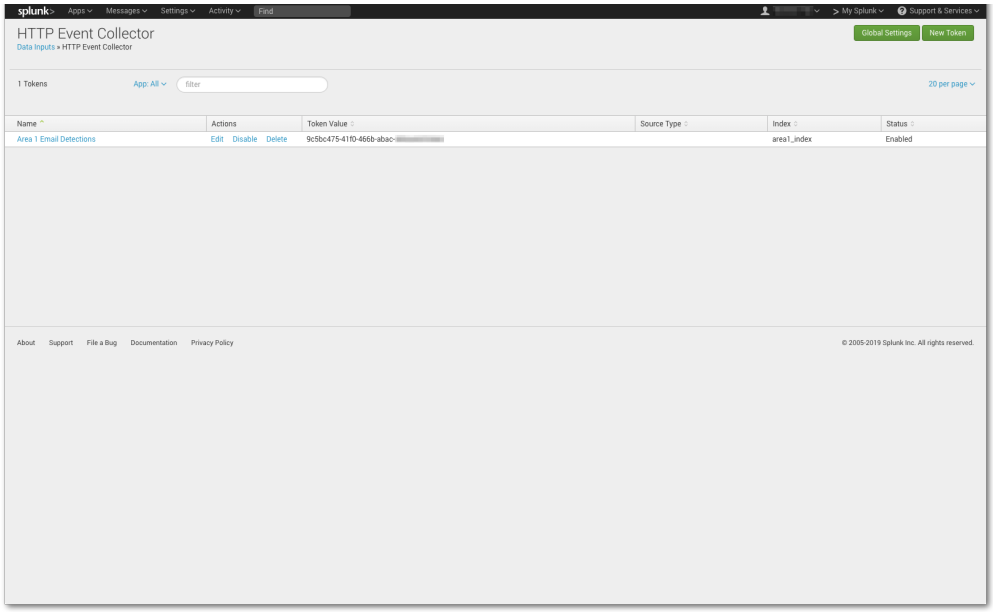
After reviewing and confirming the settings, click **Submit** to create the Collector



Note of the **Token Value**, this value is required for the Area 1 configuration in the next step.



The token can also be retrieved from the HTTP Event Collector configuration panel



To test your the HTTP Event Collector, you can manually inject an event into Splunk by using the curl:

$ curl https://<host>:8088/services/collector/event -H 'Authorization: Splunk <token>' -d '{"sourcetype": "mysourcetype", "event":"Hello, World!"}'

Note: When creating requests to Splunk, the url and port number changes as per the type of Splunk setup. Please see below:

Splunk Cloud Platform free trials:

<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>

Splunk Cloud Platform is as follows:

<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>

Splunk Enterprise is as follows:

<protocol>://<host>:<port>/<endpoint>

Port Numbers:
8088 on Splunk Cloud Platform free trials
443 by default on Splunk Cloud Platform instances
8088 on Splunk Enterprise

Please refer to the Splunk documentation for more information:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/UsetheHTTPEventCollector

Note: If your instance is on-premises, specify the appropriate hostname and ensure that your firewall allows the configured port through to your instance. The connections will be coming from the following egress IP addresses, if you need them for your ACLs:

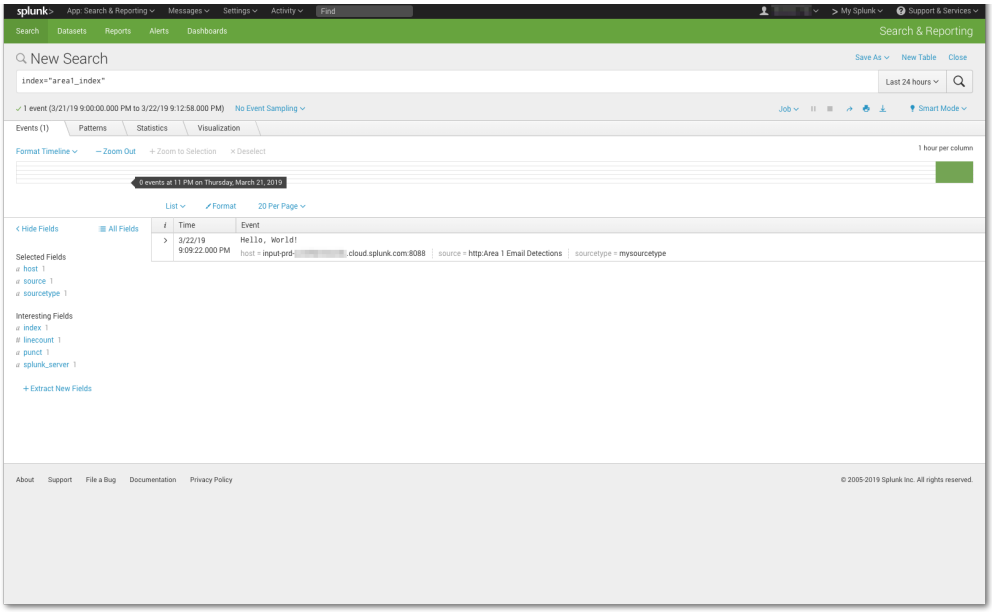
- 52.11.209.211
- 52.89.255.11
- 52.0.67.109
- 54.173.50.115

Note: Ensure that a valid SSL certificate is configured on your instance - the certificate cannot be expired and cannot be a self-signed certificate.

If all the requirements are met, you will receive the following response back to the curl command

{"text":"Success","code":0}

Additionally, you can search your instance of Splunk for the test event using the index or other search criteria (e.g. index=”area1_index”):

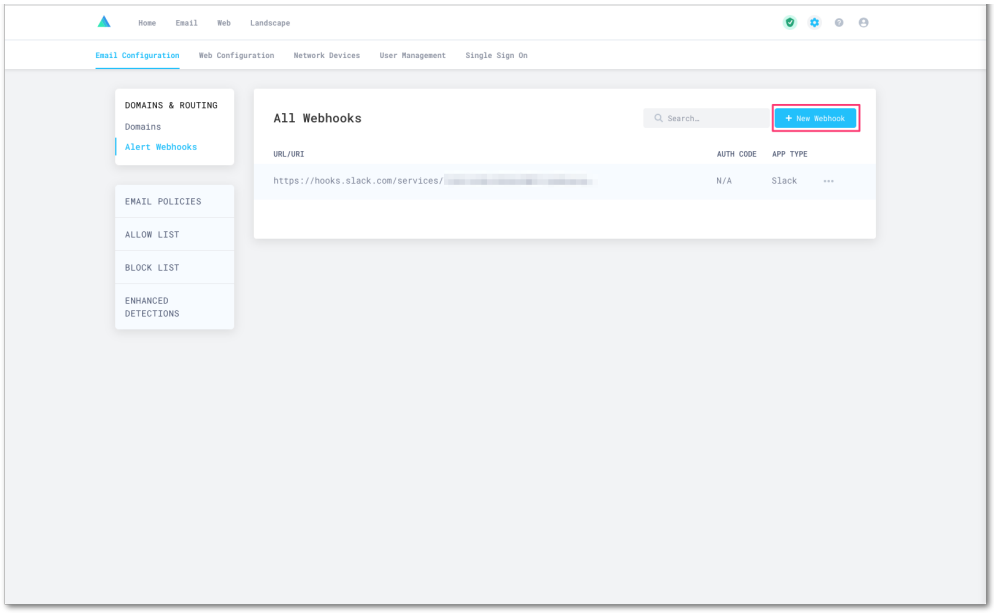


Configure Area 1 to push the Email Detection Event to the Splunk HTTP Event Collector

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

Alert Webhooks configuration section (Under configuration icon >> Email Configuration >> Alert Webhooks)

Click the **New Webhook** button to configure the Splunk HTTP Event Collector



Configure the Webhook with the appropriate details

Select SIEM >> Splunk
Enter the Splunk token for your HTTP Event Collector
Enter the Target URI of our Splunk instance

Note: The Target URI will typically have the following format
https://<host>:8088/services/collector

Note: When creating requests to Splunk Cloud, you must add a prefix to the URI of the hostname according to your subscription.

Note: When creating requests to Splunk, the url and port number changes as per the type of Splunk setup. Please see below:

Splunk Cloud Platform free trials:

<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>

Splunk Cloud Platform is as follows:

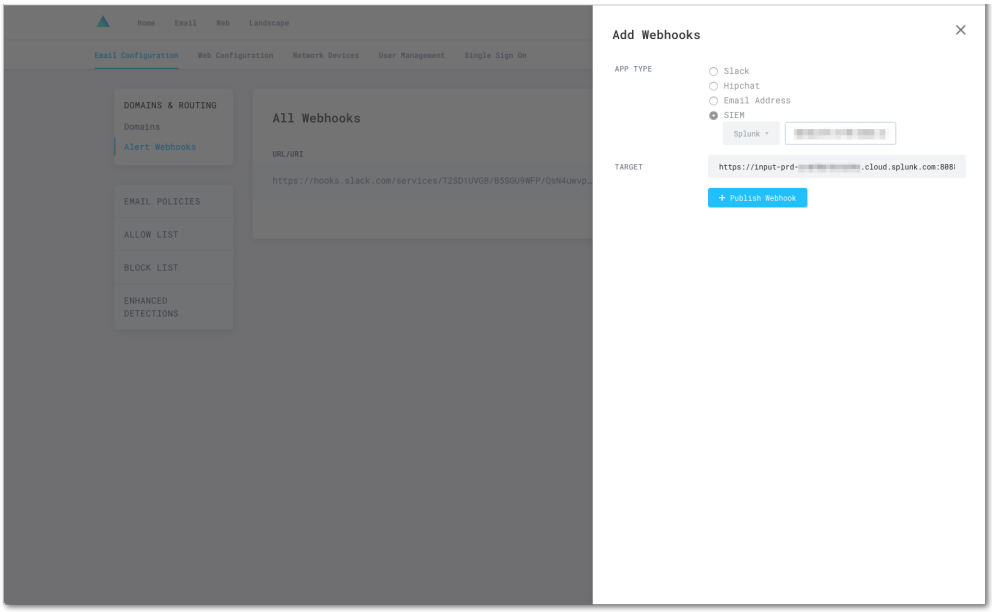
<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>

Splunk Enterprise is as follows:

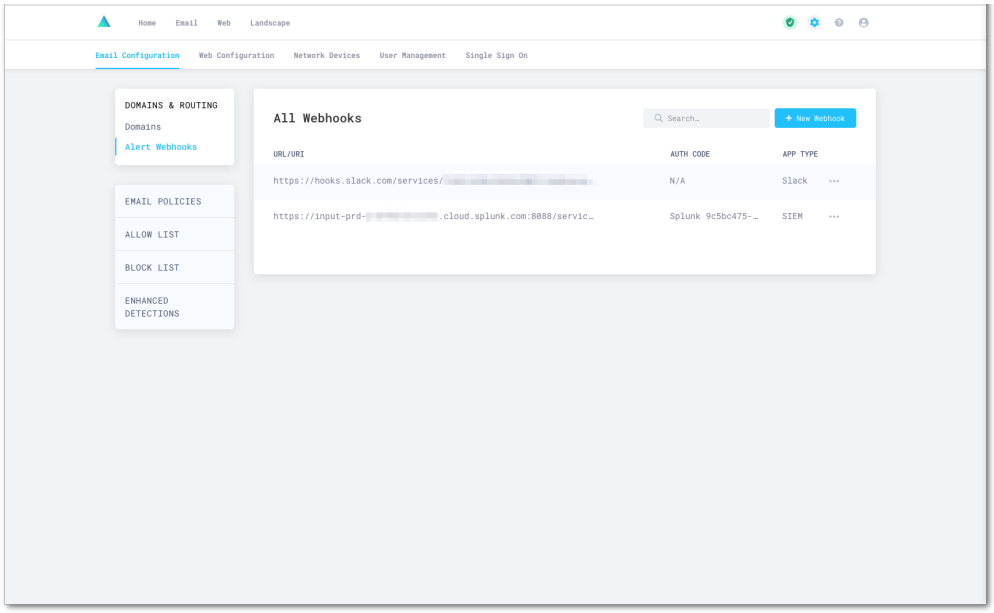
<protocol>://<host>:<port>/<endpoint>

Port Numbers:
8088 on Splunk Cloud Platform free trials
443 by default on Splunk Cloud Platform instances
8088 on Splunk Enterprise

Please refer to the Splunk documentation for more information:
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/UsetheHTTPEventCollector


Home
Email
Web
Landscape
Email Configuration
Web Configuration
Network Devices
User Management
Single Sign On
DOMAINS & ROUTING
Domains
Alert Webhooks
EMAIL POLICIES
ALLOW LIST
BLOCK LIST
ENHANCED DETECTIONS
All Webhooks
URL/URI
Add Webhooks
APP TYPE
Slack
Hipchat
Email Address
SIEM
Splunk
TARGET
+ Publish Webhook

The Splunk integration will now show up in the **All Webhook** panel



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 Splunk.

Installing the Area 1 Splunk App

To install the Area 1 Splunk App, access the app by going to: https://splunkbase.splunk.com/app/4329/ or by installing the app through Splunk App Manager