

# **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:

sumo logic 🛛 🗧 🧑	f 🖹 Collection + New
⊙ ★ 🖻 🖴	Collection Status
Recently Opened By Me 🛛 👻	Q     Search for collectors and sources by name or sourceCategory     Betwee Waters' Upprade Categors' Add
No Recent Items When you run searches and open dasbboards, they'll appear here.	No Collectors found. Make sure you activate your installed Collectors.
App Catalog	
Collection	
Settings	
Alerts	
Administration	
Help	
(dom@area1security.com)	

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

sumo logic $\leftarrow$	n 🖿 🗧 Collection + New E
o * E E	Collection Status
Recently Opened By Me 🔍 🔍 Vecently Opened By Me Vecently Opened By Me Vecently Opened By Me Vecently Opened Astronomy Opened By Me Vecently Opened Astronomy	A since Since Nation Nation Select Collector Type Installed Collector Installed Collector Installed Collector Installed Collector Installed Collector Installed Collector Installed Collector Betto set ups a Collector Installed Collector Betto set ups a Collector Installed Collector Inst
App Catalog	
Collection	
Settings	
Alerts	
Administration	
😧 Help	
Dominic Yip (Area 1 Security)	

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

sumo logic $\leftarrow$ 🖨 🖀 Scollection	+ New		1
O ★ E ► Collection Status			
Recently Opened By Me	sted Collector	×	C C Page: 1 of 1 > >
Name *	Area 1 Collector		ages
No Collecto: Description	Area 1 Security Collectors		
Category	Anti-Phishing		
e e e e e e e e e e e e e e e e e e e	Unless overwritten by Source metadata, the Collector will set the Source category of all messages to this value.		
No Recent Items	(UTC) Etc/UTC	•	
When you run searches and open dashboards, they'll appear here.	Unities overwritten by source time zool, the collector was set the source time zool or all messages to this value.		
App Catalog			
Collection			
Settings			
Alerts			
4 Administration			
🚱 Help			
L Dominic Yip (Area 1 Security)			

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:

sumo logic ( # 😂 Scollection	+ New	
O 🛧 🖪 🔚 Collection Status	ŝ	
Recently Opened By Me   Collectors and Source	ces > Select Source for Collector Area 1 Collector > HTTP Logs &	Metrics
Name*	Area 1 Detections	FAQs How do Lunipad to an HTTP Source?
	Maximum name length is 128 characters.	Can I use the URL to upload from more than one data source?
Description	Phishing Detection Events	Is there a way to generate a new URL?
Source Host		> What file types can be collected from an HTTP Source?
Ο	Host name for the system from which the data is being collected. This is	How do I send metrics to an HTTP Source?
<b>→</b> <sup>₩</sup>	set in the "Host Name" field at the Collector level. This was override the denaut set in the "Host Name" field at the Collector level. This data is queried using the "accurate of the the set of the	How do I search for metrics sent to an HTTP Source?
Saura Catagory	_sourceriost key name.	How do I append custom metadata and dimensions to metrics sent to an HTTP Source?
No Recent Items	Category metadata to use later for querying, e.g. prod/web/apache/access. Thi data is ouvried using the ' sourceCategory' key name.	> How should I configure my timestamp options?
When you run searches and open		
dashboards, they'll appear nere. Advanced Optio	ins for Logs	
Processing Rule	es for Logs What are Processin	g Rules?
	Cancel S	ive
App Catalog		
😂 Manage Data		
Collection		
Settings		
Alerts		
Administration		
1 Help		
Dominic Yip (Area 1 Security)		

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 (<u>https://horizon.area1security.com</u>) and navigate to the

**Alert Webhooks** configuration section (located under the configuration <sup>(2)</sup> icon >> Email Configuration >> Alert Webhooks)

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

	All Webhooks	Q Search	+ New Webhook
Alert Webhooks	URL/URI	AUTH CODE	APP TYPE
	https://hooks.slack.com/services/	N/A	Slack
EMAIL POLICIES			
ALLOW LIST			
BLOCK LIST			
ENHANCED DETECTIONS			

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)

Home Email Web	Landscape	Add Webhooks	×
Email Configuration Web Confi	g Network Devices User Config Email Subscriptions	APP TYPE	○ Slack ○ Hipchat
DOMAINS & ROUTING Domains	All Webhooks		<pre>O Email Address SIEM Sumologic * Sumologic</pre>
	URL/URI https://hooks.slack.com/services/T2SD1UVGB/B5SGU9WFP	TARGET	https://endpoint4.collection.us2.sumologic.com/receiv
EMAIL POLICIES			+ Publish Webhook
BLOCK LIST			

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

Domains & ROUTING	All Webhooks	Q Search	+ New Webhook	
Alert Webhooks	URL/URI	AUTH CODE	APP TYPE	
	https://endpoint4.collection.us2.sumologic.com/receiver/v1/ht_	Sumologic	SIEM	
ALLOW LIST	https://hooks.slack.com/services/	N/A	Slack	
BLOCK LIST				
ENHANCED DETECTIONS				

**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*:

sumo logic $\leftarrow$	A Second		n	🗐 Source - Area 1 Detecti	ons
0 ★ 🖻 🖿	Collection Status				
Recently Opened By Me	<b>Q</b> Search for collector	s and sources by name or source(	Category		5
RECENTLY RUN SEARCHES	Show: All Collectors	Show up to: 10 collectors	Expand: All	None	
_source="Area 1 Detections" and _c	Name	Type Status	Source Category	Sources Last Hour	Messa
_source="Area 1 Detections" and _c	▼ Area 1	Hosted 🣀	Anti-Phishing	1 None	
	Area 1 Detections	🗐 🗹 🔗			
App Catalog					
🛢 Manage Data					
Collection					

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

sumo logic	🚓 🔚 🗐 Unnamed	1	+ New			:
⊘ ★ 🖪 🖕	✓ _collector="Area 1     ☆   Save As   Info   Shar	Coll e   Pi	r" Jive Tail		Last 24 Hours	Start
RECENTLY RUN SEARCHES	05/28/2019 9:39:47 AM -0700 8 6 4 2 12:00 05/28/2019 9:39:47 AM -0700	PM	3.00 PM 6.00 PM 9.00 P	4 12.00 AM	3.00 AM	05/29/2019 9:39:47 AM-0700 Hide 8 4 2 6:00 AM 05/29/2019 9:39:47 AM-0700
	<ul> <li>Display Fields</li> <li>Display Fields</li> <li>Message a</li> <li>Hidden Fields</li> <li>Collector a</li> <li>Stare a</li> <li>Source a</li> <li>Source Category a</li> <li>Source Hoat a</li> <li>Source Hame a</li> </ul>	E)	Image         Image         Image           Time         Message         LogReduce         Log           05/20/2019         View as Rawe         Sourcetyse: "mailstreamset016.producting sourcetyse: "mailstream", tame 1597185784, tame 1597182792, tame 159718279, tame 1597182792, tame 159718279, tame 1597182792, tame 1597182792	gCompare v in.ares1.internal*, Ditopory Anti-Phabing  Ditopory Anti-Phabing  Cotopory Anti-Phabing		Eppand JSON O
App Catalog     Manage Data     Administration     Help     Dominic Vip (Area 1 Security)			013058.000-0700 {     hot: "militreamest002.product!     bot: "militreamest002.product!     bot: "militreamest002.product!     bot: "arailsecurity",     event: +(_)     Hest: 0.110.0211_Viane.Http:hpud. {         for the same             223411300-0700 {	n,areal.internal", Dategory AntiPhishing ∽ on,areal.internal",		