Team Cymru Scout App For Splunk - User Guide

Table of contents

Introduction

- Team Cymru Scout Platform is used to get information about Domains and IP addresses for initial threat investigations, to quickly triage and respond to incidents using rich data from Team Cymru's Pure Signal, to analyze and understand potential risks on their organization.

Compatibility Matrix

Splunk Enterprise Version	9.2.x , 9.1.x , 9.0.x
Supported OS Version	Independent
Browser	Independent
Python Version	Python3

System Requirement

The basic system requirements for the Team Cymru Scout App For Splunk are the same as the basic requirements of Splunk deployment. Please refer to this (Reference) to find the hardware and software details.

Installation of Team Cymru Scout App For Splunk User Guide

Team Cymru Scout App For Splunk can be installed through the UI as shown below or extract the zip file directly into the $SPLUNK_HOME/etc/apps/ folder.

- Installation step from UI:

    1. Log in to Splunk and navigate to Apps > Manage Apps.
    2. Click Install app from the file.
    3. Click Choose file and select the TeamCymruScoutAppForSplunk App installation file.
    4. Click on Upload.
    5. Restart Splunk if prompted.

- Topologies according to the environment:

1. Standalone Mode

    - Install the Team Cymru Scout App For Splunk.

    - Configure an account and create modular input.

2. Distributed Environment

    - Install the Team Cymru Scout App For Splunk on the Search Head and OnPremise/IDM/UF/HF.

    - Configure an account and modular input on Forwarder.

    - Configure KV store-related settings on the Splunk KV Lookup Rest page on Forwarder only.

    - Configure correlation-related settings on the Correlation Settings page on Search Head only.

3. Cloud Environment

    - Users need to raise a ticket to the Splunk support team for the App installation Or users can install the app from the Manage Apps page.

Prerequisites

- Splunk Common Information Model (CIM data models) (To match the indicators with the data model events)(https://splunkbase.splunk.com/app/1621).

- Before configuring this App, User must have the following information from User Team Cymru Scout instance:

    - Team Cymru Scout Username, Team Cymru Scout Password or Team Cymru Scout Account API Key

Configuration for Team Cymru Scout App

Configure Account

Team Cymru Scout App supports 2 types of authentication, so users can add accounts with 2 types of authentication.

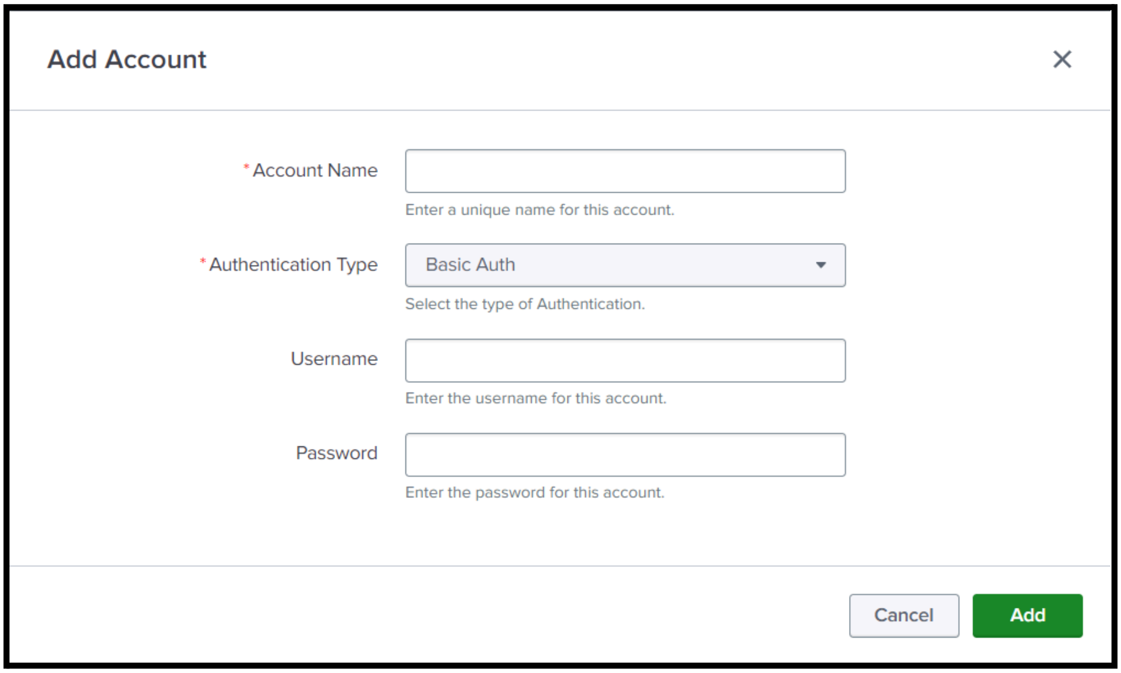
- Basic Auth
- API Key

To Configure the Team Cymru Scout details, please follow the below steps:

Configure Account by Basic Auth

1. Go to Team Cymru Scout App For Splunk > Configuration
2. Click Add from the top right corner.
3. Add a unique Account Name, Authentication Type as Basic Auth, Username and Password.
4. Click on the Add button.

● Once The Account is added. The list of all the added Accounts is visible on the Configurations page.



Add Account

* Account Name

Enter a unique name for this account.

* Authentication Type: Basic Auth

Select the type of Authentication.

Username

Enter the username for this account.

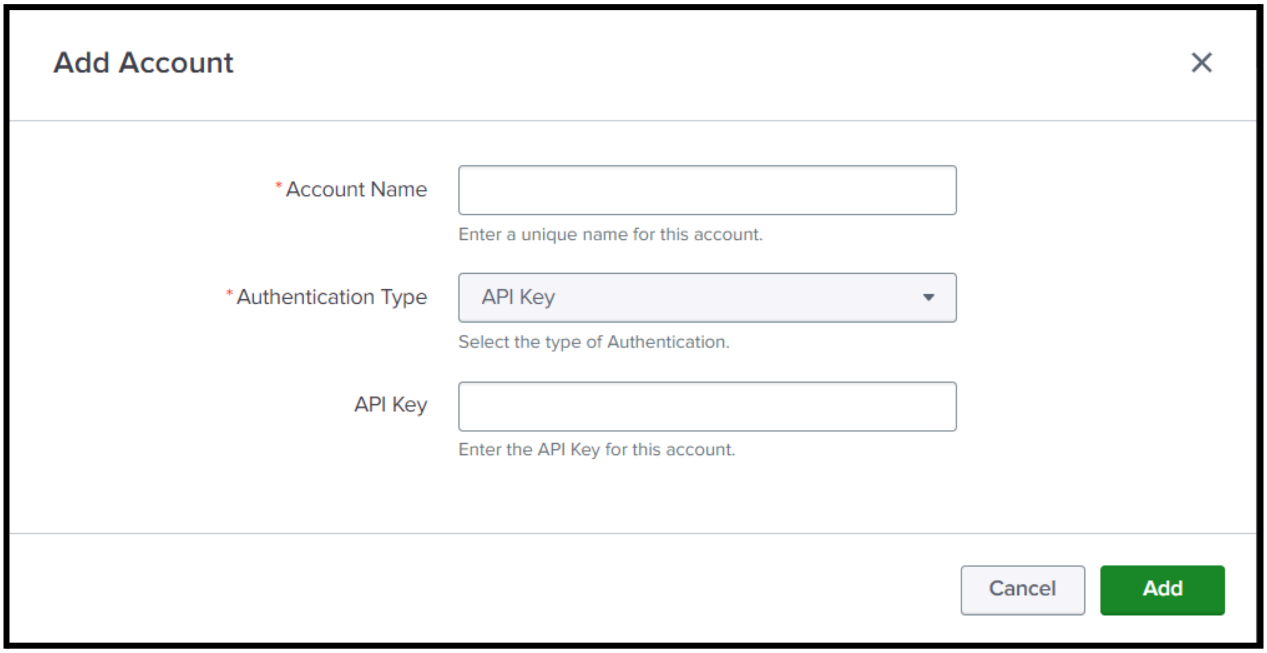
Password

Enter the password for this account.

Configure Account by API Key

1. Go to Team Cymru Scout App For Splunk > Configuration
2. Click Add from the top right corner.
3. Add a unique Account Name, and Authentication Type as API Key and enter API Key
4. Click on the Add button.

● Once The Account is added. The list of all the added Accounts is visible on the Configurations page.



Add Account

*Account Name

Enter a unique name for this account.

*Authentication Type: API Key

Select the type of Authentication.

API Key

Enter the API Key for this account.

To update an Account

1. Go to Team Cymru Scout App For Splunk > Configuration
2. Find the account User wants to Edit from the list of configured accounts.
3. Click on Action > Edit
4. Update the required parameters in the dialogue box.
5. Click on Update.

To clone an Account

1. Go to Team Cymru Scout App For Splunk > Configuration
2. Find the account User wants to Clone from the list of configured accounts.
3. Click on Action > Clone
4. Add the required parameters in the dialogue box.
5. Click on save.

To remove an Account

Note: Before removing the Account make sure none of the Input is using the account User wants to remove.

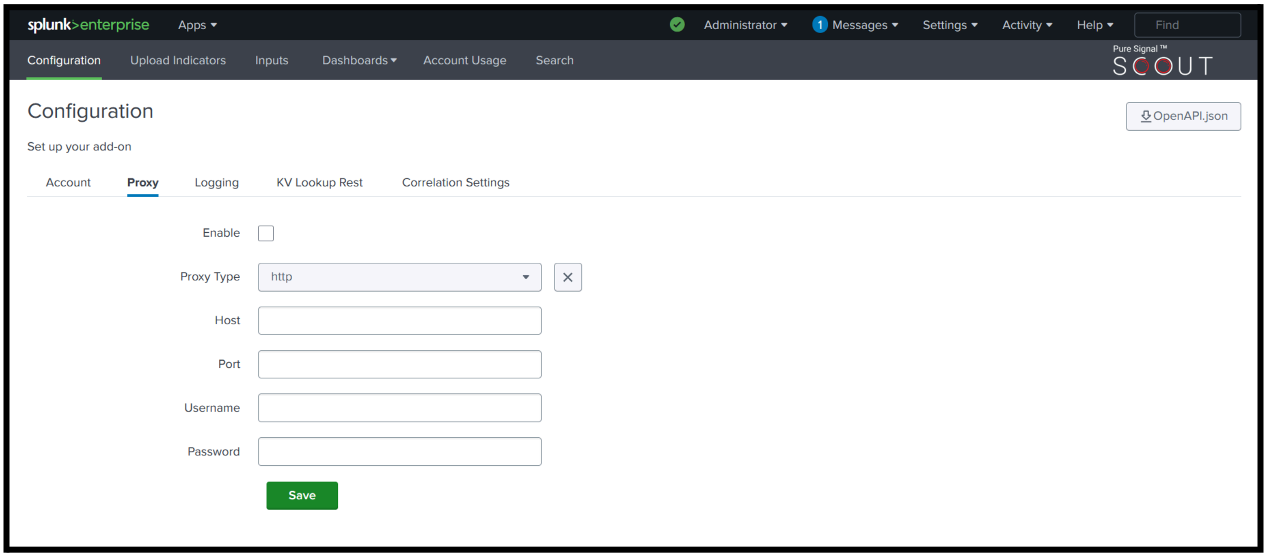
1. Go to Team Cymru Scout App For Splunk > Configuration
2. Find the account User wants to Delete from the list of configured accounts.

Click on Action > Delete.Proxy page

Note: It is mandatory to click on the Enable checkbox to use a proxy.

A user can configure the proxy for Team Cymru Scout App through this page. And supported proxy types are http and socks5.

1. Go to Team Cymru Scout App For Splunk > Configuration > Proxy.
2. Provide Proxy Type, Host, Port, Username and Password then click on Save button.



Configuration

Set up your add-on

Enable ☐

Proxy Type: http

Host:

Port:

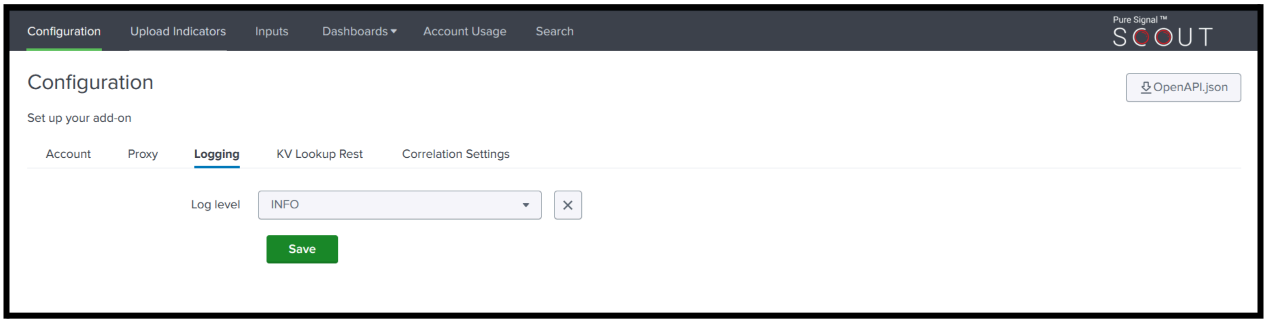
Username:

Password:

Logging Page

A user can configure the logging level for the Team Cymru Scout App through this page.

1. Go to Team Cymru Scout App For Splunk > Configuration > Logging.
2. Select the Log Level from the drop-down and Save it.



Configuration

Set up your add-on

Log level: INFO

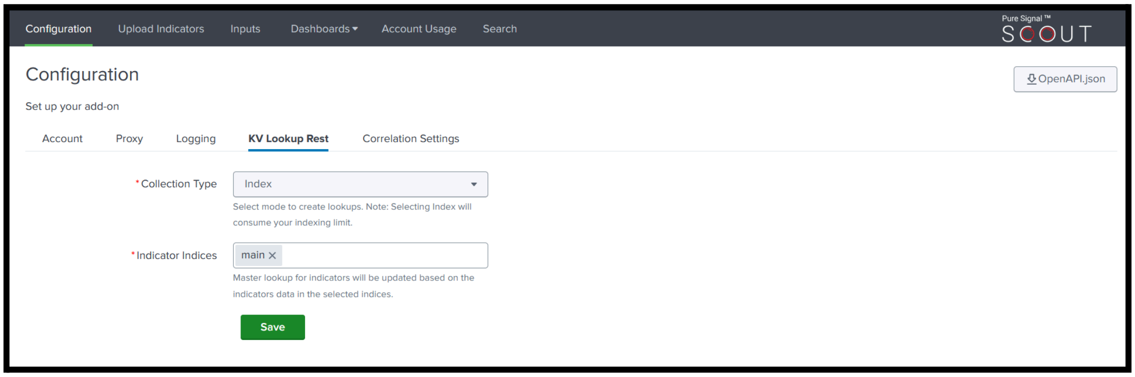
Splunk KV Lookup Rest

Users can configure Splunk KV Lookup Rest through 2 methods

- Collection type as index
- Collection type as lookup

To add Splunk KV Lookup Rest details by index

1. Go to Team Cymru Scout App For Splunk > Configuration > Splunk KVStore Creation
2. Enter the collection type as index and select indicator indices from the dropdown.
3. Then click Save.



Configuration

Set up your add-on

*Collection Type: Index

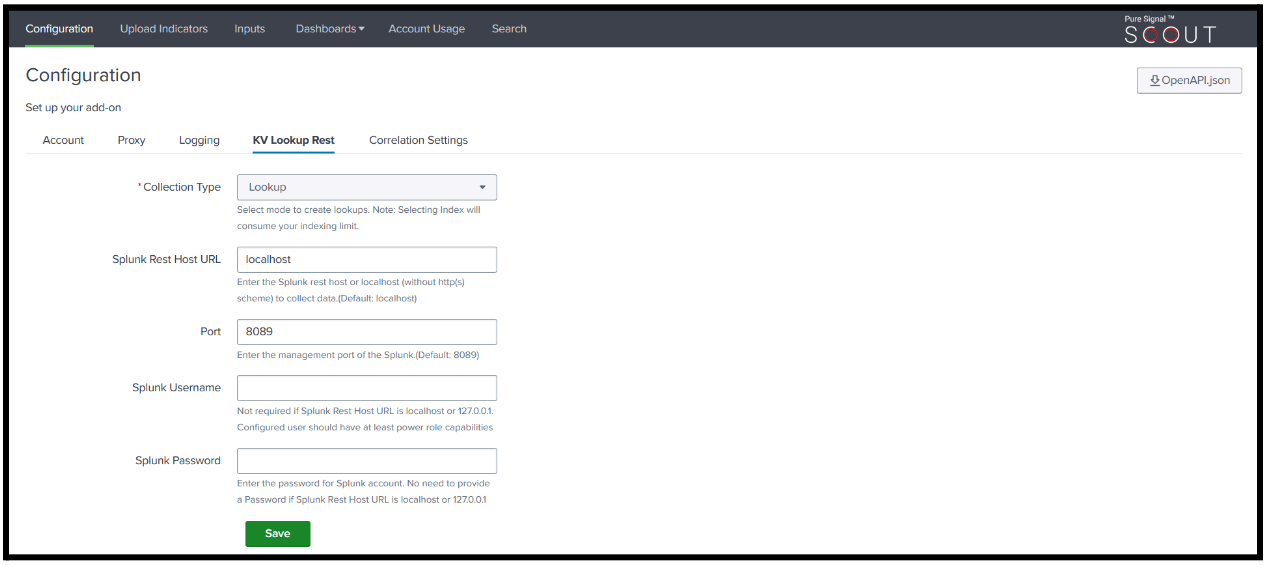
Select mode to create lookups. Note: Selecting Index will consume your indexing limit.

*Indicator Indices: main ×

Master lookup for indicators will be updated based on the indicators data in the selected indices.

To add Splunk KV Lookup Rest details by lookup

1. Go to Team Cymru Scout App For Splunk > Configuration > Splunk KVStore Creation
2. Enter collection type as index, Splunk Rest Host URL, Port, Splunk username and splunk password. Splunk Rest Host URL will be default as localhost and port as 8089.
3. Then click Save.



Configuration

Set up your add-on

*Collection Type: Lookup

Select mode to create lookups. Note: Selecting Index will consume your indexing limit.

Splunk Rest Host URL: localhost

Enter the Splunk rest host or localhost (without http(s) scheme) to collect data.(Default: localhost)

Port: 8089

Enter the management port of the Splunk.(Default: 8089)

Splunk Username:

Not required if Splunk Rest Host URL is localhost or 127.0.0.1. Configured user should have at least power role capabilities

Splunk Password:

Enter the password for Splunk account. No need to provide a Password if Splunk Rest Host URL is localhost or 127.0.0.1

NOTE:

● No need to configure anything in this tab if the app is present in localhost. Just make sure that the "Splunk Rest Host URL" field is by default set as "localhost" and the "Port" field is by default set as "8089".

● If using the Cluster environment then make sure that all fields are configured and splunkd port 8089 of Splunk Management is open for storing lookups.

To update a Splunk KV Lookup Rest details

1. Go to Team Cymru Scout App For Splunk > Configuration > Splunk KV Lookup Rest
2. Update the required parameters.
3. Click on Save.

Correlation Settings

User can use correlation setting by 2 methods

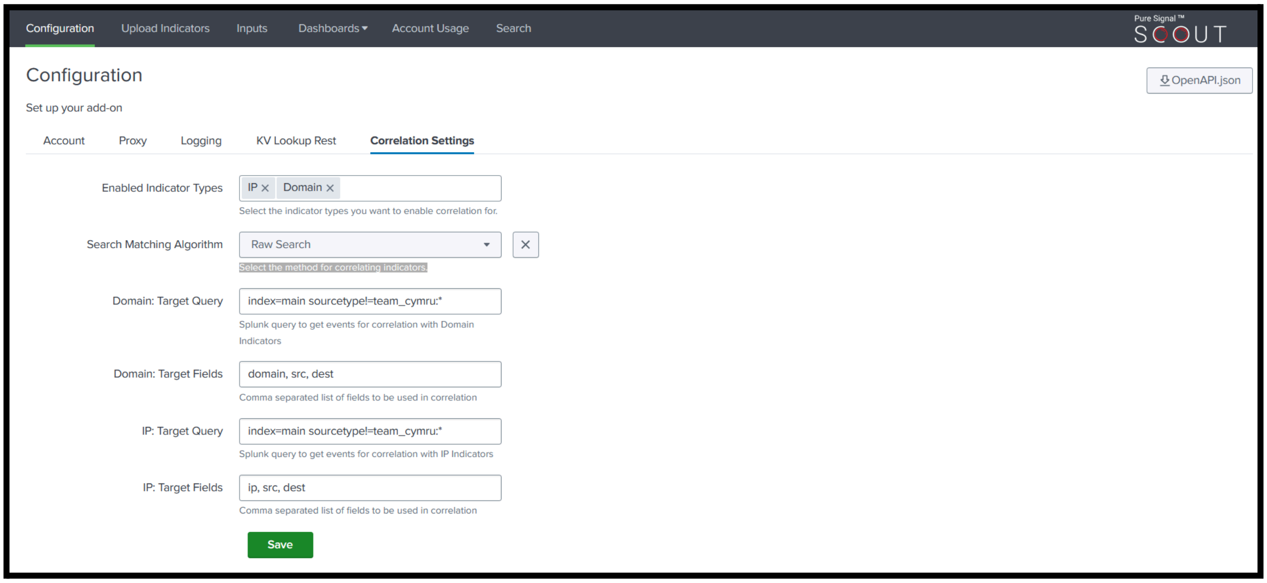
- Search matching Algorithms as Raw Search
- Search matching Algorithms as Data Model Search.

Correlation Setting as Raw Search

1. Go to Team Cymru Scout1 App for Splunk > Configuration > Correlation Settings

2. Add Enabled Indicator Types, and Search Matching Algorithm as Raw Search, Target Query, Target Fields

a. Default values of IP: Target Query will be “index=main sourcetype!=*team_cymru_*” ,IP: Target Fields will be “ip, src, dest”, Domain: Target Query : “index=main sourcetype!=*team_cymru_*”, Domain: Target field=”domain, src, dest”.



Configuration

Set up your add-on

Enabled Indicator Types: IP × Domain ×
Select the indicator types you want to enable correlation for.

Search Matching Algorithm: Raw Search ▾ ×
Select the method for correlating indicators.

Domain: Target Query: index=main sourcetype!=team_cymru:*
Splunk query to get events for correlation with Domain Indicators

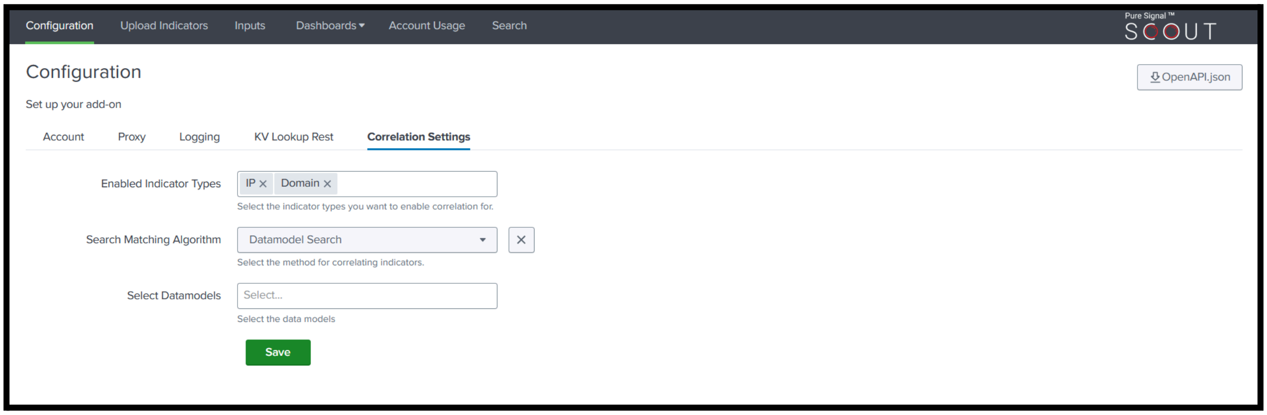
Domain: Target Fields: domain, src, dest
Comma separated list of fields to be used in correlation

IP: Target Query: index=main sourcetype!=team_cymru:*
Splunk query to get events for correlation with IP Indicators

IP: Target Fields: ip, src, dest
Comma separated list of fields to be used in correlation

Correlation Setting as Data Model Search

1. Go to Team Cymru Scout1 App for Splunk > Configuration > Correlation Settings
2. Add Enabled Indicator Types, and Search Matching Algorithm as Data Model, And select Data model from dropdown.



Configuration

Set up your add-on

Enabled Indicator Types: IP × Domain ×
Select the indicator types you want to enable correlation for.

Search Matching Algorithm: Datamodel Search ▾ ×
Select the method for correlating indicators.

Select Datamodels: Select...
Select the data models

To update a Splunk Correlation details

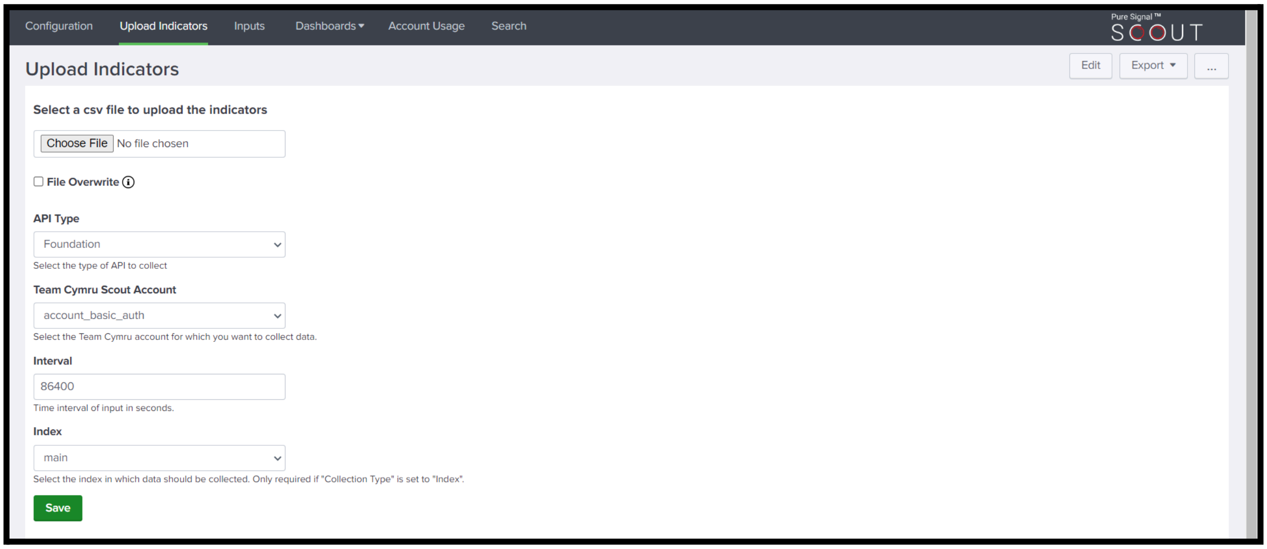
1. Go toTeam Cymru Scout App For Splunk > Configuration > Correlation Settings

2. Update the required parameters.

Click on Save.Upload Indicators

Users can upload indicators by following below methods.

1. Go to Team Cymru Scout1 App for Splunk > upload indicator.
2. Upload a csv file containing indicators (there is a checkbox if the file already exists then user can overwrite existing file)
3. Select API Type from dropbox, select Team Cymru Scout from dropbox, select interval (default value as 86400) And select index from dropdown
4. Click on Save.



Upload Indicators

Select a csv file to upload the indicators

Choose File No file chosen

□ File Overwrite ⓘ

API Type: Foundation

Select the type of API to collect

Team Cymru Scout Account: account_basic_auth

Select the Team Cymru account for which you want to collect data.

Interval: 86400

Time interval of input in seconds.

Index: main

Select the index in which data should be collected. Only required if "Collection Type" is set to "Index".

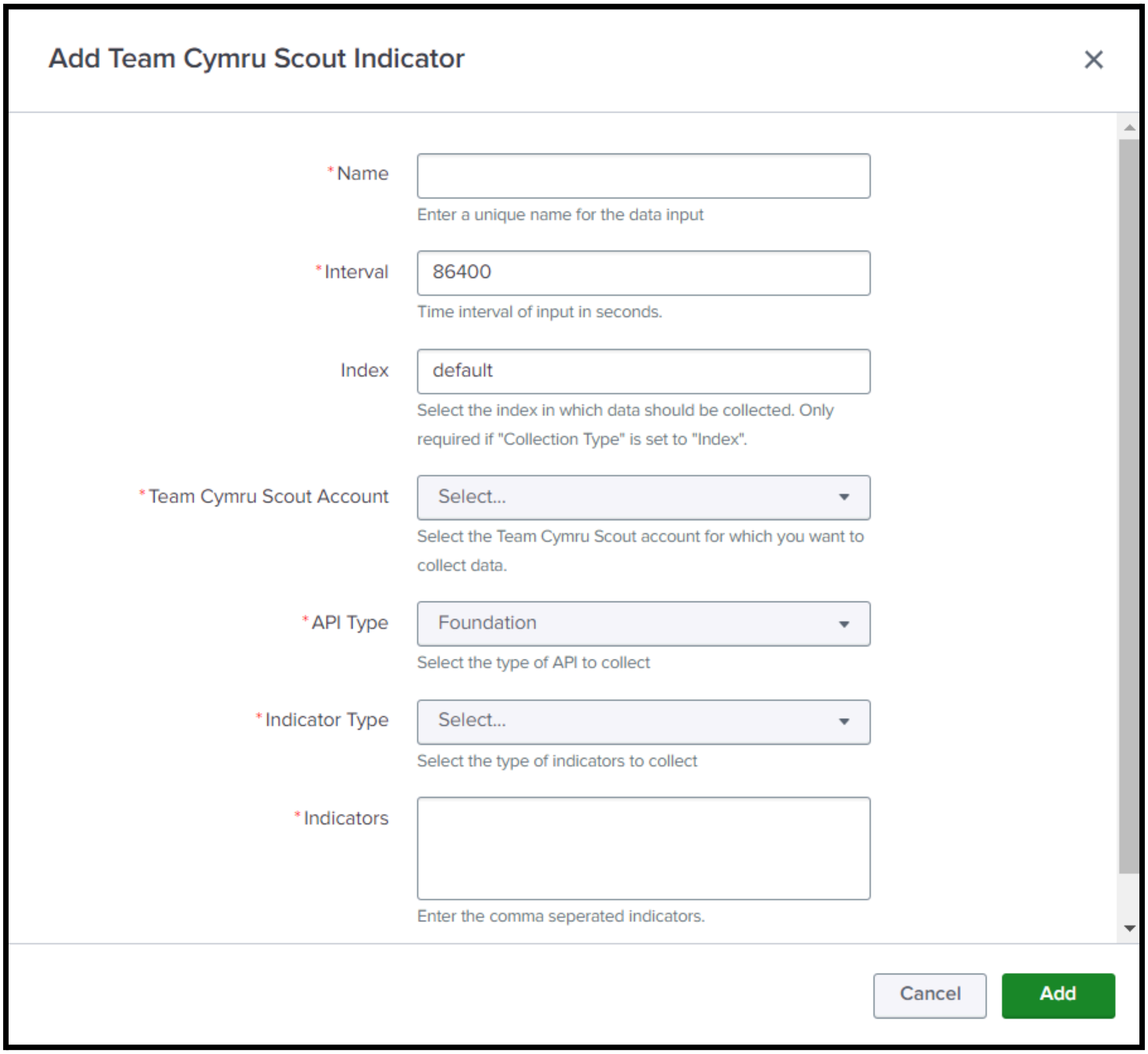
Inputs Page

Users can manually create Modular Input by following below steps.

1. Go to Team Cymru Scout1 App for Splunk >Inputs.
2. Click on create new input
3. And fill all parameters shown in this table.
4. Click on the save button.

Parameters	Type	Description
Name	Textbox	A name to uniquely identify the input.

Interval	Textbox	Time interval for input in seconds. Default = 86400
Index	Dropdown	The index in which data should be collected. Only required if "Collection Type" is set to "Index".
Team Cymru Scout Account	Dropdown	Select the Team Cymru Scout Account for which you want to collect data.
API Type	Dropdown	Select the type of API to collect.
Indicator Type	Dropdown	Select the type of indicator to collect
Indicators	Textbox	Select the comma-separated indicators



Add Team Cymru Scout Indicator

*Name

Enter a unique name for the data input

*Interval: 86400

Time interval of input in seconds.

Index: default

Select the index in which data should be collected. Only required if "Collection Type" is set to "Index".

*Team Cymru Scout Account: Select...

Select the Team Cymru Scout account for which you want to collect data.

*API Type: Foundation

Select the type of API to collect

*Indicator Type: Select...

Select the type of indicators to collect

*Indicators

Enter the comma seperated indicators.

To Disable an Input

1. Go to Team Cymru Scout App For Splunk > Inputs.
2. Find the input User wants to Disable from the list of inputs.
3. Click on Status> Enabled.

To Enable an Input

1. Go to Team Cymru Scout App For Splunk > Inputs.
2. Find the input User wants to Enable from the list of inputs.
3. Click on Status> Disabled

To Edit an Input

1. Go to Team Cymru Scout App For Splunk > Inputs
2. Find the Input User wants to edit from the list of configured inputs.
3. Click on Action > Edit
4. Update the required(desired) parameters in the dialogue box.
5. Click on Update.

To Clone and Delete Input

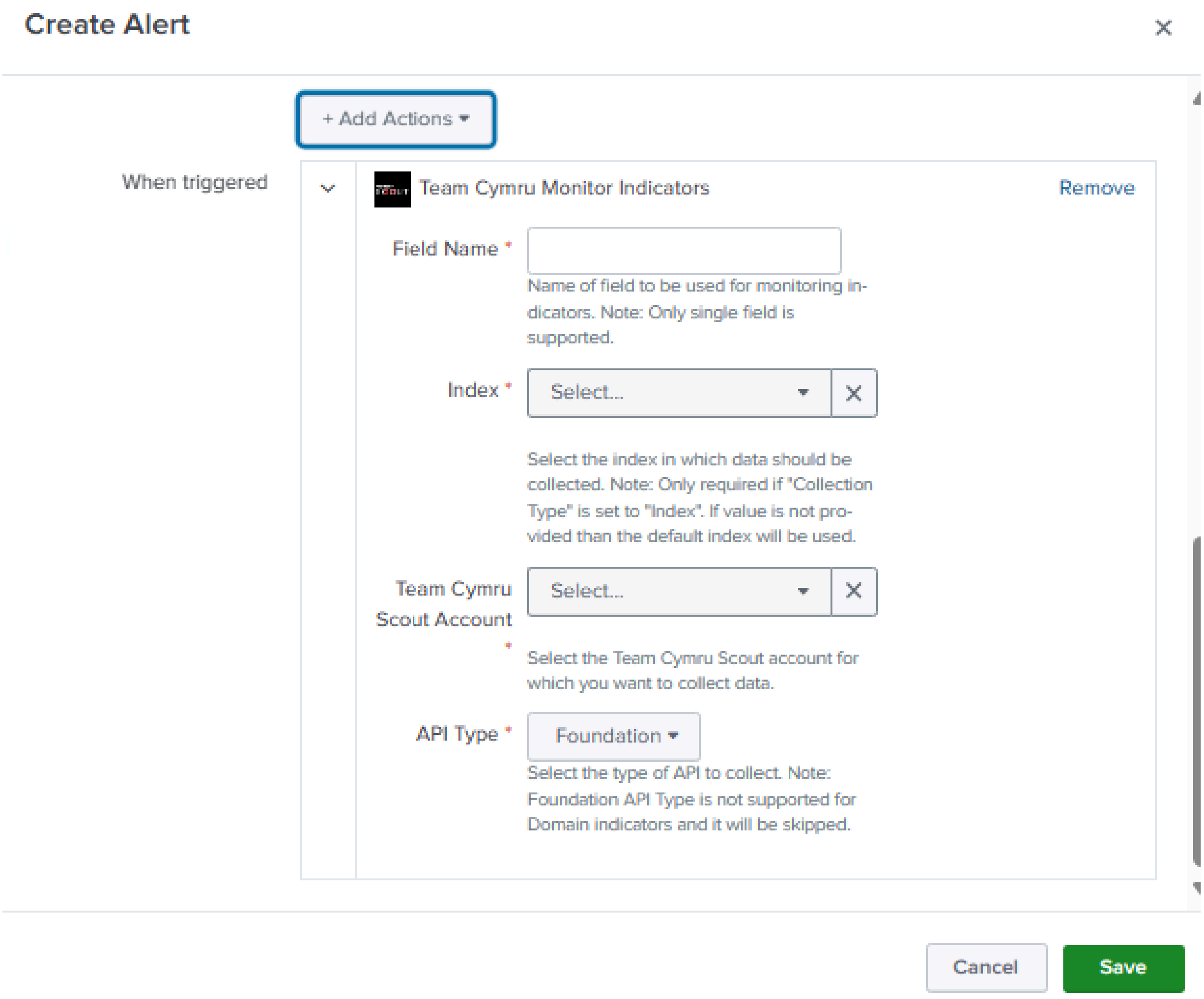
1. Perform the same steps as above mentioned:
2. Go to Team Cymru Scout App for Splunk > Inputs
3. Action > Clone/Delete

Monitor Indicators Page

Users can manually create Monitor Indicators by following below steps.

1. Go to "Settings > Searches, Reports, and Alerts > New Alert -> Add Action > Team Cymru Monitor Indicators".
2. And fill all parameters shown in this table.
3. Click on the save button.

Parameters	**Type**	**Description**
Field Name	Text Box	Name of field to be used for monitoring indicators.
Team Cymru Scout Account	Dropdown	Select the Team Cymru Scout account for which you want to collect data.
Index	Dropdown	Select the index in which data should be collected.
API Type	Dropdown	The type of data user wants to collect for either foundation or details.



Create Alert

When triggered

Team Cymru Monitor Indicators

Field Name *

Name of field to be used for monitoring indicators. Note: Only single field is supported.

Index * Select...

Select the index in which data should be collected. Note: Only required if "Collection Type" is set to "Index". If value is not provided than the default index will be used.

Team Cymru Scout Account * Select...

Select the Team Cymru Scout account for which you want to collect data.

API Type * Foundation ▾

Select the type of API to collect. Note: Foundation API Type is not supported for Domain indicators and it will be skipped.

To Disable an Monitor Indicators

1. Go to “Settings > Searches, Reports, and Alerts”.
2. Find the Monitor Indicators User wants to Disable from the list.
3. Click on Edit > Disable.

To Enable an Monitor Indicators

1. Go to “Settings > Searches, Reports, and Alerts”.
2. Find the Monitor Indicators User wants to Enable from the list.
3. Click on Edit > Enable.

To Edit an Monitor Indicators

1. Go to “Settings > Searches, Reports, and Alerts”.
2. Find the Monitor Indicators User wants to Edit from the list.
3. Click on Edit > Edit Alert.

4. Update the required(desired) parameters in the dialogue box.
5. Click on Save.

To Delete Monitor Indicators

1. Go to “Settings > Searches, Reports, and Alerts”.
2. Find the Monitor Indicators User wants to Delete from the list.
3. Click on Edit > Delete.

Dashboards

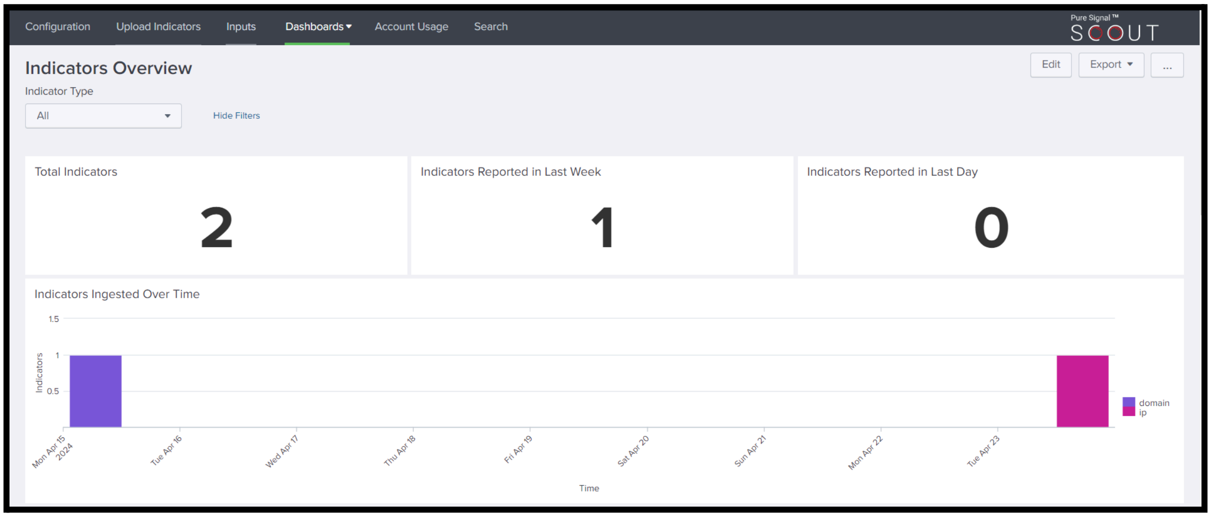
The Team Cymru Scout App For Splunk provides these four dashboards.

1) Indicators Overview

This dashboard shows the user complete information of one or more particular indicators.

Panel Name	Visualization	Description
Total Indicators	Single Value	This panel displays the total number of Indicators which were collected from the Team Cymru Scout platform to Splunk.
	Drill Down	This Will open a new search that shows information of all listed indicators.
Indicators Reported in Last Week	Single Value	This panel displays the total number of Indicators which were collected from the Team Cymru Scout platform to Splunk in the last week.
	Drill Down	This Will open a new search that shows information of all indicators reported last week.
Indicators Reported in Last Day	Single Value	This panel displays the total number of Indicators which were collected from the Team Cymru Scout platform to Splunk on the last day.
	Drill Down	This Will open a new search that shows information of all indicators reported last Day.
Indicators Over Time	Time Chart	This panel contains a Timechart that displays the total number of indicators over time.
	Drill Down	This Will open a new search that shows information of all listed indicators in that time range..
Identity Information by Indicators	Table	In this panel a Table displays the identity information of selected indicators.

Insights Information by Indicators	Table	In this panel a Table displays the insights information of selected indicators.
Indicators Details	Table	In this panel a Table displays the indicator's details.



Indicators Overview

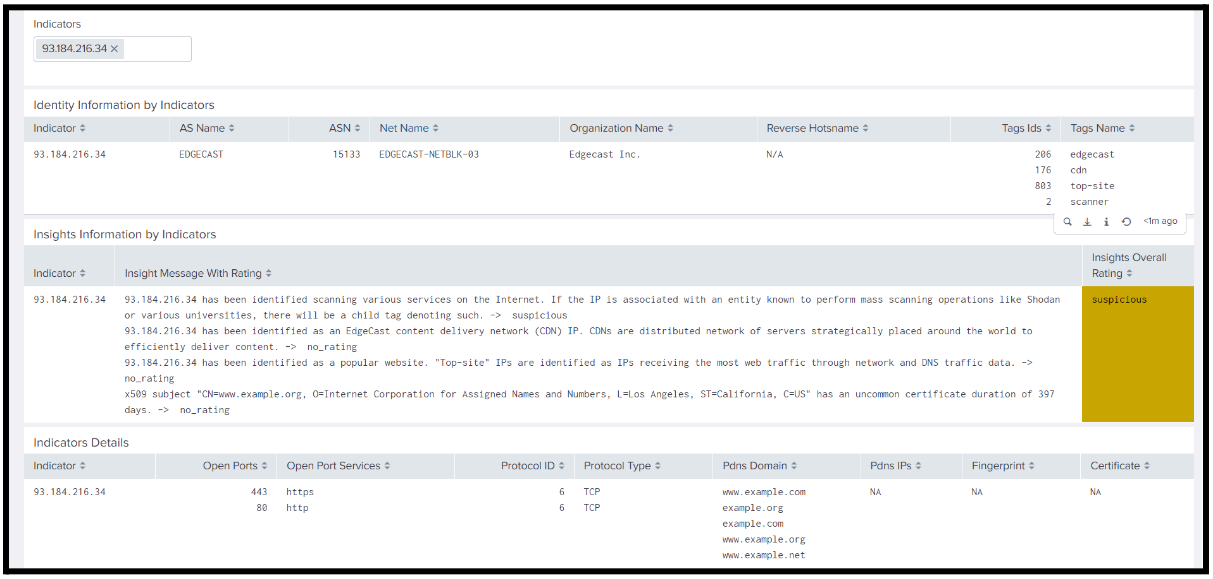
Indicator Type: All

Total Indicators: 2

Indicators Reported in Last Week: 1

Indicators Reported in Last Day: 0

Indicators Ingested Over Time



Indicators

93.184.216.34 ×

Identity Information by Indicators

Indicator	AS Name	ASN	Net Name	Organization Name	Reverse Hotsname	Tags Ids	Tags Name
93.184.216.34	EDGECAST	15133	EDGECAST-NETBLK-03	Edgecast Inc.	N/A	206 176 803 2	edgecast cdn top-site scanner

Insights Information by Indicators

Indicator	Insight Message With Rating	Insights Overall Rating
93.184.216.34	93.184.216.34 has been identified scanning various services on the Internet. If the IP is associated with an entity known to perform mass scanning operations like Shodan or various universities, there will be a child tag denoting such. -> suspicious 93.184.216.34 has been identified as an EdgeCast content delivery network (CDN) IP. CDNs are distributed network of servers strategically placed around the world to efficiently deliver content. -> no_rating 93.184.216.34 has been identified as a popular website. "Top-site" IPs are identified as IPs receiving the most web traffic through network and DNS traffic data. -> no_rating x509 subject "CN=www.example.org, O=Internet Corporation for Assigned Names and Numbers, L=Los Angeles, ST=California, C=US" has an uncommon certificate duration of 397 days. -> no_rating	suspicious

Indicators Details

Indicator	Open Ports	Open Port Services	Protocol ID	Protocol Type	Pdns Domain	Pdns IPs	Fingerprint	Certificate
93.184.216.34	443 80	https http	6 6	TCP TCP	www.example.com example.org example.com www.example.org www.example.net	NA	NA	NA

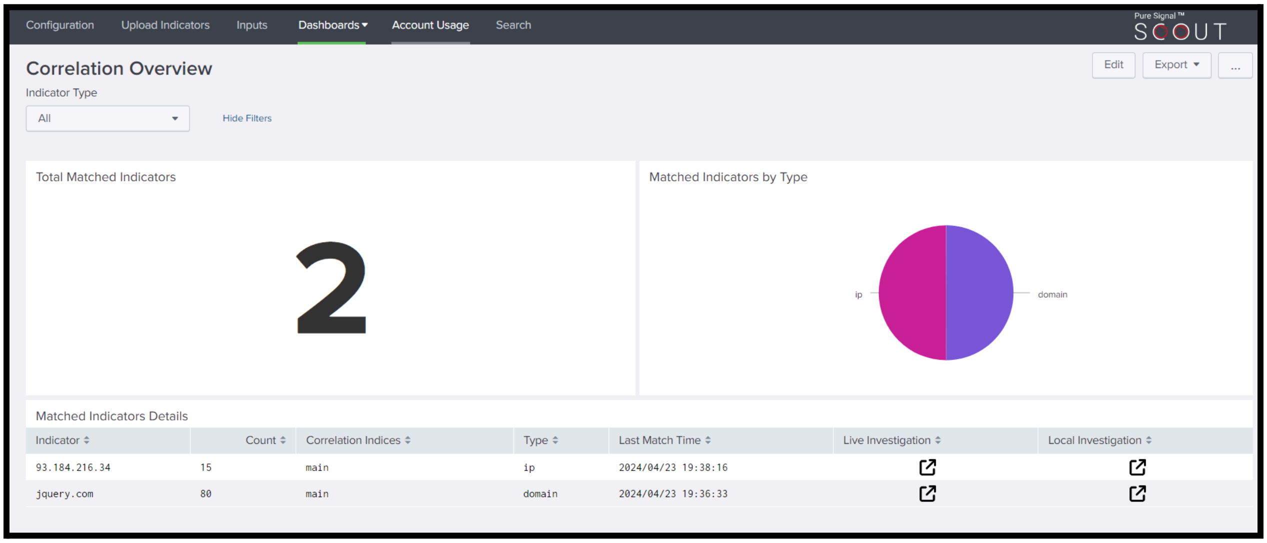
2) Correlation Overview

This dashboard shows the complete information of matched indicators.

Panel Name	Visualization	Description

Total Matched Indicators	Single Value	This panel displays the total number of Indicators which are found in the Splunk index.
	Drill Down	This will open a new search with information of that total matched indicators.
Matched Indicators by Type	Column chart	This panel will display the distribution of sightings over the Type. Users can see the matched Indicators per type from this panel.
	Drill Down	This will open a new search with information of that total matched indicators by type.
Matched Indicators Details	Table	displays matched indicators information according to the selected indicator type.

Note: The local investigation button will only be clickable if the Correlation Indices have some value.



Matched Indicators Details

Indicator	Count	Correlation Indices	Type	Last Match Time	Live Investigation	Local Investigation
93.184.216.34	15	main	ip	2024/04/23 19:38:16	↗	↗
jquery.com	80	main	domain	2024/04/23 19:36:33	↗	↗

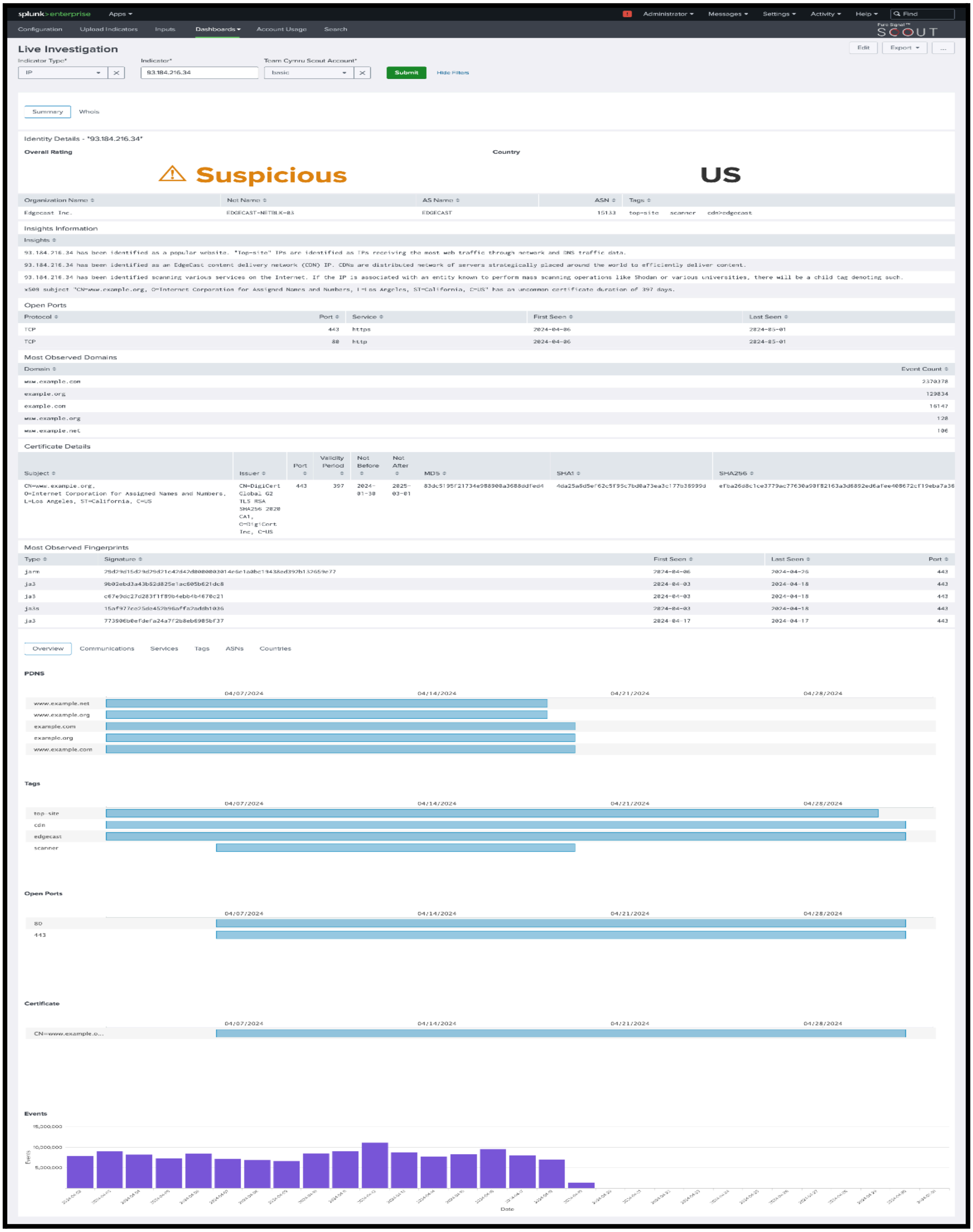
3) Live Investigation

This dashboard shows complete information based on indicator type and particular indicator.

Panel Name	Visualization	Description

Indicator Type	Dropdown	Users can select either IP or Domain.
Indicator	Textbox	This filter user can enter a specific indicator.
Team Cymru Scout Account	Dropdown	This filter shows a list of all the configured accounts.
Identity Details	Table	This panel displays the complete information of the indicator.
Insights	Table	This panel displays insights of the indicator.
Open Ports	Table	This panel displays the open ports information of the indicator
Most Observed Domain	Table	This panel displays the most observed panel and count.
Certificate Details	Table	This panel displays the certificate details for the indicators.
Most Observed Fingerprints	Table	This panel displays the most observed fingerprints.
Overview -> PDNS	Timeline	This panel shows the timeline of the domain in that indicator.
Overview -> tags	Timeline	This panel shows the timeline of tags in that indicator.
Overview -> Open Ports	Timeline	This panel shows the timeline of Open ports in that indicator.
Overview -> Certificate	Timeline	This panel shows the timeline of the Certificate in that indicator.
Overview -> Events	Chart	This panel shows a chart of total events in a time range.
Communication -> Protocols for "indicator" and Its Peers	chart	This panel gives information of a particular protocol for indicator and its peers.
Services -> Top 10 Services for "indicator"	chart	This panel gives information of top 10 services for a particular indicator.

Tags -> Top 10 Tags for “Indicator” and Its Peers	chart	This panel gives information of top 10 tags for a particular indicator and its peers.
ASNs -> Top 10 ASNs for "indicator" and Its Peers	chart	This panel gives information of top 10 ASNs for a particular indicator and its peers.
Country code -> Top 10 Countries for "indicator" and Its Peers	chart	This panel gives information of top 10 countries for a particular indicator and its peers.
Whois -> General	Table	This panel shows General information of a particular indicator. Like asn, asn_name
Whois -> Admin	Table	This panel shows General information of a particular indicator. Like an admin address.
Whois -> Tech	Table	This panel shows Tech information of a particular indicator. Like Texh contact details.
Whois -> Organization	Table	This panel shows Organization information of a particular indicator. Like the Organization name.
Domain Details for: "indicator"	Table	This panel shows complete information of a particular domain indicator. Like ip, Tag_name.



Live Investigation

Indicator Type*: IP

Indicator*: 93.184.216.34

Team Cymru Scout Account*: basic

Identity Details - "93.184.216.34"

Overall Rating

⚠ Suspicious

Country

US

Organization Name ≑	Net Name ≑	AS Name ≑	ASN ≑	Tags ≑
Edgecast Inc.	EDGECAST-NETBLK-03	EDGECAST	15133	top-site scanner cdn>edgecast

Insights Information

Insights ≑
93.184.216.34 has been identified as a popular website. "Top-site" IPs are identified as IPs receiving the most web traffic through network and DNS traffic data.
93.184.216.34 has been identified as an EdgeCast content delivery network (CDN) IP. CDNs are distributed network of servers strategically placed around the world to efficiently deliver content.
93.184.216.34 has been identified scanning various services on the Internet. If the IP is associated with an entity known to perform mass scanning operations like Shodan or various universities, there will be a child tag denoting such.
x509 subject "CN=www.example.org, O=Internet Corporation for Assigned Names and Numbers, L=Los Angeles, ST=California, C=US" has an uncommon certificate duration of 397 days.

Open Ports

Protocol ≑	Port ≑	Service ≑	First Seen ≑	Last Seen ≑
TCP	443	https	2024-04-06	2024-05-01
TCP	80	http	2024-04-06	2024-05-01

Most Observed Domains

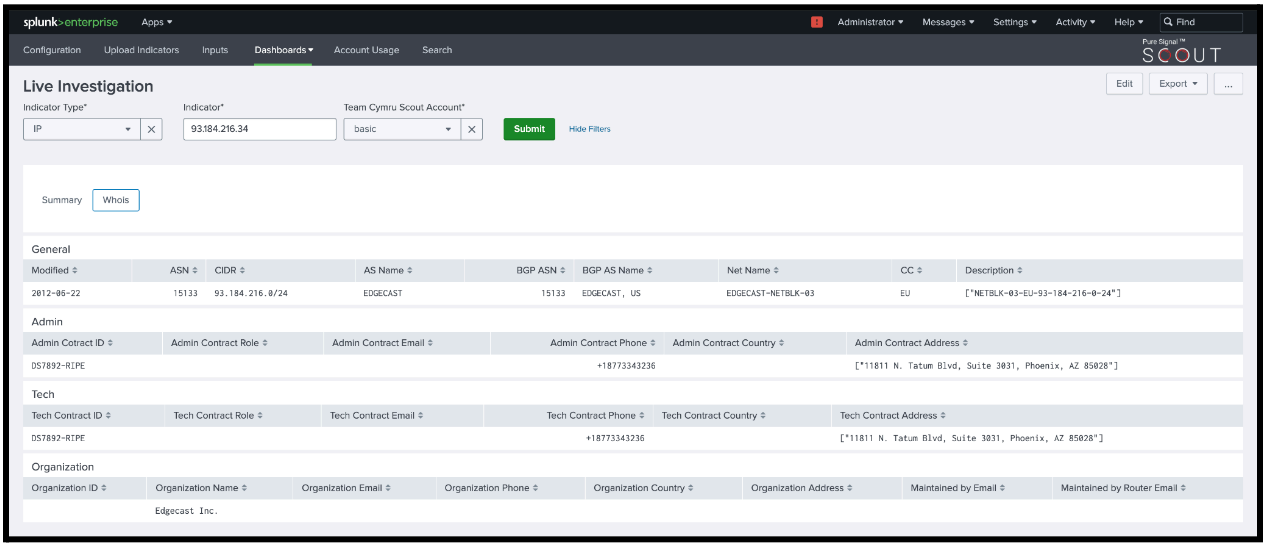
Domain ≑	Event Count ≑
www.example.com	2370378
example.org	129834
example.com	16147
www.example.org	128
www.example.net	106

Certificate Details

Subject ≑	Issuer ≑	Port ≑	Validity Period ≑	Not Before ≑	Not After ≑	MD5 ≑	SHA1 ≑	SHA256 ≑
CN=www.example.org, O=Internet Corporation for Assigned Names and Numbers, L=Los Angeles, ST=California, C=US	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	443	397	2024-01-30	2025-03-01	83dc5195f21734e988908a3688ddfed4	4da25a6d5ef62c5f95c7bd0a73ea3c177b36999d	efba26d8c1ce3779ac77630a90f82163a3d6892ed6afee408672cf19eba7a36

Most Observed Fingerprints

Type ≑	Signature ≑	First Seen ≑	Last Seen ≑	Port ≑
jarm	29d29d15d29d29d21c42d42d000000307014e6e1a0bc19438ad392b132659e77	2024-04-06	2024-04-26	443
ja3	9b02ebd3a43b62d825e1ac605b621dc8	2024-04-03	2024-04-18	443
ja3	c67e9dc27d283f1f89b4ebb4b4670c21	2024-04-03	2024-04-18	443
ja3s	15af977ce25de452b96affa2addb1036	2024-04-03	2024-04-18	443
ja3	773906b0efdefa24a7f2b8eb6985bf37	2024-04-17	2024-04-17	443



Live Investigation

Indicator Type*: IP

Indicator*: 93.184.216.34

Team Cymru Scout Account*: basic

General

Modified	ASN	CIDR	AS Name	BGP ASN	BGP AS Name	Net Name	CC	Description
2012-06-22	15133	93.184.216.0/24	EDGECAST	15133	EDGECAST, US	EDGECAST-NETBLK-03	EU	["NETBLK-03-EU-93-184-216-0-24"]

Admin

Admin Cotract ID	Admin Contract Role	Admin Contract Email	Admin Contract Phone	Admin Contract Country	Admin Contract Address
DS7892-RIPE			+18773343236		["11811 N. Tatum Blvd, Suite 3031, Phoenix, AZ 85028"]

Tech

Tech Contract ID	Tech Contract Role	Tech Contract Email	Tech Contract Phone	Tech Contract Country	Tech Contract Address
DS7892-RIPE			+18773343236		["11811 N. Tatum Blvd, Suite 3031, Phoenix, AZ 85028"]

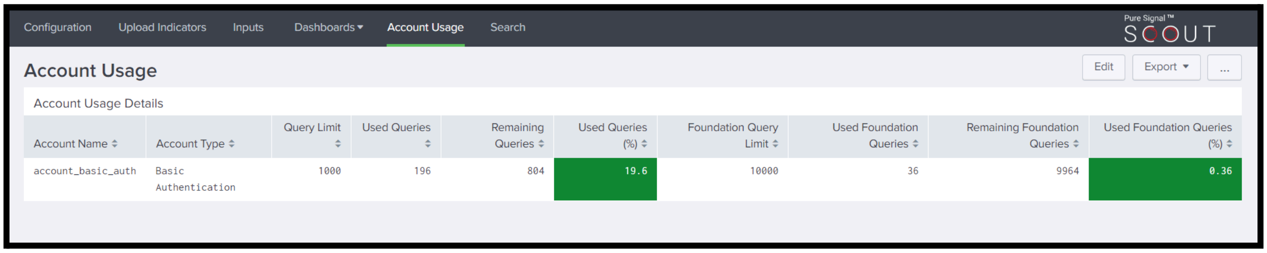
Organization

Organization ID	Organization Name	Organization Email	Organization Phone	Organization Country	Organization Address	Maintained by Email	Maintained by Router Email
	Edgecast Inc.						

4) Account Usage

This dashboard shows complete details of users accounts.

Panel Name	Visualization	Description
Account Usage Details	Table	This panel displays the overall usage of accounts, like query limit and query usages..



Account Usage

Account Usage Details

Account Name	Account Type	Query Limit	Used Queries	Remaining Queries	Used Queries (%)	Foundation Query Limit	Used Foundation Queries	Remaining Foundation Queries	Used Foundation Queries (%)
account_basic_auth	Basic Authentication	1000	196	804	19.6	10000	36	9964	0.36

How To make Dashboards

If User wants to make dashboards and Panels First Follow below steps for going to the dashboards.

1. Go to Team Cymru Scout App For Splunk > Dashboards.

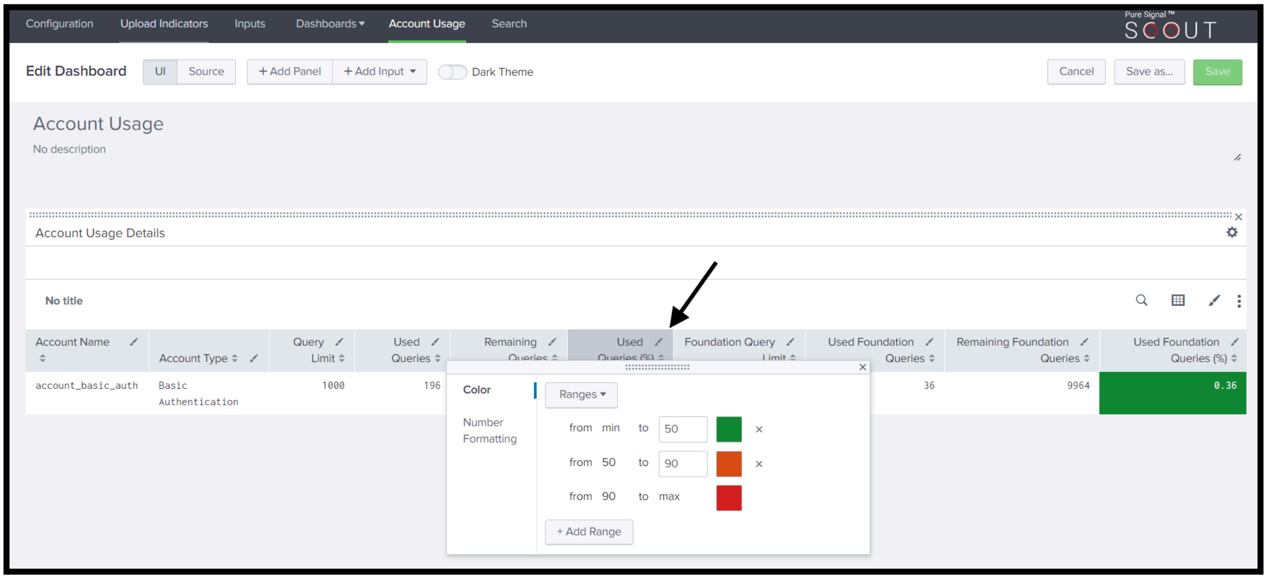
2. Select Create new Dashboard on Top right corner

After that User can follow this (reference) to learn how to create dashboards and panels.

How to change Color of a panel

If a user wishes to change the color of a panel or a column of any dashboard follow below steps.

1. Go to the desired dashboard > click on Edit button on top right corner.
2. Then go to the panel or particular column User wants to change color and click on an icon that says' format visualization’ That looks like a pencil icon and there User can change the color of any panel.
3. In the picture below an arrow shows that button.
4. If User wants to change color with a particular range Ex. In Account usage dashboard User want Used queries in color green when it is From min to 50 and User want it Red when Used queries percentage is between 90 to 100. Users can do that by following the above steps than choosing color Range option.



Account Name	Account Type	Query Limit	Used Queries	Remaining Queries	Used Queries (%)	Foundation Query Limit	Used Foundation Queries	Remaining Foundation Queries	Used Foundation Queries (%)
account_basic_auth	Basic Authentication	1000	196				36	9964	0.36

from min to 50 🟩 ×
from 50 to 90 🟧 ×
from 90 to max 🟥

Uninstalling the App

1. Follow these instructions based on the User environment.

Uninstalling from a Standalone Environment

1. Remove $SPLUNK_HOME/etc/apps/TeamCymruScoutAppForSplunk

2. Remove $SPLUNK_HOME/var/log/Splunk/ta_team_cymru_scout*.log*.
3. To reflect the cleanup changes in UI, Restart Splunk Enterprise instance

Splunk Knowledge Objects

Sourcetypes

The Team Cymru Scout App For Splunk provides the search-time knowledge for Team Cymru Scout data in the following formats:

Sourcetype	Description
team_cymru_details_domain	This sourcetype will have details data for domains.
team_cymru_details_ip	This sourcetype will have details data for ip.
team_cymru_foundation_ip	This sourcetype will have foundation data for ip.
stash_team_cymru_details_domain	This sourcetype will have details data for domains collected with monitor indicators.
stash_team_cymru_details_ip	This sourcetype will have details data for ip collected with monitor indicators.
stash_team_cymru_foundation_ip	This sourcetype will have foundation data for ip collected with monitor indicators.
ta_team_cymru_scout_log	This sourcetype will contain the all logs of Team Cymru Scout App For Splunk

Lookups

- This application contains the following lookup

- Master lookup
  - Team_cymru_indicators_foundation_ip: This lookup contains the foundation data for IP.
  - Team_cymru_indicators_details_ip: This lookup contains the details data for IP.
  - Team_cymru_indicators_details_domain: This lookup contains the details data for the domain .
- Match lookup
  - Team_cymru_matched_indicators_ip : This lookup contains the matched indicator data for IP.

    - Team_cymru_matched_indicators_domain: This lookup contains the matched indicator data for Domain.

Savedsearches

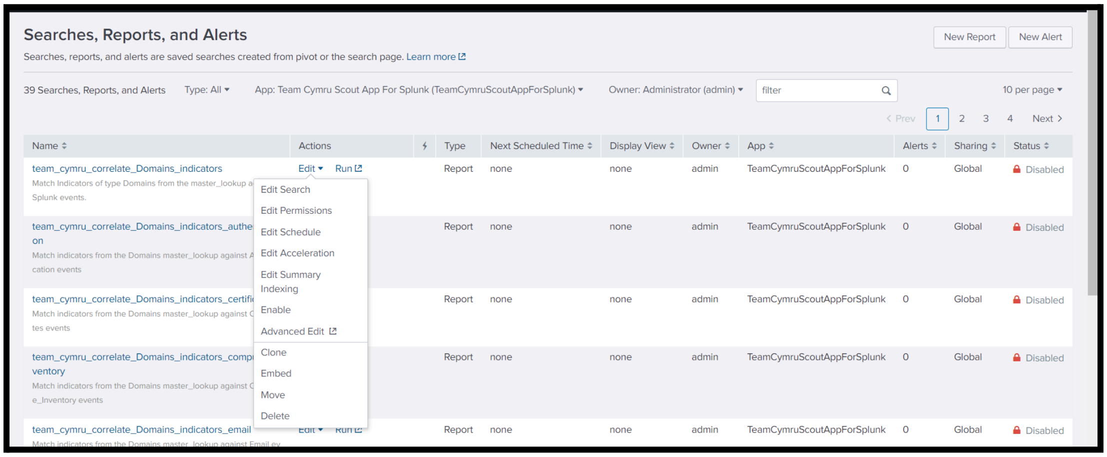
- This application contains the following saved search

- **team_cymru_correlate_Domains_indicators_malware** - Match indicators from the Domains master_lookup against Malware events .
- **team_cymru_correlate_Domains_indicators_intrusion_detection** - Match indicators from the Domains master_lookup against Intrusion_Detection events .
- **team_cymru_correlate_Domains_indicators_authentication** - Match indicators from the Domains master_lookup against Authentication events .
- **team_cymru_correlate_Domains_indicators_certificates** - Match indicators from the Domains master_lookup against Certificates events.
- **team_cymru_correlate_Domains_indicators_endpoint_filesystem** - Match indicators from the Domains master_lookup against Endpoint (Filesystem dataset) events .
- **team_cymru_correlate_Domains_indicators_endpoint_services** - Match indicators from the Domains master_lookup against Endpoint (Services dataset) events.
- **team_cymru_correlate_Domains_indicators_endpoint_processes** - Match indicators from the Domains master_lookup against Endpoint (Processes dataset) events.
- **team_cymru_correlate_Domains_indicators_email** -Match indicators from the Domains master_lookup against Email events.
- **team_cymru_correlate_Domains_indicators_compute_inventory** - Match indicators from the Domains master_lookup against Compute_Inventory events .
- **team_cymru_correlate_Domains_indicators_network_resolution** -Match indicators from the Domains master_lookup against Network_Resolution events
- **team_cymru_correlate_Domains_indicators_updates** - Match indicators from the Domains master_lookup against Updates events.
- **team_cymru_correlate_Domains_indicators_web** - Match indicators from the Domains master_lookup against Web events.
- **update_team_cymru_foundation_ip_indicator_master_lookup** - Update Foundation IP Indicators from index to `team_cymru_indicators_foundation_ip`
- **update_team_cymru_details_ip_indicator_master_lookup** -Update Details IP Indicators from index to `team_cymru_indicators_details_ip`
- **update_team_cymru_details_domain_indicator_master_lookup** - Update Details Domain Indicators from index to `team_cymru_indicators_details_domain` .
- **team_cymru_correlate_Domains_indicators** -Match Indicators of type Domains from the master_lookup against Splunk events .
- **team_cymru_correlate_IPs_indicators** - Match Indicators of type IPs from the master_lookup against Splunk events.
- **team_cymru_correlate_IPs_indicators_network_traffic** - Match indicators from the IPs master_lookup against Network_Traffic events.
- **team_cymru_correlate_IPs_indicators_malware** - Match indicators from the IPs master_lookup against Malware events
- **team_cymru_correlate_IPs_indicators_intrusion_detection** - Match indicators from the IPs master_lookup against Intrusion_Detection events
- **team_cymru_correlate_IPs_indicators_authentication** - Match indicators from the IPs master_lookup against Authentication events.
- **team_cymru_correlate_IPs_indicators_certificates** - Match indicators from the IPs master_lookup against Certificates events.
- **team_cymru_correlate_IPs_indicators_endpoint_filesystem** - Match indicators from the IPs master_lookup against Endpoint (Filesystem dataset) events.

- **team_cymru_correlate_IPs_indicators_endpoint_services** - Match indicators from the IPs master_lookup against Endpoint (Services dataset) events.
- **team_cymru_correlate_IPs_indicators_endpoint_processes** - Match indicators from the IPs master_lookup against Endpoint (Processes dataset) events.
- **team_cymru_correlate_IPs_indicators_email** - Match indicators from the IPs master_lookup against Email events.
- **team_cymru_correlate_IPs_indicators_compute_inventory** - Match indicators from the IPs master_lookup against Compute_Inventory events.
- **team_cymru_correlate_IPs_indicators_network_resolution** - Match indicators from the IPs master_lookup against Network_Resolution events.
- **team_cymru_correlate_IPs_indicators_updates** - Match indicators from the IPs master_lookup against Updates events.
- **team_cymru_correlate_IPs_indicators_web** - Match indicators from the IPs master_lookup against Web events.
- **team_cymru_correlate_Domains_indicators_network_traffic** - Match indicators from the Domains master_lookup against Network_Traffic events .

If User want to enable/disable Savedsearches

1. If User wishes to enable or disable any existing savedsearches follow below steps.
2. Click on setting > Searches, reports, and alerts
3. Then select App as ‘Cymru_Scout_App’ and type the name in the filter section And User will see that savedsearch.
4. That User can click on the Edit button where User will see the enable/disable button.
5. All savedsearches will be disabled by default except our master lookup savedsearches.



Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more

39 Searches, Reports, and Alerts   Type: All   App: Team Cymru Scout App For Splunk (TeamCymruScoutAppForSplunk)   Owner: Administrator (admin)   filter   10 per page

Name	Actions	⚡	Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
team_cymru_correlate_Domains_indicators Match Indicators of type Domains from the master_lookup a Splunk events.	Edit ▾ Run		Report	none	none	admin	TeamCymruScoutAppForSplunk	0	Global	Disabled
team_cymru_correlate_Domains_indicators_authe on Match indicators from the Domains master_lookup against A cation events			Report	none	none	admin	TeamCymruScoutAppForSplunk	0	Global	Disabled
team_cymru_correlate_Domains_indicators_certifi Match indicators from the Domains master_lookup against C tes events			Report	none	none	admin	TeamCymruScoutAppForSplunk	0	Global	Disabled
team_cymru_correlate_Domains_indicators_comp ventory Match indicators from the Domains master_lookup against C e_Inventory events			Report	none	none	admin	TeamCymruScoutAppForSplunk	0	Global	Disabled
team_cymru_correlate_Domains_indicators_email Match indicators from the Domains master_lookup against Email ev	Edit ▾ Run		Report	none	none	admin	TeamCymruScoutAppForSplunk	0	Global	Disabled

Troubleshooting

General Checking

- To troubleshoot Team Cymru Scout App For Splunk, check $SPLUNK_HOME/var/log/Splunk/ta_team_cymru_scout*.log or user can search `index="_internal" source=*ta_team_cymru_scout*.log*` query to see all the logs in the UI. Also, user can use `index="_internal" source=*ta_team_cymru_scout*.log* ERROR` query to see ERROR logs in the Splunk UI.

- Note that all log files of this App will be generated in `$SPLUNK_HOME/var/log/Splunk/` directory.
- if User are facing a problem related to ip address, than check for the lookup `team_cymru_indicators_details_ip`
- if User are facing a problem related to domain address, than check for the lookup `team_cymru_indicators_details_domain`
- if User are facing a problem related to foundation ip address, than check for the lookup `team_cymru_indicators_foundation_ip`
- App icons are not showing up: The App does not require restart after the installation in order for all functionalities to work. However, the icons will be visible after one Splunk restart post installation.
- If a dashboard panel fails to load and displays a triangle icon, attempt to refresh the panel. This issue could be caused by a 429 API error.

Data Collection

- If data collection is not working then ensure that the internet is active (On a proxy machine, if proxy is enabled) and also ensure that the kvstore is enabled.
- Check `ta_team_cymru_scout*.log*` file for Team Cymru Scout App For Splunk data collection for any relevant error messages.

Correlation

- Note that correlation is field based and it will only match to those Splunk events having value exactly the same as indicator value.
- Check the `ta_team_cymru_scout_correlation_command.log` file for further analysis.

Master Lookup

- If it seems that all the data of indicators from the Splunk index is not available in `team_cymru_scout_indicators_<indicator_type>` lookup, then execute the savedsearch `update_TeamCymruScoutAppForSplunk_<indicator_type>_indicator_master_lookup` manually over a larger time range to refill the lookup.

Custom Commands

- teamcymrumatchindicators
    - Check that indices of the collected Indicators data are stored in `Indicator Indices` parameter of correlation settings.
    - Check that `team_cymru_scout_indicators_<indicator_type>` lookup is not empty and also ensure that ``team_cymru_scout_correlate_<indicator_type>_indicators` savedsearch is enabled.
    - Check the `ta_TeamCymruScout App_correlation_command.log` file for further analysis.
- teamcymruaccountusage
    - Check that `ta_team_cymru_scout_indicators_<indicator_type>` lookup is not empty
- teamcymruscoutsectionsearch
    - Check the `ta_team_cymru_scout_section_search_command.log` file for further analysis.
- teamcymruscoutsearch

- Check the `ta_team_cymru_scout_search_command.log` file for further analysis.

Alert Actions

This application contains the following alert actions:

- **team_cymru_indicators_monitors**
    - Description : To monitor indicators from a given search with Team Cymru Scout.
    - Parameters :
        - field_name: Name of field to be used for monitoring indicators.
        - index: Select the index in which data should be collected.
        - global_account: Select the Team Cymru Scout account for which you want to collect data.
        - api_type: Select the type of API to collect.

SEARCHES

- To see ingested data for Team Cymru Scout App For Splunk, select the Search tab. Search `team_cymru_indicator_indices` sourcetype=*team_cymru_*.

Troubleshooting Dashboard

While troubleshooting for dashboards if your panel is not populating first check that in queries the user has selected the same index that he uses during creating indicators.

Note: As the subsearch has a limit of max 50k records. So if you have more than 50k records in lookup and the count is not matching with dashboard then create limits.conf in $SPLUNK_HOME/etc/apps/TeamCymruScoutAppForSplunk/local and add the below stanzas:

```
[searchresults]
maxresultrows = 9999999

[subsearch]
maxtime=120
```

1. Indicator Overview:
    a. If the data is not populated in any panels, then ensure that Indicator data is collected in Splunk and the `team_cymru_matched_indicators_<indicator_type>` lookup is filled with the latest data.

b. Also please ensure that savedsearches `team_cymru_indicators_<indicator_type>` savedsearches are enabled.
c. If dashboard panels are not populating data, it is possible that App's Saved Searches have not yet encountered newly ingested data on their previous execution. Please check Next Schedule Time in Settings -> Searches, reports and alerts. Most likely the panels will be populated once all saved searches complete their next execution.

2. Correlation overview:
    a. If the data is not populated in the above listed panels, then ensure that Indicator data is collected in Splunk and the `team_cymru_matched_indicators_<indicator_type>` lookup is filled with the latest data.
    b. Also please ensure that savedsearches `team_cymru_correlate_IPs_indicators_<indicator_type>` savedsearches are enabled.
    c. If dashboard panels are not populating data, it is possible that App's Saved Searches have not yet encountered newly ingested data on their previous execution. Please check Next Schedule Time in Settings -> Searches, reports and alerts. Most likely the panels will be populated once all saved searches complete their next execution.

3. Live Investigation:
    a. If the data is not populated in the above listed panels, then ensure that Indicator data is collected in Splunk and the `team_cymru_indicators_<indicator_type>` is filled with the latest data.
    b. Also update the indices on correlation settings -> `Indicator Indices` from which user wants to fill TeamCymruScout App_indicators_<indicator_type>.
    c. Also please ensure that savedsearch `update_team_cymru_details_<indicator_type>_master_lookup` is enabled.
    d. If dashboard panels are not populating data, it is possible that App's Saved Searches have not yet encountered newly ingested data on their previous execution. Please check Next Schedule Time in Settings -> Searches, reports and alerts. Most likely the panels will be populated once all saved searches complete their next execution.

4. Account Usage:
    a. If dashboard panels are not populating data, it is possible that App's Saved Searches have not yet encountered newly ingested data on their previous execution. Please check Next Schedule Time in Settings -> Searches, reports and alerts. Most likely the panels will be populated once all saved searches complete their next execution.

Field Extraction Issues

- Verify that the Team Cymru Scout App For Splunk is installed properly in the Splunk environment.
- Verify that the sourcetype of the data is according to the list of sourcetype mentioned.
- Check the data is being collected by the Team Cymru Scout App For Splunk in the Specified index.

SUPPORT

Contact us at support@cymru.com