

Secureworks CTP Functions for IBM Resilient

- [Release Notes](#)
- [Overview](#)
- [Requirements](#)
- [Installation](#)
- [Uninstall](#)
- [Troubleshooting](#)
- [Support](#)

Release Notes

v1.0.0

- Initial Release


Overview



The Secureworks Counter Threat Platform (CTP) uses the global visibility gained from gathering and analyzing data from clients all over the world to more accurately identify, contain and eradicate cybersecurity threats. By combining up-to-the-minute threat intelligence with the CTP's machine learning and analytics capabilities, organizations can make faster, more informed decisions about how to predict, prevent, detect, and respond to threat activity.

CTP is used with the Secureworks SOC team when they find a security issue that needs to be communicated to the customer. The issues can be informational, research-based or require proscriptive actions by the customer. Secureworks CTP provides a “ticket-like” interface that allows you acknowledge, add files and notes, and provide ability to close tickets.

The Secureworks CTP integration implements the following functionality in Resilient:

- Poll Secureworks CTP for tickets and create a corresponding incident in the Resilient platform for each ticket.
- Get Secureworks CTP ticket workLogs and attachments and add them as notes and attachments in the corresponding Resilient incident.
- Close a Secureworks CTP ticket when the corresponding Resilient incident is closed.
- Close a Resilient incident when the corresponding Secureworks CTP ticket is closed in Secureworks.


 Dashboards ▾ Inbox Incidents Create ▾

  Resilient Sysadmin resilient ▾

Customization Settings


Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

Functions

sec

Name	Description
Secureworks CTP Close Ticket	Close a Secureworks CTP ticket in an incident that has a Secureworks CTP ticket associated with it.

© Copyright IBM Corporation 2020



Requirements

- Resilient platform >= v35.0.5445
- An Integration Server running resilient_circuits>=30.0.0

- To set up an Integration Server see: ibm.biz/res-int-server-guide
- If using API Keys, minimum required permissions are:
 - Incidents: Read, Create
 - Edit Incidents: Fields, Notes
 - Org Data: Read, Edit
 - Functions: Read

Installation

App Host

All the components for running this integration in a container already exist when using the App Host app.

To install,

- Navigate to Administrative Settings and then the Apps tab.
- Click the Install button and select the downloaded file: app-fn_secureworks_ctp-x.x.x.zip.
- Go to the Configuration tab and edit the app.config file, editing the username and password for Secureworks CTP and making any additional setting changes.

Config	Required	Example
base_url	Yes	https://api.secureworks.com/api/ticket/v3
username	Yes	user@example.com
password	Yes	''
query_ticket_grouping_types	Yes	INCIDENT:SECURITY
query_limit	Yes	10
polling_interval	Yes	600
close_codes	No	Authorized Activity,Confirmed Security Incident,Duplicate,Incident Misidentified,Inconc

Config	Required	Example
template_file_escalate	No	“
template_file_close	No	“
template_file_update	No	“
cafile	No	“

Integration Server

- Download the `fn_secureworks_ctp.zip`.
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:


```
$ unzip fn_secureworks_ctp-x.x.x.zip
```
- **Change Directory** into the unzipped directory:


```
$ cd fn_secureworks_ctp-x.x.x
```
- **Install** the package:


```
$ pip install fn_secureworks_ctp-x.x.x.tar.gz
```
- Import the **configurations** into your `app.config` file:


```
$ resilient-circuits config -u -l fn-secureworks-ctp
```
- Import the `fn_secureworks_ctp` **customizations** into the Resilient platform:


```
$ resilient-circuits customize -y -l fn-secureworks-ctp
```
- Open the config file, scroll to the bottom and edit your `fn_secureworks_ctp` configurations:


```
$ vi ~/.resilient/app.config
```

Config	Required	Example
base_url	Yes	<code>https://api.secureworks.com/api/ticket/v3</code>
username	Yes	<code>user@example.com</code>
password	Yes	“

Config	Required	Example
query_ticket_grouping_types	Yes	INCIDENT:SECURITY
query_limit	Yes	10
polling_interval	Yes	600
close_codes	No	Authorized Activity,Confirmed Security Incident,Duplicate,Incident Misidentified,Inconc
template_file_escalate	No	“
template_file_close	No	“
template_file_update	No	“
cafile	No	“

- **Save** and **Close** the app.config file.
- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-secureworks-ctp
```
- **Run** resilient-circuits or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

Uninstall

- SSH into your Integration Server.
- **Uninstall** the package:

```
$ pip uninstall fn-secureworks-ctp
```
- Open the config file, scroll to the [fn_secureworks_ctp] section and remove the section or prefix **#** to comment out the section.
- **Save** and **Close** the app.config file.

Custom Layouts

Customize Secureworks CTP and Close Incident Layouts to provide Secureworks specific information in the Resilient UI.

Secureworks CTP Layout Tab

Create a Secureworks CTP custom incident tab so that you can view Secureworks CTP ticket information in one place.

- Go to the Customizations Settings -> Layouts tab.
- Click the Incident Tabs menu item on the left.
- Click the Add Tab button.
- Enter Secureworks CTP in Add a Tab popup and click Add.

The screenshot shows the Resilient Sysadmin interface. The top navigation bar includes 'Dashboards', 'Inbox', 'Incidents', and a 'Create' dropdown. The main header is 'Customization Settings' with tabs for 'Layouts', 'Rules', 'Scripts', 'Workflows', 'Functions', 'Message Destinations', 'Phases & Tasks', 'Incident Types', 'Breach', and 'Artifacts'. The 'Layouts' tab is active, showing 'Incident: Manage Tabs'. On the left, a sidebar lists 'Incident Tabs' with a sub-menu 'Manage Tabs' containing 'Summary Section', 'Tasks', 'Details', 'Breach', 'Notes', 'Members', 'News Feed', 'Attachments', 'Stats', 'Timeline', 'Artifacts', 'Email', 'Exchange Online', and 'Add Tab'. A red arrow points to the 'Add Tab' button. The main area shows a grid of tabs: 'Tasks', 'Details', 'Breach', 'Notes', 'Members', 'News Feed', 'Attachm...', 'Stats', 'Timeline', and 'Artifacts'. Below the grid, there is a 'Tab Text' field with 'Tasks' and a 'Tab Visible' section with radio buttons for 'Yes' (selected), 'No', and 'Conditional'. 'Cancel' and 'Save' buttons are at the top right.

- Next, search for the Secureworks CTP (scwx) custom incident fields in the Fields search bar.
- Drag Secureworks custom incidents fields on to the layout in the center of the screen.
- Click Save.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

New Incident Wizard >

Incident Tabs ▾

Manage Tabs >

Summary Section >

Tasks >

Details >

Breach >

Notes >

Members >

News Feed >

Attachments >

Stats >

Timeline >

Artifacts >

Email >

Exchange Online >

✓ Secureworks CTP >

+ Add Tab

Close Incident >

Incident: Secureworks CTP

Delete Save

Secureworks CTP ticketId x

Secureworks CTP ticketType x

Secureworks CTP groupingType x

Secureworks CTP requestType x

Secureworks CTP dateCreated x

Secureworks CTP priority x

Secureworks CTP closeCode x

Secureworks CTP category x

Secureworks CTP categoryClass x

Secureworks CTP categoryItem x

Secureworks CTP categoryType x

Secureworks CTP contact ID x

Secureworks CTP contact name x

Secureworks CTP source x

Secureworks CTP status x

Add Field

Fields ⓘ

sec

Secureworks CTP category

Secureworks CTP categoryClass

Secureworks CTP categoryItem

Secureworks CTP categoryType

Secureworks CTP closeCode

Secureworks CTP contact ID

Secureworks CTP contact name

Secureworks CTP dateCreated

Secureworks CTP groupingType

Add Table

Data Tables ⓘ

Exchange Online Message Query Results

Views ⓘ

Address

Analytics Widget

Artifacts Widget

Close Incident Layout Tab

Modify the Close Incident tab so the the Secureworks close code can be selected from the Close Incident popup from Resilient.

- Go to the Customizations Settings -> Layouts tab.
- Click the Close Incident menu item on the left as shown in the screenshot below.

resilient Dashboards ▾ Inbox Incidents **Create ▾** Resilient Sysadmin resilient

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

New Incident Wizard >
Incident Tabs >
Close Incident >

New Wizard

Add Step Save

Describe the Incident

Describe and Name the Incident

Incident Type

NIST Attack Vectors

Incident Disposition

Description

Name

Date and Location

Date Occurred

Date Discovered

HTML Block

Address

Fields

Search...

Address

Alberta Health Risk Assessment

Assessed Liability

City

Country/Region

Created By

Criminal Activity

Customizations Field (internal)

Data Encrypted

Views

Address

Criminal Status View

Data Types

Employee Involvement View

GDPR Form

- Next, search for the Secureworks CTP Close Code custom incident fields in the Fields search bar.
- Drag the Secureworks CTP Close Code onto the Close Incident layout tab.

resilient Dashboards ▾ Inbox Incidents **Create ▾** Resilient Sysadmin resilient

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

New Incident Wizard >
Incident Tabs >
Close Incident >

Incident Close

Save

Secureworks CTP Close Code

Fields

close

Date Closed

Secureworks CTP Close Code

Data Tables

Exchange Online Message Query Results

Blocks

Header

HTML

Troubleshooting

There are several ways to verify the successful operation of a function.

Resilient Action Status

- When viewing an incident, use the Actions menu to view **Action Status**.
- By default, pending and errors are displayed.

- Modify the filter for actions to also show Completed actions.
- Clicking on an action displays additional information on the progress made or what error occurred.

Resilient Scripting Log

- A separate log file is available to review scripting errors.
- This is useful when issues occur in the pre-processing or post-processing scripts.
- The default location for this log file is: `/var/log/resilient-scripting/resilient-scripting.log`.

Resilient Logs

- By default, Resilient logs are retained at `/usr/share/co3/logs`.
- The `client.log` may contain additional information regarding the execution of functions.

Resilient-Circuits

- The log is controlled in the `.resilient/app.config` file under the section `[resilient]` and the property `logdir`.
- The default file name is `app.log`.
- Each function will create progress information.
- Failures will show up as errors and may contain python trace statements.

Support

Name	Version	Author	Support URL
fn_secureworks_ctp	1.0.0	Resilient Labs	https://ibm.biz/resilientcommunity