User Guide: Secureworks CTP Functions for IBM Resilient v1.0.0

Table of Contents

Key Features

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.

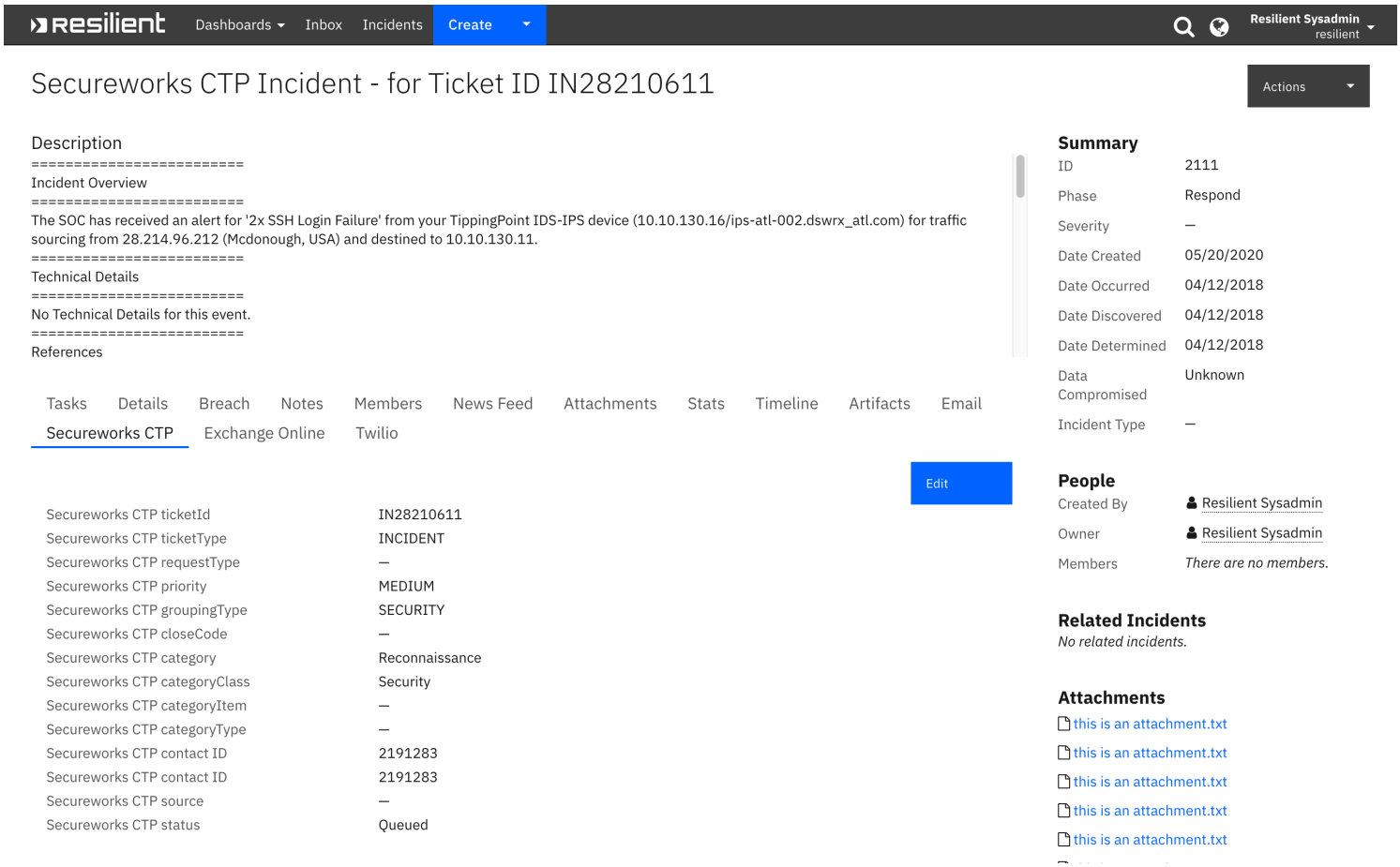
CTP is used with the Secureworks SOC team when they find a security issue that needs to be communicated to the customer. The issues can be informational, research-based or require proscriptive actions by the customer. Secureworks CTP provides a “ticket-like” interface that allows you acknowledge, add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

The Secureworks CTP integration implements the following functionality in the Resilient platform:

- 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.

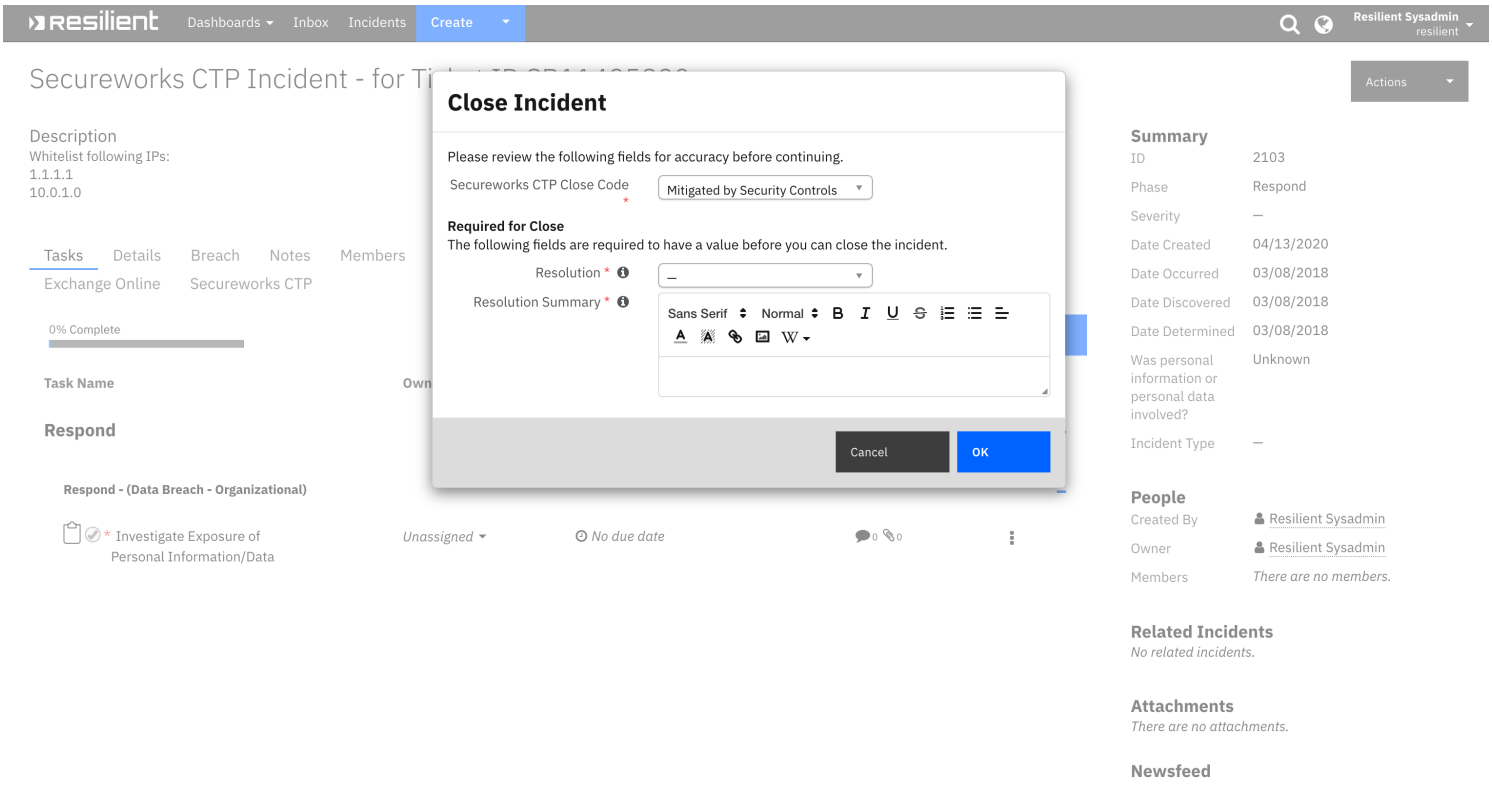
Integration Flow for Ticket Management

The primary use case for the Secureworks CTP integration with the Resilient platform is to bring Secureworks CTP tickets of interest into the Resilient platform for further inspection and migitation. Below is a screenshot of a sample Secureworks CTP incident with the incident tab displayed:



Once a Secureworks incidents is resolved, the incident is closed in the Resilient platform by the user via the Actions menu Close Incident item, triggering the close menu popup to appear as depicted below. Select the Secureworks CTP close code, the Resilient Resolution ID and enter the Resolution Summary. Once the user clicks OK, the Secureworks CTP Close Ticket automatic rule is activated, starting the Example Secureworks Close Ticket workflow. The Secureworks CTP close code and the Resolution summary are sent back to Secureworks when the function is activated to close the corresponding Secureworks Ticket in Secureworks.

NOTE: The integration uses default Secureworks CTP close codes that appear in the Close Incident popup select input field. The defaults can be overridden in the app.config by setting close_code parameter.



If the Secureworks ticket is closed in Secureworks portal, the poller detects this in Resilient and closes the corresponding incident. The poller uses a default jinja template for closing an incident in this case. The jinja template defines the incident fields and values necessary at incident closure. The user can customize their own template if needed and specify the file location in the template_file_close parameter in the app.config file.

Poller

The integration poller runs continuously while the integration is running.

- The poller creates a Resilient incident for each Secureworks CTP ticket returned matching the search criteria.
- The user can specify which of the following Secureworks CTP ticket types to be searched during polling:
  - SERVICE_REQUEST
  - INCIDENT
  - CHANGE
- The user can specify the following Secureworks CTP ticket groups to searched for during polling:
  - REQUEST
  - CHANGE
  - HEALTH

    - SECURITY
- The poller adds Secureworks CTP ticket workLogs and attachments as incident notes and attachments in the corresponding Resilient incident.
- Poller interval can be set in the app.config to specify how often the integration checks for updated tickets from Secureworks CTP. An interval value of zero will turn off the poller.
- The poller closes a Resilient incident if the corresponding Secureworks ticket is closed in the Securewokrs portal.

Custom Incident Fields

The following custom incident fields are available in the integration and can be viewed on the Secureworks CTP custom layout tab. The Secureworks CTP Install Guide describes how to create the layout in the Resilient Platform UI. A jinja template file is used to map the Securework ticket fields to a field in Resilient. The user can add more fields and customizations using their own jinja escalate template file defined in the app.config template_file_escalate parameter.

Resilient custom incident field	Secureworks CTP Ticket field
scwx_ctp_category	category
scwx_ctp_category_class	categoryClass
scwx_ctp_category_item	categoryItem
scwx_ctp_category_type	categoryType
scwx_ctp_close_code	closeCode
scwx_ctp_contact_id	contact: id
scwx_ctp_contact_name	contact: name
scwx_ctp_date_created	dateCreated
scwx_ctp_grouping_type	groupingType
scwx_ctp_priority	priority
scwx_ctp_request_type	requestType
scwx_ctp_source	source
scwx_ctp_status	status

Resilient custom incident field	Secureworks CTP Ticket field
scwx_ctp_ticket_id	ticketId
scwx_ctp_ticket_type	ticketType

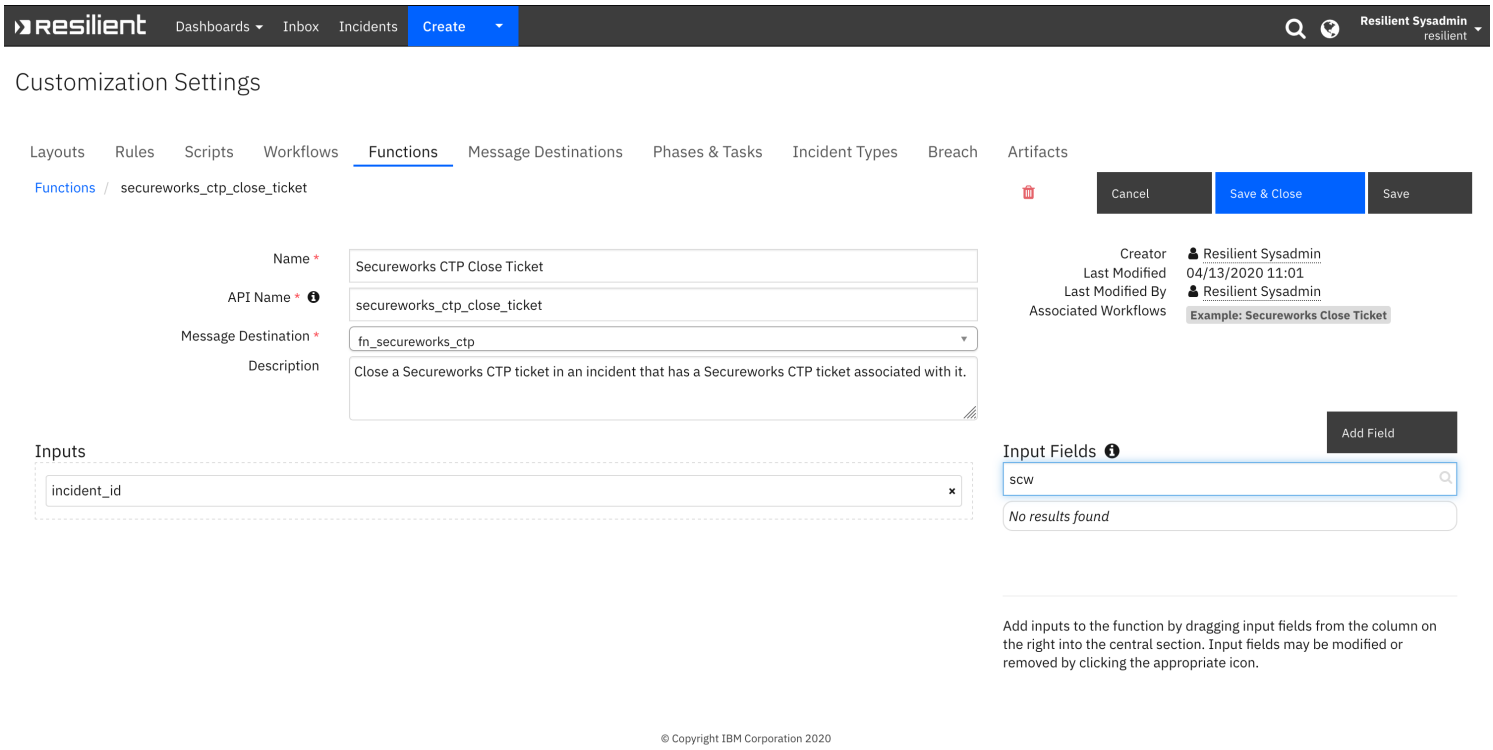
The poller will update custom incident fields in Resilient when Secureworks updates a ticket. To update the custom incident fields, the poller renders a default update template that contains the following Resilient custom incident fields which are the ones mostly to be changed or updated by Secureworks:

Resilient custom incident field	Secureworks CTP Ticket field
scwx_ctp_contact_id	contact: id
scwx_ctp_contact_name	contact: name
scwx_ctp_priority	priority
scwx_ctp_status	status

The user can add more fields and customizations using their own jinja update template file defined in the app.config template_file_update parameter.

Function - Secureworks CTP Close Ticket

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



- ▶ Inputs:
- ▶ Outputs:
- ▶ Workflows

Rules

Rule Name	Object	Workflow Triggered
Secureworks CTP Close Ticket	incident	`example_secureworks_close_ticket`

- ▶ Example Rule: