

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

Table of Contents

- [Key Features](#)
- [Poller](#)
- [Function - Secureworks CTP Close Ticket](#)
- [Rules](#)

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.

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 mitigation. Below is a screenshot of a sample Secureworks CTP incident with the incident tab displayed:

Resilient

Dashboards ▾InboxIncidentsCreate ▾

Resilient Sysadminresilient

Q🔍

Secureworks CTP Incident - for Ticket ID CH1004856

Actions ▾

Description

#format_version=1.0##

Block IP Request for Firewall
NOTE: Please do not modify this information or format

#Request information
Requester=contact@gmail.com
Device_Name=CiscoExternalASA.DSWRX_ATL.COM / 10.10.130.110
Device_site=SecureWorks Demo Customer
Severity=Emergency Deployment

TasksDetailsBreachNotesMembersNews FeedAttachmentsStatsTimelineArtifactsEmail

Exchange OnlineSecureworks CTP

Secureworks CTP ticketIdCH1004856
Secureworks CTP ticketTypeCHANGE
Secureworks CTP groupingTypeCHANGE
Secureworks CTP requestTypeFirewall Change Request - Block/Allow
Secureworks CTP priority—
Secureworks CTP dateCreated1469457607000
Secureworks CTP Close Code—

Edit

Summary

ID2102
PhaseRespond
Severity—
Date Created04/13/2020
Date Occurred07/25/2016
Date Discovered07/25/2016
Date Determined07/25/2016
Was personal information or personal data involved?Unknown
Incident Type—

People

Created ByResilient Sysadmin
OwnerResilient Sysadmin
MembersThere are no members.

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

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.

The screenshot displays the Resilient web interface. At the top, a navigation bar includes 'Dashboards', 'Inbox', 'Incidents', and a 'Create' button. The main header shows 'Secureworks CTP Incident - for T...' and a user profile 'Resilient Sysadmin resilient'. A modal dialog titled 'Close Incident' is centered on the screen. It prompts the user to review fields before continuing. The 'Secureworks CTP Close Code' is set to 'Mitigated by Security Controls'. Below, the 'Required for Close' section lists 'Resolution' and 'Resolution Summary' as required fields. The 'Resolution' dropdown is currently empty. The 'Resolution Summary' field has a rich text editor with options for font face (Sans Serif), size (Normal), bold, italic, underline, link, unlink, and list. The background shows an incident detail view for 'Exchange Online' with a 'Secureworks CTP' breach. The right sidebar contains sections for 'Summary' (ID: 2103, Phase: Respond, Date Created: 04/13/2020), 'People' (Created By: Resilient Sysadmin, Owner: Resilient Sysadmin), 'Related Incidents' (No related incidents), 'Attachments' (There are no attachments), and 'Newsfeed'.

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.

Function - Secureworks CTP Close Ticket

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

resilient

Dashboards ▾InboxIncidentsCreate ▾

Q

🌐

Resilient Sysadmin
resilient ▾

Customization Settings

LayoutsRulesScriptsWorkflowsFunctionsMessage DestinationsPhases & TasksIncident TypesBreachArtifacts

Functions / secureworks_ctp_close_ticket

Cancel

Save & Close

Save

Name *

Secureworks CTP Close Ticket

API Name * ⓘ

secureworks_ctp_close_ticket

Message Destination *

fn_secureworks_ctp ▾

Description

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

Inputs

incident_id

×

Creator

Resilient Sysadmin

Last Modified

04/13/2020 11:01

Last Modified By

Resilient Sysadmin

Associated Workflows

Example: Secureworks Close Ticket

Input Fields ⓘ

scw

Q

No results found

Add Field

Add inputs to the function by dragging input fields from the column on the right into the central section. Input fields may be modified or removed by clicking the appropriate icon.

- Inputs:
- Outputs:
- Workflows

Rules

Rule Name	Object	Workflow Triggered
Secureworks CTP Close Ticket	incident	example_secureworks_close_ticket

- Example Rule: