

 README.md

User Guide: fn_proofpoint_tap_v1.0.0

Table of Contents

- [Key Features](#)
- [Function - Proofpoint TAP Get Campaign](#)
- [Function - Proofpoint TAP Get Forensics](#)
- [Custom Fields](#)
- [Rules](#)

Key Features

- Poller
- Get Forensics
- Get Campaign

Poller

Threaded Poller which runs continuously while the integration is running.

- Polls Proofpoint TAP events for all clicks and messages relating to known threats within the specified time period.
- Filters the events based on their classification threat type such as malware, phish, spam, and impostor. The chosen type_filter is defined in the app.config file.
- Filters the type of events to import based on the respective threat score that is configured in the app.config file.
- Creates Incidents in the Resilient platform based on the events.
- Adds artifacts to incidents in the Resilient platform corresponding to Proofpoint TRAP Campaign ID and Threat ID.

Resilient

Dashboards

Simulations

Incidents

Create

All

Search

Orchestration Engine
Test Organization

Proofpoint TAP Event: 2fab740f143fc1aa4c1cd0146d334c5593b142...

Actions

Description

TAP Event Kind: messagesBlocked
Classification: malware
Sender: e99d7ed5580193f36a51f597bc2c0210@evil.zz
Subject: Please find a totally safe invoice attached.
From address: badguy@evil.zz
From header: 'A. Badguy' <badguy@evil.zz>
Header Reply To: None
Header To: 'Clark Kent' <clark.kent@pharmtech.zz>; 'Diana Prince' <diana.prince@pharmtech.zz>
Recipient: ['clark.kent@pharmtech.zz', 'diana.prince@pharmtech.zz']
Sender IP: 192.0.2.255
Click To N/A

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

Email

0% Complete

Filter: Active

Selected

Add Task

Task Name	Owner	Due Date	Flags	Actions
Engage				
Initial Triage	Unassigned	No due date		...
Interview key individuals	Unassigned	No due date		...
Notify internal management chain (preliminary)	Unassigned	No due date		...
Determine if inappropriate	Unassigned	No due date		...

Summary

ID2147

PhaseEngage

Severity-

Date Created10/31/2019

Date Occurred-

Date Discovered06/24/2016

Data CompromisedUnknown

Incident TypeMalware

People

Created ByOrchestration Engine

OwnerOrchestration Engine

MembersThere are no members.

Related Incidents

#2146 Proofpoint TAP Event: malware

Attachments

There are no attachments.

Function - Proofpoint TAP Get Forensics

Function pulls detailed forensic evidence about individual threats or campaigns observed in their environment. The results are saved in a Note.

Resilient

Dashboards

Simulations

Incidents

Create

All

Search

Orchestration Engine
Test Organization

Customization Settings

Layouts

Rules

Scripts

Workflows

Functions

Message Destinations

Phases & Tasks

Incident Types

Breach

Artifacts

Functions / fn_pp_forensics

Name *Proofpoint TAP Get Forensics

API Name *fn_pp_forensics

Message Destination *Proofpoint TAP

DescriptionFunction pulls detailed forensic evidence about individual threats or campaigns observed in their environment.

CreatorOrchestration Engine

Last Modified09/17/2019 15:20

Last Modified ByOrchestration Engine

Associated Workflows

Example: Proofpoint TAP - Aggregate Forensics for Th...

Example: Proofpoint TAP - Get Forensics by Campaig...

Example: Proofpoint TAP - Aggregate Forensics for C...

Inputs

proofpoint_campaign_id

proofpoint_threat_id

proofpoint_malicious_flag

proofpoint_aggregate_flag

Input Fields

Search...

incident_id

proofpoint_aggregate_flag

proofpoint_campaign_id

proofpoint_malicious_flag

proofpoint_threat_id

test

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:

Name	Type	Required	Example	Tooltip
------	------	----------	---------	---------

Name	Type	Required	Example	Tooltip
proofpoint_aggregate_flag	boolean	No	–	A boolean value, defaulting to false. May optionally be used with the threatId parameter. It cannot be used with the campaignId parameter. If false, aggregate forensics for that specific threat identifier will be returned. If true AND if the threat has been associated with a campaign, aggregate forensics for the entire campaign are returned. Otherwise, aggregate forensics for the individual threat are returned.
proofpoint_campaign_id	text	No	–	A string containing a campaign identifier.
proofpoint_malicious_flag	boolean	No	–	Show malicious results only
proofpoint_threat_id	text	No	–	A string containing a threat identifier.

▼ Workflows:

There are three Workflows for this function:

- Example: Proofpoint TAP - Aggregate Forensics for Threat

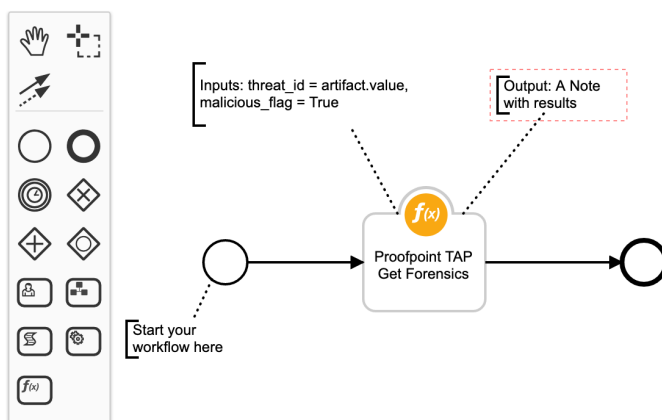
Workflow imports additional forensic information based on the given threat identifier. Aggregate forensics for the given threat identifier are returned and additionally filtered to include malicious results only.

Customization Settings

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

Workflows / Example: Proofpoint TAP - Aggregate Forensics for Threat

Name *	Example: Proofpoint TAP - Aggregate Forensics for Threat	Created By
API Name * ⓘ	get_forensics_by_threat_id	Last Modified By
Description	Workflow imports additional forensic information based on the given threat identifier. Aggregate forensics for the given threat identifier are returned and additionally filtered to include malicious results only.	Last Modified
Object Type *	Artifact	Associated Rule



- Example: Proofpoint TAP - Get Forensics by Campaign ID

Workflow imports additional forensics information based on the given campaign identifier.

Customization Settings

Name *

API Name * ⓘ

Description

Object Type *

Example: Proofpoint TAP - Get Forensics by Campaign ID

get_forensics_by_campaign_id

Workflow imports additional forensics information based on the given campaign identifier.

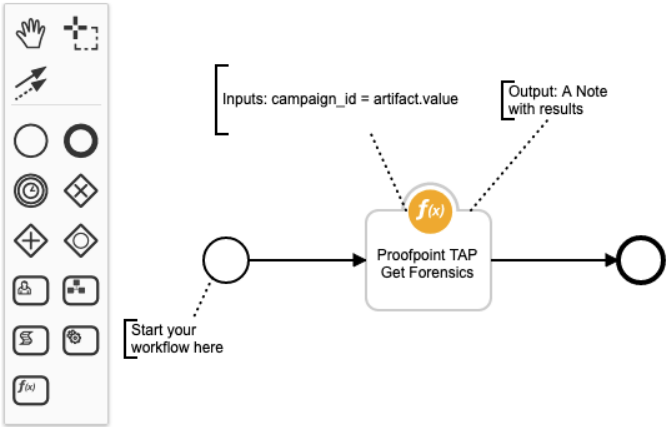
Artifact

Crea

Last Modifi

Last Modified

Associated Ru



- Example: Proofpoint TAP - Aggregate Forensics for Campaign

Workflow imports additional forensic information based on the given threat identifier. If the threat has been associated with a campaign, aggregate forensics for the entire campaign are returned. Otherwise aggregate forensics for the individual threat are returned.

Customization Settings

LayoutsRulesScriptsWorkflowsFunctionsMessage DestinationsPhases & TasksIncident TypesBreachArtifacts

Workflows / Example: Proofpoint TAP - Aggregate Forensics for Campaign

Name *

API Name * ⓘ

Description

Object Type *

Example: Proofpoint TAP - Aggregate Forensics for Campaign

get_aggregate_forensics_by_threat_id

Workflow imports additional forensic information based on the given threat identifier. If the threat has been associated with a campaign, aggregate forensics for the entire campaign are returned. Otherwise aggregate forensics for the individual threat are returned.

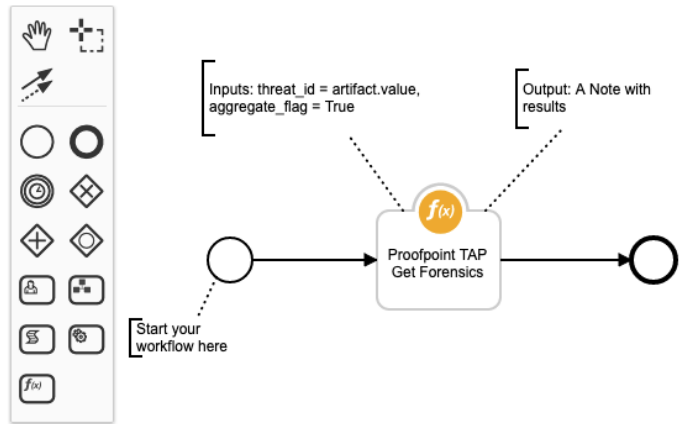
Artifact

Creator

Last Modified By

Last Modified By

Associated Rule:



▼ Outputs:

```
results {
  "inputs": {
    "campaign_id": None,
    "threat_id": "355e7ff321fc141e057c2ad6a593a9a264ed910065fe6c099f5cd0e097824474",
    "aggregate_flag": None,
    "malicious_flag": True
  },
  "success": True,
  "data": [
    "Malicious content dropped during execution\nType: behavior\nMalicious: True\nNote: Malicious content dropped duri",
    "Malicious content dropped during execution\nType: behavior\nMalicious: True\nNote: Malicious content dropped duri",
    "Malicious attachment with url: http://skillededucators.com\nType: url\nMalicious: True\nNote: \nOS: Win7\nURL: http",
    "Malicious attachment with url: http://skillededucators.com\nType: url\nMalicious: True\nNote: \nOS: Win7\nURL: http"
  ]
}
```

▼ Example Pre-Process Script:

```
inputs.proofpoint_threat_id = artifact.value
inputs.proofpoint_malicious_flag = True
```

▼ Example Post-Process Script:

```
# results is a Dictionary and data is a List
if results and results.get("data"):
    incident.addNote("\n\n".join(results.get("data")))
else:
    incident.addNote("No malicious Forensics information found for artifact {}".format(artifact.value))
```

Function - Proofpoint TAP Get Campaign

Function pulls specific details about campaigns including description, the actor, malware family, techniques and the threat variants associated with the campaign. The results are saved in a Note.

Resilient

Dashboards ▾SimulationsIncidentsCreate

All ▾Search

Orchestration Engine
Test Organization ▾

Customization Settings

LayoutsRulesScriptsWorkflowsFunctionsMessage DestinationsPhases & TasksIncident TypesBreachArtifacts

Functions / fn_pp_campaign

Name *Proofpoint TAP Get Campaign

API Name * ⓘfn_pp_campaign

Message Destination *Proofpoint TAP

DescriptionFunction pulls specific details about campaigns including description, the actor, malware family, techniques and the threat variants associated with the campaign.

Inputs

proofpoint_campaign_id

CreatorOrchestration Engine

Last Modified09/17/2019 15:20

Last Modified ByOrchestration Engine

Associated WorkflowsExample: Proofpoint TAP - Get Campaign

Input Fields ⓘ

Add Field

Search...

incident_id

proofpoint_aggregate_flag

proofpoint_campaign_id

proofpoint_malicious_flag

proofpoint_threat_id

test

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:

Name	Type	Required	Example	Tooltip
proofpoint_campaign_id	text	No	–	A string containing a campaign identifier.

▼ Workflows:

There is one Workflow for this function:

- Example: Proofpoint TAP - Get Campaign

Workflow imports detailed information for given campaign identifier, including description, the actor, malware family, techniques and the threat variants associated with the campaign.

Customization Settings

Layouts

Rules

Scripts

Workflows

Functions

Message Destinations

Phases & Tasks

Incident Types

Breach

Art

Workflows / Example: Proofpoint TAP - Get Campaign

Name *

API Name * ⓘ

Description

Object Type *

Example: Proofpoint TAP - Get Campaign

get_campaign_flow

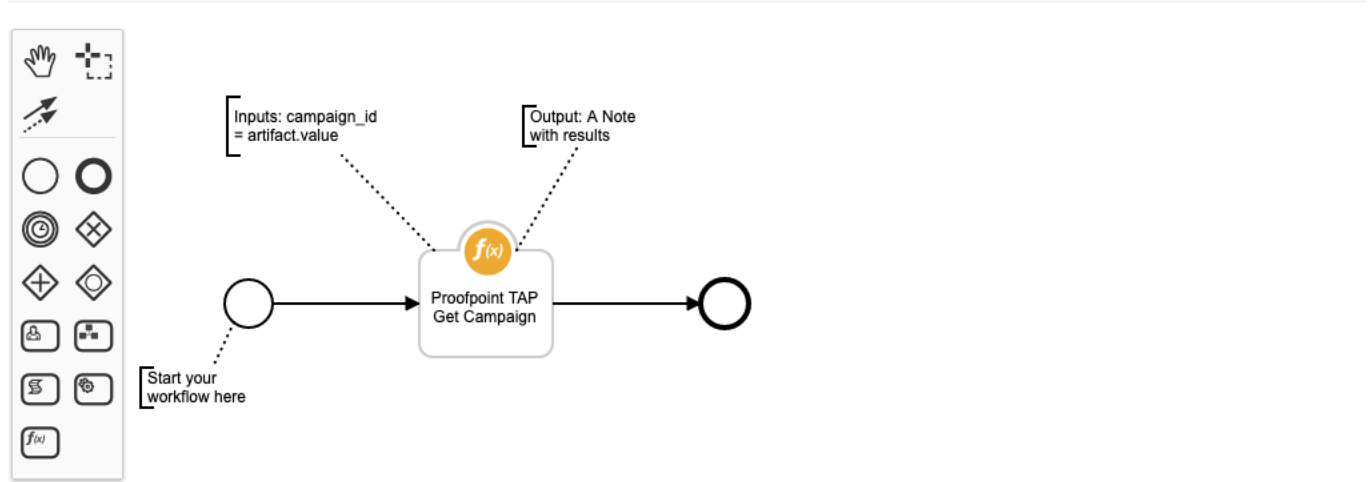
Workflow imports detailed information for given campaign identifier, including description, the actor, malware family, techniques and the threat variants associated with the campaign.

Artifact

L

Last

Asso



▼ Example Pre-Process Script:

```
inputs.proofpoint_campaign_id = artifact.value
```

▼ Example Post-Process Script:

```
# results and results.data are both a Dictionary
if results and results.get("data"):
    incident.addNote(str(results.get("data")))
else:
    incident.addNote("No Campaign information found for artifact {}".format(artifact.value))
```

Custom Fields

Label	API Access Name	Type	Prefix	Placeholder	Tooltip
Proofpoint Campaign ID	campaignId	text	properties	-	A string containing a campaign identifier.

Label	API Access Name	Type	Prefix	Placeholder	Tooltip
Proofpoint Message ID	messageID	text	properties	-	A string containing a threat identifier.

Rules

Rule Name	Object	Workflow Triggered
Example: Proofpoint TAP - Aggregate Forensics by Threat ID and Show Malicious Results Only	artifact	get_forensics_by_threat_id
Example: Proofpoint TAP - Get Campaign Information by Campaign ID	artifact	get_campaign_flow
Example: Proofpoint TAP - Get Forensics by Campaign ID	artifact	get_forensics_by_campaign_id
Example: Proofpoint TAP - Aggregate Forensics for Entire Campaign Associated with Threat ID	artifact	get_aggregate_forensics_by_threat_id