README.md

Proofpoint TAP Functions for IBM Resilient

Release Notes

What's new in this Beta

- Created two new custom Artifact Types for Threat ID and Campaign ID and filtered Rules based on the Artifact type.
- If Threat ID or Campaign ID don't exist in Proofpoint Tap system, instead of ending the Workflow with an Error, a Note is created with a message explaining the user Threat ID or Campaign ID cannot be found.
- When Get Campaign Workflow is completed a Note is created with the name of the Workflow and some basic information about the Campaign. Detailed Campaign information is saved in Proofpoint TAP Campaign Object Details Data Table. Additionally a Script is available for the Data Table to create an Artifact based on chosen row.
- Get Forensics function has an additional input parameter incident_id which is used for creating Forensics Report Attachment.
- Results of all three Workflows for Get Forensics function are saved in a Note and an Attachment.
- Aggregate Forensics for entire campaign now returns malicious results only.

What's new in the Beta 11/1/2019

- Fixed a bug for Get Forensics function where adding a Note caused the Workflow a long time to complete.
- Improved the poller logic and filtering based on score threshold.
- Improved the documentation.
- Renamed the Rules and Workflows for clarity.
- Updated both jinja2 templates to extract more information from the endpoint.
- NOTE: If using both Proofpoint TAP and TRAP integrations, TAP polls events and TRAP polls incidents. One could be more granular than the other; therefore, you might not need to use both pollers at the same time.

Overview

Proofpoint Targeted Attack Protection (TAP) helps you stay ahead of attackers with an innovative approach that detects, analyzes and blocks advanced threats before they reach your inbox. This includes ransomware and other advanced email threats delivered through malicious attachments and URLs.

The Proofpoint TAP function package provides the following features:

- Poll detailed information about several types of TAP events in a SIEM-compatible, vendor-neutral format. This includes Blocked or permitted clicks to threats recognized by URL Defense and Blocked or delivered messages that contain threats recognized by URL Defense or Attachment Defense are exposed.
- Get detailed forensic evidences about individual threats or campaigns observed in their environment. These evidences could be used as indicators of compromise to confirm infection on a host, as supplementary data to enrich and correlate against other

security intelligence sources, or to orchestrate updates to security endpoints to prevent exposure and infection.
- Pull specific details about campaigns, including their description, the actor, malware family, and techniques associated with the campaign and the threat variants which have been associated with the campaign.

Requirements

- Resilient platform `>= v32`
- An Integration Server running `resilient_circuits>=32.0.186`
  - To set up an Integration Server see: ibm.biz/res-int-server-guide

Installation

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

```
$ unzip fn_proofpoint_tap-x.x.x.zip
```

- **Change Directory** into the unzipped directory:

```
$ cd fn_proofpoint_tap-x.x.x
```

- **Install** the package:

```
$ pip install fn_proofpoint_tap-x.x.x.tar.gz
```

- Import the **configurations** into your app.config file:

```
$ resilient-circuits config -u
```

- Import the fn_proofpoint_tap **customizations** into the Resilient platform:

```
$ resilient-circuits customize -y -l fn-proofpoint-tap
```

- Open the config file, scroll to the bottom and edit your fn_proofpoint_tap configurations:

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

Config	Required	Example	Description
base_url	Yes	`https://tap-api-v2.proofpoint.com/v2`	*URL and credentials to authenticate to Proofpoint TAP*
username	Yes	``	*URL and credentials to authenticate to Proofpoint TAP.*
password	Yes	``	*URL and credentials to authenticate to Proofpoint TAP.*

Config	Required	Example	Description
polling_interval	Yes	`5`	*How often, in minutes, to check for new events, 0 to turn off.*
startup_interval	No	`30`	*How long, in minutes (max 60) to check for previous events at startup.*
type_filter	No	`malware, phish, spam, impostor, all`	*Filtering a comma-separated list of types of events to import into the Resilient platform*
score_threshold	No	`50`	*Classification for the type of event to import based on the respective threat score.*
threat_template	No		*Jinja template to override default threat description format.*
forensics_template	No		*Jinja template to override default forensic format.*
cafile	No	`cafile=~/.resilient/tap/cert.cer`	*If required by Proofpoint.*
http_proxy	No	`http://proxyhost:8080`	*For access via a proxy.*
https_proxy	No	`https://proxyhost:8080`	*For access via a proxy.*

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

```
$ resilient-circuits selftest -l fn-proofpoint-tap
```

- **Run** resilient-circuits or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

Custom Layouts

- To use the functions, the Resilient playbook designer needs to create a new Incident tab containing the Proofpoint TAP Campaign Object Details Data Table. The examples in this guide assume that the incident tab is named Proofpoint TAP.
- Additionally there are two custom incident fields Proofpoint Campaign ID and Proofpoint Threat ID that you may show on a desired layout. These two fields get automatically populated by the Proofpoint TAP poller.

Uninstall

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

```
$ pip uninstall fn-proofpoint-tap
```

- Open the config file, scroll to the [fn_proofpoint_tap] section and remove the section or prefix `#` to comment out the section.
- **Save** and **Close** the app.config file.

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.

Timeout error

- If you receive a timeout error from the Proofpoint TAP endpoint while making a request, you can increase the default timeout value in the app.config file by adding this section:

```
[integrations]
timeout=60
```

Support

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