Resilient Circuits Components for function: fn_virustotal.

VirusTotal is an artifact enrichment solution.
Queries are possible for:

- IP Addresses,
- URLs,
- hashes,
- domains and
- files

Files and URLs may require additional time to complete their scans, so a link is returned to review the results at a later time.

Contents:

Message Destinations:

fn_virustotal

Functions:

VirusTotal

Workflows:

Example: VirusTotal Scan
Example: VirusTotal Scan (Attachment)

Rules:

Example: Virus Total
Example: Virus Total for Attachments

This template project was generated by

```
resilient-circuits codegen -p fn_virustotal -m
fn_virustotal –rule “Example: Virus Total” “Example: Virus
Total for Attachments”
```

To install in "development mode"

```
pip install -e fn_virustotal-<version>.tar.gz
```

After installation, the package will be loaded by resilient-circuits run.
To uninstall,

```
pip uninstall fn_virustotal
```

To package for distribution,

```
python ./fn_virustotal/setup.py sdist
```

Requirements:

- resilient-circuits

Installation:

Run the following command to import this function into IBM resilient

```
resilient-circuits customize
```

To configure this function run and following command

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

Then edit the app.config file, providing the api_token for the [fn_virustotal] section necessary to communicate with VirusTotal.