Bluecoat Site Review

Introduction

This function provides data enrichment on DNS Names and URLs available from Symantec WebPulse (formally Bluecoat) Site Review to enrich artifact values.

Installation

Install the function package by first unpacking the .zip file exposing the .tar.gz file.

To install in "development mode"

```
[sudo] pip install -e ./fn_bluecoat_site_review/
```

or to the python libraries

```
[sudo] pip install fn_bluecoat_site_review-1.0.0.tar.gz
```

To configure `app.conf`, run

```
resilient-circuits config [-c or -u] -l fn-bluecoat-site-review
```

To load Resilient with all the object definitions needed for use, run

```
resilient-circuits customize -l fn-bluecoat-site-review
```

After installation, the package will be loaded and executed with `resilient-circuits run`.

To uninstall:

```
[sudo] pip uninstall fn-bluecoat-site-review
```

Components

The following components are loaded into Resilient

- Function: Bluecoat Site Review Lookup
- Workflow: Example: Bluecoat Site Review Search
- Rule: Example: Bluecoat Site Review

The sample rule is enabled for DNS and URL type artifacts

Results

The resulting data is appended in the artifact's description field. Your process may parse and process the data differently. A sample note in the description field is:

```
Bluecoat Categorization: Suspicious, Spam
```

This is produced by the following post-processing script:

```
if isinstance(results.content['CategorizationResult']['categorization']['categorizati
on'],list):
  categorization_list = [categorization['name'] for categorization in results.content
['CategorizationResult']['categorization']['categorization']]
  categorization_name = u", ".join(categorization_list)
else:
  categorization_name = results.content['CategorizationResult']['categorization']['ca
tegorization']['name']

existing_description = artifact.description.content+'\n' if artifact.description else
 ""

artifact.description = u"{}Bluecoat Categorization: {}".format(existing_description,
categorization_name)
```

Below is a sample result from the function returning multiple categorizations:

Sample results


```
{
  'inputs': {
    u'incident_id': 2104,
    u'artifact_value': u'http://avts.vn/hejxjrzjys/3978861743009/OCRjH-YuO_VcE-MgR/'
  },
  'metrics': {
    'package': 'fn-bluecoat-site-review',
    'timestamp': '2019-03-25 19:28:28',
```

```
    'package_version': '1.0.0',
    'host': 'marks-mbp.cambridge.ibm.com',
    'version': '1.0',
    'execution_time_ms': 139
  },
  'success': True,
  'content': {
    u'CategorizationResult': {
      u'categorization': {
        u'categorization': [
          {
            u'num': u'92',
            u'name': u'Suspicious'
          },
          {
            u'num': u'101',
            u'name': u'Spam'
          }
        ]
      },
      u'locked': u'false',
      u'translatedCategories': {
        u'fr': [
          {
            u'num': u'92',
            u'name': u'Suspect (Suspicious)'
          },
          {
            u'num': u'101',
            u'name': u'Spam (Spam)'
          }
        ],
        u'de': [
          {
            u'num': u'92',
            u'name': u'Verd\xe4chtig (Suspicious)'
          },
          {
            u'num': u'101',
            u'name': u'Spam (Spam)'
          }
        ],
        u'zh': [
          {
            u'num': u'92',
```

```
      u'name': u'\u53ef\u7591 (Suspicious)'
    },
    {
      u'num': u'101',
      u'name': u'\u5783\u573e\u90ae\u4ef6 (Spam)'
    }
  ],
  u'zh_TW': [
    {
      u'num': u'92',
      u'name': u'\u53ef\u7591 (Suspicious)'
    },
    {
      u'num': u'101',
      u'name': u'\u5783\u573e\u90f5\u4ef6 (Spam)'
    }
  ],
  u'en': [
    {
      u'num': u'92',
      u'name': u'Suspicious'
    },
    {
      u'num': u'101',
      u'name': u'Spam'
    }
  ],
  u'ja': [
    {
      u'num': u'92',
      u'name': u'\u7591\u308f\u3057\u3044 (Suspicious)'
    },
    {
      u'num': u'101',
      u'name': u'\u30b9\u30d1\u30e0 (Spam)'
    }
  ],
  u'es': [
    {
      u'num': u'92',
      u'name': u'Sospechoso (Suspicious)'
    },
    {
      u'num': u'101',
      u'name': u'Spam (Spam)'
```

```
          }
        ]
      },
      u'url': u'http://avts.vn/hejxjrzjys/3978861743009/OCRjH-YuO_VcE-MgR/',
      u'rateDate': u"Last Time Rated/Reviewed: > {{days}} days {{legacy}}The URL subm
itted for review was rated more than {{days}} days ago.  The default setting for Syma
ntec SG clients to download rating changes is once a day.  There is no need to show r
atings older than this. Since Symantec's desktop client K9 and certain OEM partners u
pdate differently, ratings may differ from those of a Symantec SG as well as those pr
esent on the Site Review Tool.",
      u'followedUrl': None,
      u'lockedSpecialNote': None,
      u'threatriskLevelEn': None,
      u'linkable': u'false',
      u'resolvedDetail': {
        u'resolveEnabled': u'true',
        u'ipAddress': u'103.28.36.58'
      },
      u'securityCategoryIds': {
        u'securityCategoryIds': [
          u'43',
          u'102',
          u'44',
          u'92',
          u'18'
        ]
      },
      u'multipleMessage': None,
      u'suggestion': None,
      u'securityCategory': u'true',
      u'ratingDtsCutoff': u'7',
      u'multiple': u'false',
      u'unrated': u'false',
      u'curTrackingId': u'478710',
      u'ratingDts': u'OLDER',
      u'lockedMessage': None,
      u'threatriskLevel': None
    }
  },
  'raw': '{"CategorizationResult": {"categorization": {"categorization": [{"num": "92
", "name": "Suspicious"}, {"num": "101", "name": "Spam"}]}, "locked": "false", "trans
latedCategories": {"fr": [{"num": "92", "name": "Suspect (Suspicious)"}, {"num": "101
", "name": "Spam (Spam)"}], "de": [{"num": "92", "name": "Verd\\u00e4chtig (Suspiciou
s)"}, {"num": "101", "name": "Spam (Spam)"}], "zh": [{"num": "92", "name": "\\u53ef\\
u7591 (Suspicious)"}, {"num": "101", "name": "\\u5783\\u573e\\u90ae\\u4ef6 (Spam)"}],
```

```
 "zh_TW": [{"num": "92", "name": "\\u53ef\\u7591 (Suspicious)"}, {"num": "101", "name
": "\\u5783\\u573e\\u90f5\\u4ef6 (Spam)"}], "en": [{"num": "92", "name": "Suspicious"
}, {"num": "101", "name": "Spam"}], "ja": [{"num": "92", "name": "\\u7591\\u308f\\u30
57\\u3044 (Suspicious)"}, {"num": "101", "name": "\\u30b9\\u30d1\\u30e0 (Spam)"}], "e
s": [{"num": "92", "name": "Sospechoso (Suspicious)"}, {"num": "101", "name": "Spam (
Spam)"}]}, "url": "http://avts.vn/hejxjrzjys/3978861743009/OCRjH-YuO_VcE-MgR/", "rate
Date": "Last Time Rated/Reviewed: > {{days}} days {{legacy}}The URL submitted for rev
iew was rated more than {{days}} days ago.  The default setting for Symantec SG clien
ts to download rating changes is once a day.  There is no need to show ratings older
than this. Since Symantec\'s desktop client K9 and certain OEM partners update differ
ently, ratings may differ from those of a Symantec SG as well as those present on the
 Site Review Tool.", "followedUrl": null, "lockedSpecialNote": null, "threatriskLevel
En": null, "linkable": "false", "resolvedDetail": {"resolveEnabled": "true", "ipAddre
ss": "103.28.36.58"}, "securityCategoryIds": {"securityCategoryIds": ["43", "102", "4
4", "92", "18"]}, "multipleMessage": null, "suggestion": null, "securityCategory": "t
rue", "ratingDtsCutoff": "7", "multiple": "false", "unrated": "false", "curTrackingId
": "478710", "ratingDts": "OLDER", "lockedMessage": null, "threatriskLevel": null}}',
  'reason': None,
  'version': '1.0'
}
```