OpenCTI client for Python

Release 5.12.20

OpenCTI Project

Jan 22, 2024

CONTENTS:

The pycti library is designed to help OpenCTI users and developers to interact with the OpenCTI platform GraphQL API.

The Python library requires Python >= 3.

CHAPTER

ONE

GETTING STARTED

1.1 Installation

Please install the latest pycti version available from PyPI:

```
$ pip3 install pycti
```

1.2 Using the helper functions

The main class `OpenCTIApiClient` contains all what you need to interact with the platform, you just have to initialize it. If your OpenCTI instance requires mTLS, you can specify either the file path of the SSL .pem file, or provide a key-value pair representing the file paths to your cert and private key in a tuple with the *cert* parameter when initializing the *OpenCTIApiClient*. If you need to require the verification of the TLS certificate at the server, you can provide a boolean value for the *ssl_verify* parameter.

The following example shows how you create an indicator in OpenCTI using the python library with TLP marking and OpenCTI compatible date format.

```
from dateutil.parser import parse
from pycti import OpenCTIApiClient
from stix2 import TLP_GREEN

# OpenCTI API client initialization
opencti_api_client = OpenCTIApiClient("https://myopencti.server", "mysupersecrettoken")

# Define an OpenCTI compatible date
date = parse("2019-12-01").strftime("%Y-%m-%dT%H:%M:%SZ")

# Get the OpenCTI marking for stix2 TLP_GREEN
TLP_GREEN_CTI = opencti_api_client.marking_definition.read(id=TLP_GREEN["id"])

# Use the client to create an indicator in OpenCTI
indicator = opencti_api_client.indicator.create(
    name="C2 server of the new campaign",
    description="This is the C2 server of the campaign",
    pattern_type="stix",
    pattern="[domain-name:value = 'www.5z8.info']",
    x_opencti_main_observable_type="IPv4-Addr",
    valid_from=date,
```

(continues on next page)

(continued from previous page)

```
    update=True,
    markingDefinitions=[TLP_GREEN_CTI["id"]],
)
```

CHAPTER

TWO

PYCTI

2.1 Functions

- `get_config_variable()`: [summary]

2.2 Classes

- `AttackPattern`: Undocumented.
- `Campaign`: Undocumented.
- `CaseIncident`: Undocumented.
- `CaseRfi`: Undocumented.
- `CaseRft`: Undocumented.
- `Task`: Undocumented.
- `ConnectorType`: Create a collection of name/value pairs.
- `CourseOfAction`: Undocumented.
- `DataComponent`: Undocumented.
- `DataSource`: Undocumented.
- `ExternalReference`: Undocumented.
- `Feedback`: Undocumented.
- `Grouping`: Undocumented.
- `Identity`: Undocumented.
- `Incident`: Undocumented.
- `Indicator`: Main Indicator class for OpenCTI
- `Infrastructure`: Main Infrastructure class for OpenCTI
- `IntrusionSet`: Undocumented.
- `KillChainPhase`: Undocumented.
- `Label`: Undocumented.
- `Location`: Undocumented.
- `Malware`: Undocumented.

- `MalwareAnalysis`: Undocumented.
- `MarkingDefinition`: Undocumented.
- `Note`: Undocumented.
- `ObservedData`: Undocumented.
- `OpenCTIApiClient`: Main API client for OpenCTI
- `OpenCTIApiConnector`: OpenCTIApiConnector
- `OpenCTIApiWork`: OpenCTIApiJob
- `OpenCTIConnector`: Main class for OpenCTI connector
- `OpenCTIConnectorHelper`: Python API for OpenCTI connector
- `OpenCTIMetricHandler`: Undocumented.
- `OpenCTIStix2`: Python API for Stix2 in OpenCTI
- `OpenCTIStix2Splitter`: Undocumented.
- `OpenCTIStix2Update`: Python API for Stix2 Update in OpenCTI
- `OpenCTIStix2Utils`: Undocumented.
- `Opinion`: Undocumented.
- `Report`: Undocumented.
- `StixCoreRelationship`: Undocumented.
- `StixCyberObservable`: Undocumented.
- `StixNestedRefRelationship`: Undocumented.
- `StixCyberObservableTypes`: Create a collection of name/value pairs.
- `StixDomainObject`: Undocumented.
- `StixMetaTypes`: Create a collection of name/value pairs.
- `MultipleRefRelationship`: Create a collection of name/value pairs.
- `StixObjectOrStixRelationship`: Undocumented.
- `StixSightingRelationship`: Undocumented.
- `ThreatActor`: Main ThreatActor class for OpenCTI
- `ThreatActorGroup`: Main ThreatActorGroup class for OpenCTI
- `ThreatActorIndividual`: Main ThreatActorIndividual class for OpenCTI
- `Tool`: Undocumented.
- `Vulnerability`: Undocumented.
- `CustomObjectCaseIncident`: Case-Incident object.
- `CustomObjectTask`: Task object.
- `CustomObservableHostname`: Hostname observable.
- `CustomObservableUserAgent`: User-Agent observable.
- `CustomObservableCryptocurrencyWallet`: Cryptocurrency wallet observable.
- `CustomObservableText`: Text observable.

2.3 Variables

- STIX_EXT_MITRE
- STIX_EXT_OCTI_SCO
- STIX_EXT_OCTI

CHAPTER

THREE

INDICES AND TABLES

- genindex
- modindex
- search