Sixgill - Darkfeed ThreatConnect User Guide

Overview

Delivering the next generation of deep & dark web threat intelligence feeds, Sixgill tailors threat intelligence to customers' intelligence needs, maximizing effective mitigation and remediation. Using an agile collection methodology and its proprietary collection automation algorithm, Sixgill provides broad coverage of exclusive-access deep and dark web sources, as well as relevant surface web sources. Sixgill harnesses artificial intelligence and machine learning to automate the production cycle of cyber intelligence from monitoring through extraction to production - unleashing both existing platforms and teams' performance.

The Sixgill Darkfeed on ThreatConnect

Leverage the power of Sixgill to supercharge ThreatConnect with real-time Threat Intelligence indicators. Get IOCs such as domains, URLs, hashes, and IP addresses straight into the Threatconnect platform.

Configuration

To install the Sixgill app in your ThreatConnect instance, refer to the ThreatConnect System Administration Guide (Install and App and Feed Deployer) for more information or contact your ThreatConnect Customer Success or Sales Engineer.

Requirements

The above requirements must be met to ingest Sixgill Darkfeed IOCs into the ThreatConnect Platform:

1. Access to ThreatConnect instance
2. At least one ThreatConnect API user (See Creating User Accounts)
3. Sixgill Darkfeed API Key provisioned by Sixgill to authenticate requests to Sixgill SaaS
4. Sixgill Darkfeed app installed in ThreatConnect Instance. (See App Installation section)
5. Sixgill Darkfeed attributes properly configured in your ThreatConnect instance (See Attributes Configuration section)

Integration Description

This integration allows the ingestion of the threat intelligence data provided in the Darkfeed Threat Intelligence feeds into the ThreatConnect Platform. Sixgill Threat Intelligence is offered in 4 different feeds:

- Address - ip address
- domain-names
- Files (MD5, SHA1, SHA256 hashes)
- URL

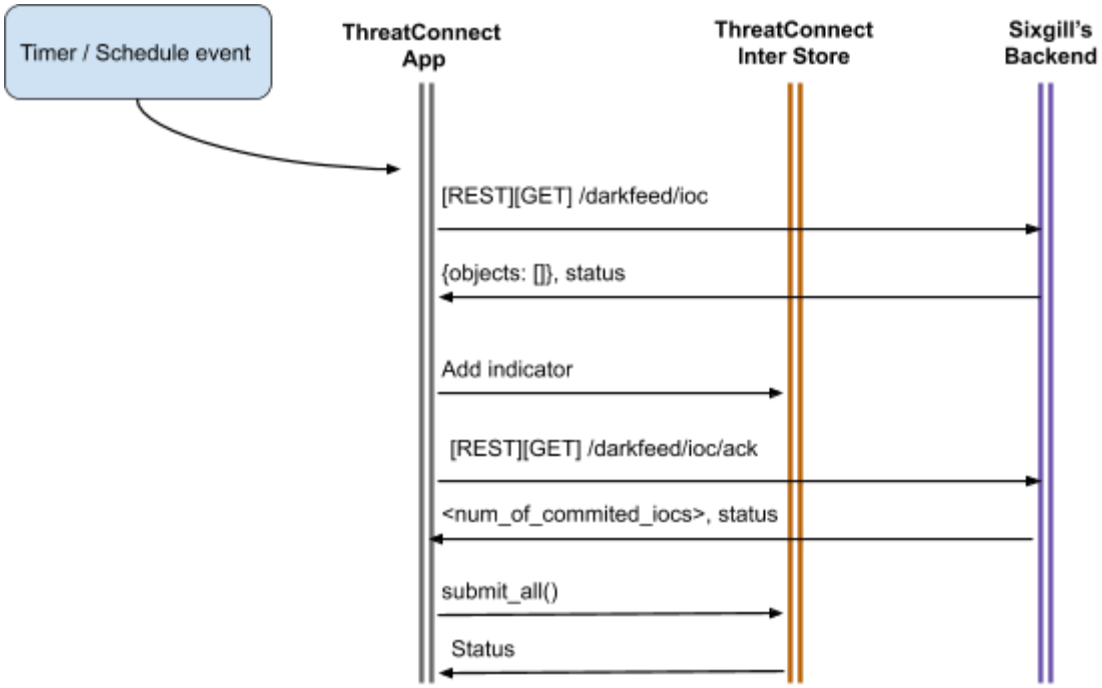
Using this integration, this data becomes usable within the ThreatConnect Platform as part of security activities.

Problem Statements

This integration addresses the following problems:

1. Customers of Sixgill that also currently use the ThreatConnect Platform have a desire to be able to ingest the Darkfeed IOC feed into the ThreatConnect Platform for analysis, collaboration, and action.
2. Existing customers and prospects of ThreatConnect may desire a unique Darkfeed IOC solution that provides a validated and curated set of high-rating, high-confidence indicators.

Integration Diagram



Integration Details

In the diagram above, the following sequence of events takes place:

1. A timer/scheduling event takes place in the ThreatConnect Platform to initiate the Darkfeed Runtime App.
2. An HTTP client requests the IOCs Intelligence payload. This request will include data about the specific intelligence requested along with the Darkfeed API Key for identification.
3. A response is generated by Sixgill's backend and returned to the sender in STIX V2.0 format.
4. The app converts the STIX item to Threatconnect indicator format.
5. The app enriches each indicator with additional tags, attributes.
6. In case Mitre information is included the client will add an additional tag based on References - Contributing MITRE ATT&CK Data
7. The IOCs are inserted using ThreatConnect TcEx Framework
8. An HTTP client requests the acknowledgment of the just-ingested IOCs Intelligence payload.
9. The iteration will end once no more new items to ingest

Consume IOCs Configuration

1. “tc_owner” [mandatory][string] - specifies who the owner of the data
2. “tc_log_level” [optional][enum] - allowed values: ["debug", "info", "warning", "error", "critical"]

Consume IOCs Data Mapping

The mapping of any data from the third-party platform to ThreatConnect should be documented in a table here.

Darkfeed Field	ThreatConnect Field	Possible Values	Notes
Indicator_type	Indicator_type	Address, File, URL	
ipv4-addr	Address	Any valid IP address	
url	URL	Any valid url in RFC3986 format	
file	File (MD5:SHA1:SHA256)	Any valid hash values for the given types	If a hash is unavailable, this field will be left blank in the ThreatConnect Platform.
domain-name	Host	A valid domain name	
Threat Rating (0-5)	Threat Rating (0-5)	Numbers 0 - 5	
Confidence	Confidence	Numbers 1 - 100	
labels	Tags	Any valid list of texts	If unavailable this field will be left empty

Consume IOCs Requirements

- ThreatConnect paid subscription (you cannot use TCOpen).
- At least one ThreatConnect API user.
- Sixgill's Darkfeed Client ID and Client secret (to be generated / delivered to the customer).

Consume IOCs Assumptions

- Indicator deprecation is handled automatically by the ThreatConnect Platform using the Deprecation Rules configured for the owner of Darkfeed indicators.
- There is no retry logic built into the Darkfeed Runtime App. Failures will be logged and must be investigated by an organization administrator.
- The owner for Darkfeed indicators on systems where the feed was deployed with the Feed Deployer Wizard will be "Sixgill Darkfeed Threat Intelligence".

Attribute configuration

The following configurations should be installed as part of the integration:

built-in attributes

Attribute name	Description	indicators
STIX ID	Threat actor that originally shared the indicator on the dark web.	Address, Host, File, URL
Eternal ID	The Id of the post in the Sixgill portal.	Address, Host, File, URL
Source	The name of the source in which the indicator appeared.	Address, Host, File, URL
Title	the actual title of the post/thread in which the indicator appeared.	Address, Host, File, URL
Description	Indicator description	Address, Host, File, URL

Observation Time	Indicator observation Time	Address, Host, File, URL
STIX Indicator Type	Indicator STIX V1.0 mapping	Address, Host, File, URL
Phase of Intrusion	Indicator phase of Intrusion	Address, Host, File, URL
Additional Analysis and Context	Indicator external reference information e.g Mitre, virusTotal	Address, Host, File, URL

Custom attributes

Attribute name	Description	indicators	Max length
Sixgill Actor	Threat actor that originally shared the indicator on the dark web.	Address, Host, File, URL	100
Sixgill Language	The language of the original post which included the indicator.	Address, Host, File, URL	100

ChangeLog

[1.0.2] - 01.04.2020

- Darkfeed indicators that are pushed are enriched with additional attributes:
    - STIX ID, Eternal ID, Source, Title, Description, Observation Time, STIX Indicator Type, Phase of Intrusion, Additional Analysis and Context, Sixgill Actor, Sixgill Language.
- Darkfeed indicators that includes Mitre Att&ck information, are added based on [References - Contributing MITRE ATT&CK Data] in the following format:

<mitre_attack_technique_id> - <mitre_attack_technique> - <tactic_abbr> - <data_abbr> - ATT&CK

[1.0.1] - 07.02.2020

- Darkfeed indicators are pushed into Threatconnect Platform.