Sixgill - DarkFeed ThreatConnect User Guide

Overview

The purpose of this document is to provide a detailed understanding of the integration between DarkFeed from Sixgill and the ThreatConnect Platform.

Sixgill's cyber threat intelligence solution focuses on customers' intelligence needs, helping them mitigate risk to their organizations more effectively and more efficiently. Using an agile and automatic collection methodology, Sixgill provides broad coverage of exclusive-access deep and dark web sources, as well as relevant surface web sources. Sixgill utilizes artificial intelligence and machine learning to automate the production cycle of cyber intelligence from monitoring through extraction to production.

Automatic monitoring of cybercrime, providing actionable intelligence from exclusive clear, deep and dark web forums and markets. Detecting, analyzing and mitigate financial fraud in near real time. IOCs include cyber Observables (suspicious IPs, domains, etc.)

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:

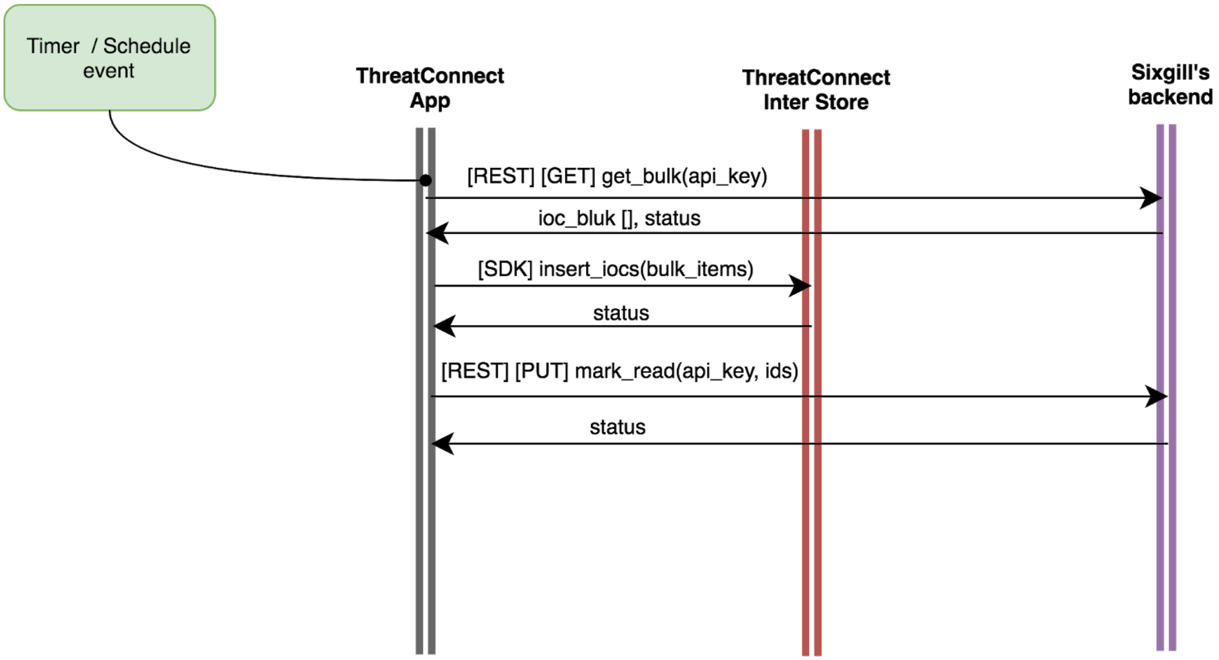
Addresses (C2 servers), MalwareDomains (C2 servers), Files (MD5, SHA1, and SHA256 hashes), CryptoWallets (SHA256 hashes). Using this integration, this data becomes usable within the ThreatConnect Platform as part of security activities.

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 feeds 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


Timer / Schedule event
ThreatConnect App
ThreatConnect Inter Store
Sixgill's backend
[REST] [GET] get_bulk(api_key)
ioc_bluk [], status
[SDK] insert_iocs(bulk_items)
status
[REST] [PUT] mark_read(api_key, ids)
status

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
4. The IOCs are inserted using ThreatConnect TcEx Framework
5. An HTTP client requests the acknowledgment of the just-ingested IOCs Intelligence payload. This request will include the IDs of the ingested IOCs using API Key for identification.
6. 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	
ip(Address)	Addresses, Tag "C2 Address"	Any valid IP address	
url(URL)	Hosts, Tag "C2 Hosts"	Any valid hostname	

md5(File)	Files (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.
Threat Rating (1-5)	Threat Rating (1-5)	Numbers 1 - 5	
Confidence	Confidence	Numbers 1 - 100	
Tags	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”.