

Darkfeed Threat Intelligence for the ThreatConnect Platform

User Guide

July 2021

Contents

Introduction	3
App Installation	4
Application Configuration	5
Job Configuration	5
Data Mapping	8
Job Output	12
Examples	13
Support	16

Introduction

Powered by the broadest, automated collection from the deep and dark web, Cybersixgill Darkfeed is a feed of malicious indicators of compromise (IOCs), including domains, URLs, hashes and IP addresses. IOCs are automatically extracted and delivered in real-time, and it is actionable, allowing ThreatConnect customers to receive and preemptively block items that threaten their organization.

App Installation

For download and installation instructions, refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

Application Configuration

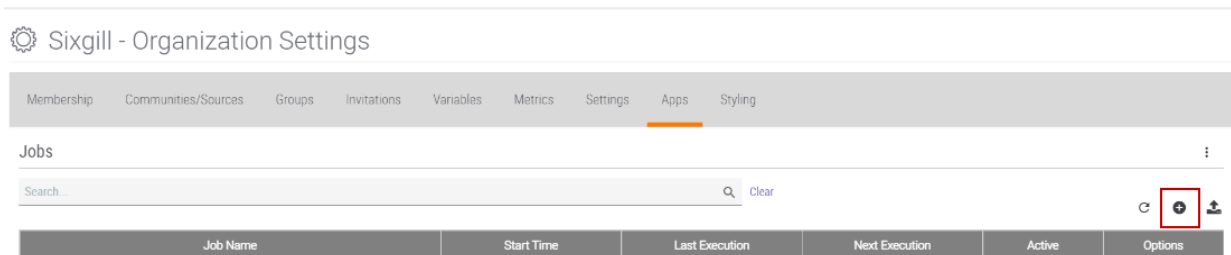


Make sure you have your **Sixgill client ID** and **Sixgill client Secret** (available from support@cybersixgill.com).

1. Verify the Cybersixgill Darkfeed Threat Intelligence App is installed.

Job Configuration

1. Click the Configure icon in the top right corner in the ThreatConnect platform and click **Organization Settings**.
2. Click **Apps**.
3. Click **+** to create a new job.



To configure a job:

1. In the **Program** window:
 - a. In **Job Name**, enter a name for this job (such as Cybersixgill Darkfeed).
 - b. Click **Run Program** and select Sixgill Darkfeed Threat Intelligence.
2. Click **NEXT**.

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

Job Name *
Cybersixgill Darkfeed

Run Program
Sixgill DarkFeed Threat Intelligence

CANCEL NEXT

To configure the job parameters:

1. In the **Parameters** window:
 - a. Click **Api User** and select your organization.
 - b. Click **ThreatConnect Owner** and select the source created by the Feed Deployer.
 - c. In the **Sixgill client ID** and **Sixgill client Secret fields**, enter the ID and secret you received from Cybersixgill (contact support@cybersixgill.com)
 - d. Click **Log Level** and select the required log level (default = warning).
2. Click **NEXT**.

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

Api User *

ThreatConnect Owner *

Sixgill client ID *

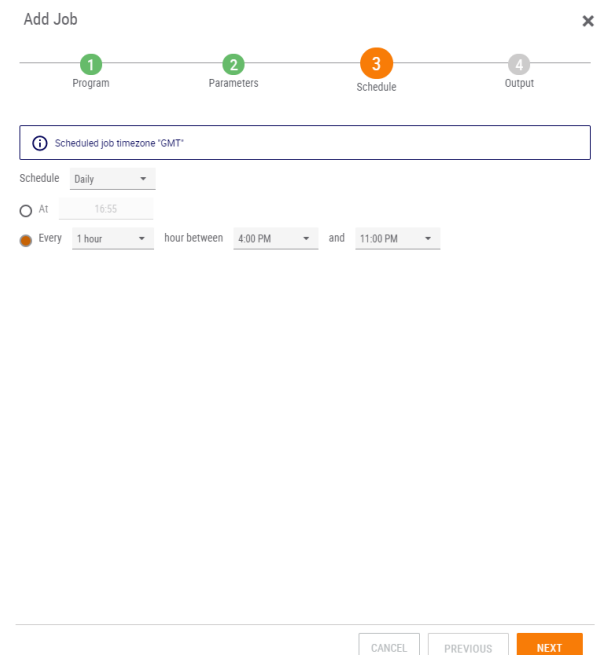
Sixgill client secret *

Log Level *
warning

CANCEL PREVIOUS NEXT

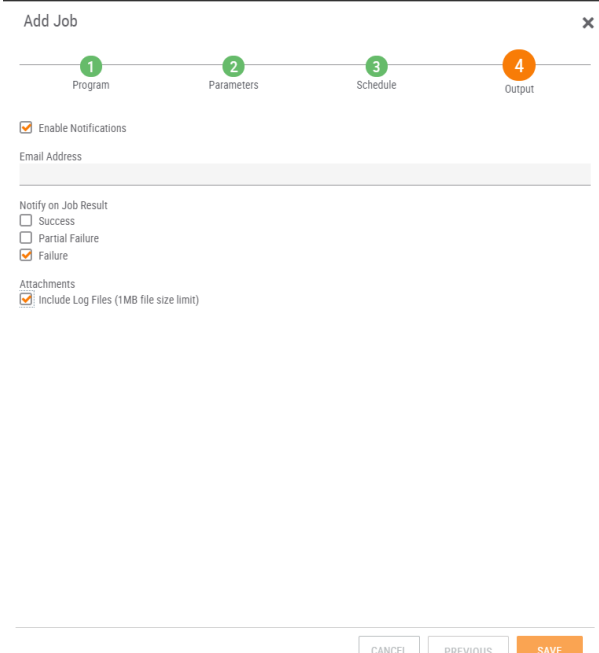
To configure the job schedule:

1. In the **Schedule** window, configure the following according to your environment:
 - a. Click **Schedule** and select the required recurrence (such as Daily, Weekly).
 - b. Click **At** or **Every** and configure the required time recurrence.
2. Click **NEXT**.



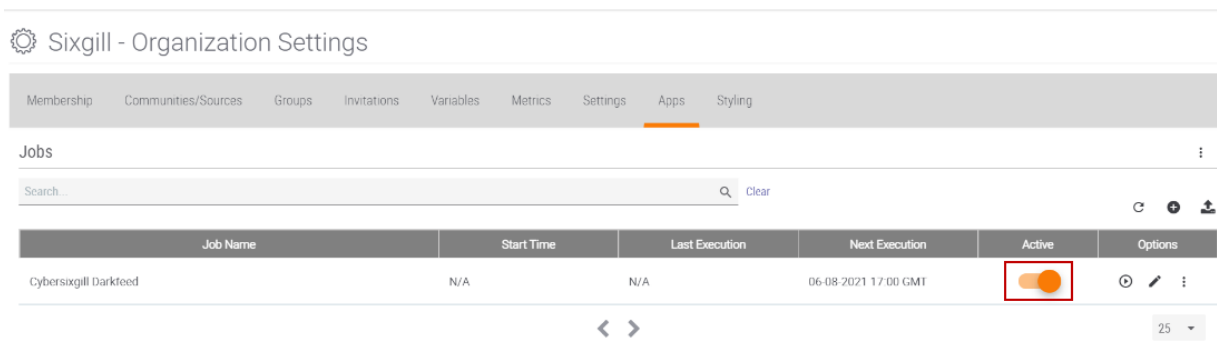
To receive job result notifications:

1. In the **Output** window:
 - a. Select the **Enable Notifications** checkbox.
 - b. In the **Email Address** box, enter the email address to which notifications will be sent.
 - c. Select the required checkboxes under **Notify on Job Result** and **Attachments**.
2. Click **SAVE**.



To activate the job:

1. In the Jobs list, on the required job row, click the Active slider.



For each job, you can view the **Start Time**, **Last Execution** status and **Next Execution** time.

To run the job manually:

1. In the Jobs list, on the required job row, in the **Options** column, click play.



Data Mapping

The table below documents the data mapping that takes place between the Sixgill Darkfeed Threat Intelligence data and the ThreatConnect Platform.

Cybersixgill Darkfeed Field	ThreatConnect Field/Object	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	

Cybersixgill Darkfeed Field	ThreatConnect Field/Object	Possible Values	Notes
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
Sixgill Post ID	Attribute -External ID	Any text String	The Id of the post in the Sixgill portal.
Source	Attribute - Source	Any text String	The name of the source in which the indicator appeared.
Title	Attribute -Title	Any text String	the actual title of the post/thread in which the indicator appeared.
Description	Attribute -Description	Any text String	Indicator description

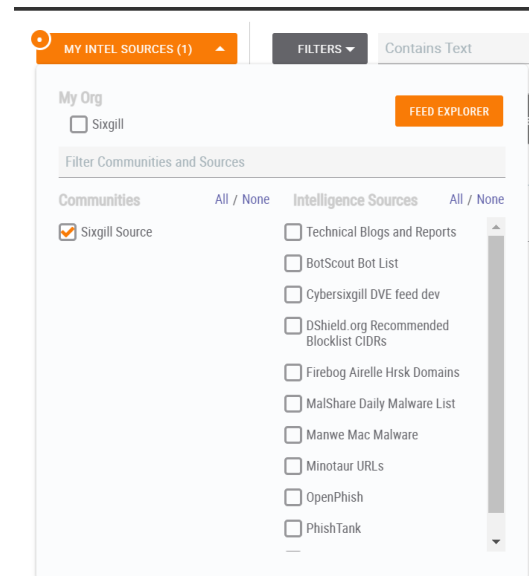
Cybersixgill Darkfeed Field	ThreatConnect Field/Object	Possible Values	Notes
Phase of Intrusion	Attribute - Phase if Intrusion	Any text String	Indicator phase of Intrusion which will be shown for Address, Host, File, URL Indicators.
Additional Analysis and Context	Attribute - Additional Analysis and Context	Any text String	Indicator external reference information e.g Mitre, virusTotal
STIX Indicator Type	Custom Attribute – Cybersixgill Darkfeed STIX Indicator Type	Any text String	Indicator STIX V1.0 mapping which will be shown for Address, Host, File, URL Indicators.
Sixgill Actor	Custom Attribute – Cybersixgill Darkfeed Actor	Any text String	Threat actor that originally shared the indicator on the dark web which will be shown for Address, Host, File, URL Indicators.

Cybersixgill Darkfeed Field	ThreatConnect Field/Object	Possible Values	Notes
Sixgill Language	Custom Attribute – Cybersixgill Darkfeed Language	Any text String	The language of the original post which included the indicator which will be shown for Address, Host, File, URL Indicators.
STIX ID	Custom Attribute – Cybersixgill Darkfeed STIX ID	Any text String	Threat actor that originally shared the indicator on the dark web which will be shown for Address, Host, File, URL Indicators.
Observation Time	Custom Attribute – Cybersixgill Darkfeed Observation Time	ISO 8601 Timestamp	Indicator observation Time.
Sixgill Feed Name	Custom Attribute - Cuybersixgill Darkfeed Feed Name	Any Text String	Feed Name


Job Output



1. Click **Browse > Indicators**.
2. Click **MY INTEL SOURCES**.
3. Select only the source configured in [Job Configuration](#), To configure the job parameters: (ThreatConnect Owner).

The source will be Sixgill Darkfeed Threat Intelligence if deployed with feed deployer.



Sample of Darkfeed Indicators imported from Cybersixgill to the ThreatConnect Platform:



dinograz.com


Status set by



Shell access to this domain is being sold on dark web markets

Type	Owner	Added	Last Modified
Host	Sixgill Source	07-05-2021	07-06-2021
DNS	Whois		
Not Active	Not Active		

Threat Rating


High

Confidence Rating


Confirmed

Tags

T1334 - Compromise 3rd party infrastructure to support delivery - EMI - PRE - ATT&CK
webshell

compromised_sites
Compromise 3rd party infrastructure to support delivery

Establish & Maintain Infrastructure
compromised
PRE-ATT&CK
shell

Attributes

Type	Last Modified	Value
Cybersixgill Darkfeed Observation Time	07-06-2021	2021-07-05T10:42:48.320Z
Title	07-06-2021	Dinograz's Collection http://dinograz.com
Cybersixgill Darkfeed Actor	07-06-2021	valyt
Source	07-06-2021	market_magbo
External ID	07-06-2021	fbf17afa1f787b9c4c4abdfd3bf57de5b0a558aa
Cybersixgill Darkfeed Language	07-06-2021	en
Cybersixgill Darkfeed Feed Name	07-06-2021	compromised_sites
Cybersixgill Darkfeed STIX ID	07-06-2021	indicator--ba804e06-5e9f-472b-8e0d-911c7d2bc70e
Phase of Intrusion	07-06-2021	Weaponization
Cybersixgill Darkfeed STIX Indicator Type	07-06-2021	Domain Watchlist
Additional Analysis and Context	07-06-2021	Source: mitre-attack description: Mitre attack tactics and technique reference mitre_attack_tactic: Establish & Maintain Infrastructure mitre_attack_tactic_id: TA0022 mitre_attack_tactic_url: https://attack.mitre.org/tactics/TA0022/ mitre_attack_technique: Compromise 3rd party infrastructure to support delivery mitre_attack_technique_id: T1334 mitre_attack_technique_url: https://attack.mitre.org/techniques/T1334/ source_name: mitre-attack

▼ CAL™ Insights



▼ Impressions

Today

0

Investigation Links

Open All [↗](#)

[abuse.net](#) [↗](#)

[Alexa](#) [↗](#)

[AlienVault OTX](#) [↗](#)

[BuiltWith](#) [↗](#)

[Censys \(Certificate\)](#) [↗](#)

[Censys \(Domain\)](#) [↗](#)

[Certificate Details](#) [↗](#)

[DomainTools](#) [↗](#)

[Google](#) [↗](#)

[Google Public DNS](#) [↗](#)

[Google Safe Browsing](#) [↗](#)

[Hurricane Electric](#) [↗](#)

[Hybrid Analysis](#) [↗](#)

[Is It Hacked?](#) [↗](#)

[NetCraft](#) [↗](#)

[Recorded Future](#) [↗](#)

[Robtex](#) [↗](#)

[Scumware](#) [↗](#)

[StopBadware](#) [↗](#)

[#totalhash](#) [↗](#)

[urlQuery](#) [↗](#)

[urlscan.io](#) [↗](#)

[URLVoid](#) [↗](#)

[VirusTotal](#) [↗](#)

[WhatCMS](#) [↗](#)

Support

For assistance, to report a bug or request a feature, please contact us via the following:

Support Portal	https://www.cybersixgill.com/contact-us/
Email	support@cybersixgill.com