

Cybersixgill DVE Feed 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

The Cybersixgill Dynamic Vulnerability Exploit (DVE) Score is based on the most comprehensive collection of vulnerability-related threat intelligence and is the only solution that provides users total context and predicts the immediate risks of a vulnerability based on threat actors' intent. ThreatConnect users can track threats stemming from CVEs that most others define as irrelevant and have a higher probability of being exploited via ThreatConnect's platform.

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

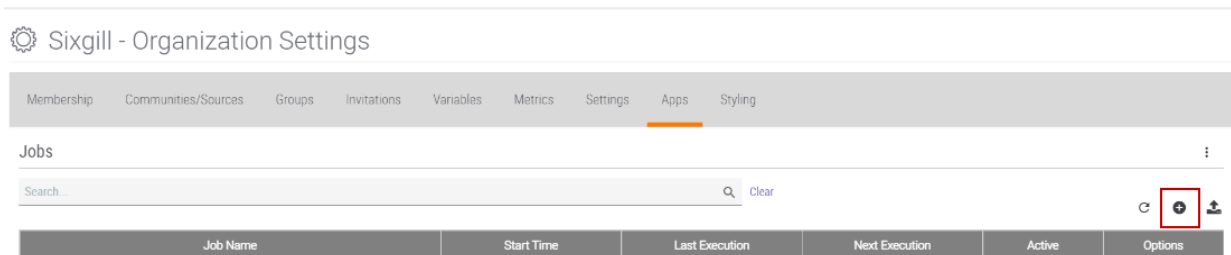


Make sure you have your **Sixgill client ID** and **Sixgill client Secret** (available from support@cybersixgill.com).

1. Verify the Cybersixgill DVE Feed App is installed.

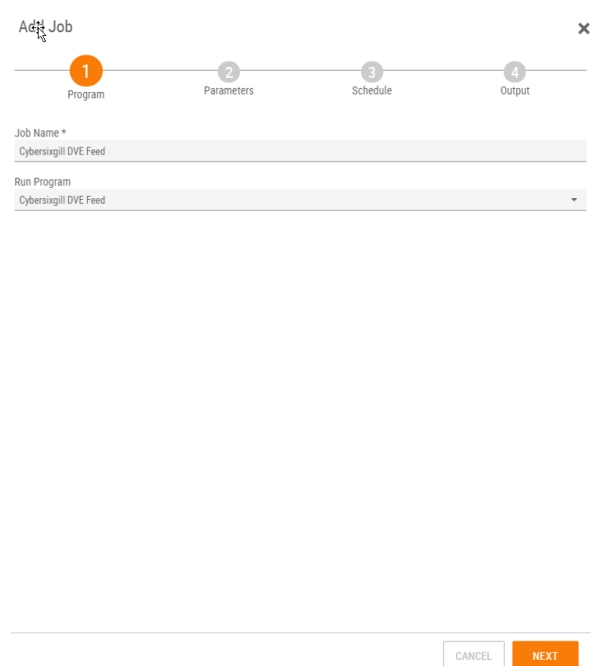
Job Configuration

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.



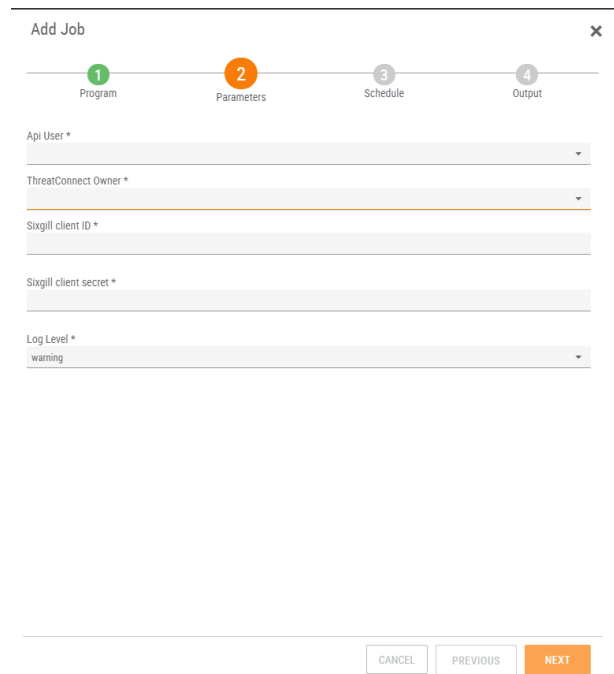
To configure a job:

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



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**.

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

Scheduled job timezone "GMT"

Schedule: Daily

At: 16:55

Every: 1 hour, hour between 4:00 PM and 11:00 PM

CANCEL PREVIOUS 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**.

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

☒ Enable Notifications

Email Address

Notify on Job Result

☐ Success

☐ Partial Failure

☒ Failure

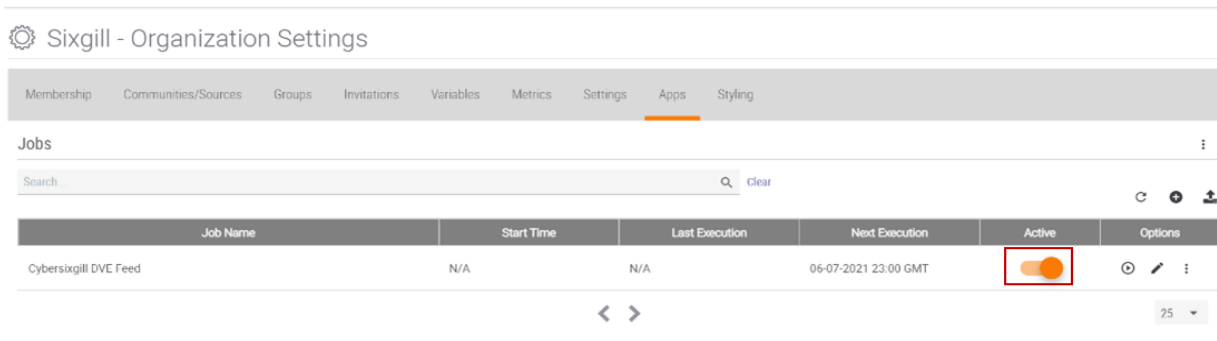
Attachments

☒ Include Log Files (1MB file size limit)

CANCEL PREVIOUS 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 Cybersixgill DVE Feed Threat Intelligence data and the ThreatConnect Platform.

Cybersixgill Field	ThreatConnect Field / Object	Possible Values	Description
Description	Summary	Any text String	Sixgill Feed Description
CVE ID	Tags	Any text String	CVE ID
DVE Score	Tags	Any text String	DVE Score Level (Low, Medium, High, Critical)

Cybersixgill Field	ThreatConnect Field / Object	Possible Values	Description
DVE Event Name	Tags	Any text String	DVE Event Name
Description	Attribute -Description	Any text String	Feed Description
created	Attribute - External Date Created	ISO 8601 Timestamp	Creation date of the event
modified	Attribute - External Date Last Modified	ISO 8601 Timestamp	Modification date of the event
External ID	Attribute - External ID	Any text String	CVE ID
DVE Feed Type	Custom Attribute – Cybersixgill DVE Feed Type	Any text String	Feed Type
DVE score - current	Custom Attribute – Cybersixgill DVE Feed DVE score - current	Number	The current DVE rating of the CVE
DVE score – highest ever date	Custom Attribute – Cybersixgill DVE Feed DVE score – highest ever date	ISO 8601 Timestamp	The date on which the CVE reached its highest ever DVE score
DVE score – highest ever	Custom Attribute – Cybersixgill DVE Feed DVE score – highest ever	Number	The highest ever DVE score given to this CVE
Previously exploited probability	Custom Attribute – Cybersixgill DVE Feed - Previously exploited probability	Number	The probability that this CVE has been previously Exploited
Event Name	Custom Attribute – Cybersixgill DVE Feed Event Name	Any text String	The event's name

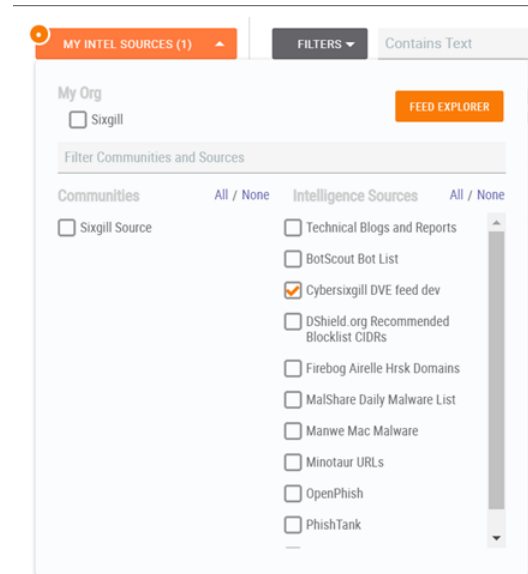
Cybersixgill Field	ThreatConnect Field / Object	Possible Values	Description
Event Type	Custom Attribute – Cybersixgill DVE Feed Event Type	Any text String	The Event's type
Event Action	Custom Attribute – Cybersixgill DVE Feed Event Action	Any text String	The event's action
Previous level	Custom Attribute – Cybersixgill DVE Feed Previous level	Any text String	The CVE's previous DVE score level
Event Datetime	Custom Attribute – Cybersixgill DVE Feed Event Datetime	ISO 8601 Timestamp	The date and time of the event
CVSS 3.1 score	Custom Attribute – Cybersixgill DVE Feed CVSS 3.1 score	Number	The CVE's score in CVSS 3.1 format
CVSS 3.1 severity	Custom Attribute – Cybersixgill DVE Feed CVSS 3.1 severity	Any text String	The CVE's severity level in CVSS 3.1 format
NVD Link	Custom Attribute – Cybersixgill DVE Feed NVD Link	Any text String	The Link to the CVE's page on NVD
NVD – last modified date	Custom Attribute – Cybersixgill DVE Feed NVD – last modified date	ISO 8601 Timestamp	The CVE's last modification date on NVD
NVD – publication date	Custom Attribute – Cybersixgill DVE Feed NVD – publication date	ISO 8601 Timestamp	The CVE's publication date on NVD

Cybersixgill Field	ThreatConnect Field / Object	Possible Values	Description
CVSS 2.0 score	Custom Attribute – Cybersixgill DVE Feed CVSS 2.0 score	Number	CVSS 2.0 score
CVSS 2.0 severity	Custom Attribute – Cybersixgill DVE Feed CVSS 2.0 severity	Any text String	CVSS 2.0 severity
NVD Vector – V2.0	Custom Attribute – Cybersixgill DVE Feed NVD Vector – V2.0	Any text String	NVD Vector - V2.0
NVD Vector – V3.1	Custom Attribute – Cybersixgill DVE Feed NVD Vector – V3.1	Any text String	NVD Vector - V3.1

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 Cybersixgill DVE Feed if deployed with feed deployer.




Examples

Sample of DVE Scores from Cybersixgill to ThreatConnect Platform:

ThreatConnect					
Dashboard Workflow Posts Playbooks Browse Spaces Create Import ? ⚙️ 🔔 🔍					
Groups Adversary Campaign Document E-mail Event Incident Intrusion Set Report Signature Task Threat ✓	Threat	CVE-2021-27135 is trending on Twit...	Cybersixgill DVE feed ...	CVE-2021-27135 DVE Critical risk trend_Twitter	07-05-2021
	Threat	CVE-2021-27928 is trending on Twit...	Cybersixgill DVE feed ...	CVE-2021-27928 trend_Twitter	07-05-2021
	Threat	CVE-2020-25097 is trending on Twit...	Cybersixgill DVE feed ...	CVE-2020-25097 trend_Twitter	07-05-2021
	Threat	CVE-2021-22986 is trending on Twit...	Cybersixgill DVE feed ...	CVE-2021-22986 DVE High risk trend_Twitter	07-05-2021
	Threat	CVE-2021-22986 is trending on Twit...	Cybersixgill DVE feed ...	CVE-2021-22986 DVE High risk trend_Twitter	07-05-2021
Tags					
Tracks					
Victims					
Victim Assets					
E-mail Address					
Network Account					
Phone					

DVE Score Details:

 CVE-2021-1656 is trending on Twitter.

☰

✕

CVE-2021-1656 is trending on Twitter.

Type	Owner	Added
Threat	Cybersixgill DVE feed dev	07-05-2021


Tags

trend_Twitter

DVE High risk

CVE-2021-1656

Attributes



Type	Last Modified	Value
External Date Created	07-05-2021	2021-04-22T11:07:45Z
External Date Last Modified	07-05-2021	2021-04-22T11:07:45Z
External ID	07-05-2021	CVE-2021-1656
Cybersixgill DVE Feed Type	07-05-2021	x-cybersixgill-com-cve-event

Cybersixgill DVE Feed DVE score - current	07-05-2021	7.12
Cybersixgill DVE Feed DVE score - highest ever date	07-05-2021	2021-03-31T00:00:00.000Z
Cybersixgill DVE Feed DVE score - highest ever	07-05-2021	7.12
Cybersixgill DVE Feed - Previously exploited probability	07-05-2021	5.19
Cybersixgill DVE Feed Event Name	07-05-2021	trend_Twitter
Cybersixgill DVE Feed Event Type	07-05-2021	dark_mention
Cybersixgill DVE Feed Event Action	07-05-2021	trend

Cybersixgill DVE Feed Event Datetime	07-05-2021	2021-03-29T00:00:00.000Z
Cybersixgill DVE Feed CVSS 3.1 score	07-05-2021	5.5
Cybersixgill DVE Feed CVSS 3.1 severity	07-05-2021	MEDIUM
Cybersixgill DVE Feed NVD Link	07-05-2021	https://nvd.nist.gov/vuln/detail/CVE-2021-1656
Cybersixgill DVE Feed NVD - last modified date	07-05-2021	2021-01-19T15:40:00.000Z
Cybersixgill DVE Feed NVD - publication date	07-05-2021	2021-01-12T20:15:00.000Z
Cybersixgill DVE Feed CVSS 2.0	07-05-2021	2.1

Cybersixgill DVE Feed CVSS 2.0 severity	07-05-2021	LOW
Cybersixgill DVE Feed NVD Vector - V2.0	07-05-2021	AV:L/AC:L/Au:N/C:P/I:N/A:N
Cybersixgill DVE Feed NVD Vector - V3.1	07-05-2021	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

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