



**Bambenek  
Consulting**

# **ThreatConnect – Bambenek Consulting User Guide**

Version 1.0.0

## **Contents**

<b>Introduction .....</b>	<b>2</b>
<b>Release Notes .....</b>	<b>3</b>
<b>Data Mapping .....</b>	<b>4</b>
<b>Configuration Requirements .....</b>	<b>4</b>
<b>Job App Installation .....</b>	<b>4</b>
<b>ThreatConnect Job Configuration .....</b>	<b>5</b>
<b>Browsing Bambenek Consulting Feed .....</b>	<b>9</b>
<b>IP Address Feed: .....</b>	<b>10</b>
<b>Host Feed: .....</b>	<b>11</b>
<b>Support .....</b>	<b>11</b>

## Introduction

**Bambenek Consulting** is a leading cybersecurity threat intelligence and data science firm led by industry veteran John Bambenek. Services include the Well-Fed Intelligence feeds used by thousands of organizations all over the world.

Using our novel techniques, we surveil attackers to see where they actually live so you have the latest information to feed into your security tools or SIEM to protect yourself. With Well Fed, you can be sure your security tools are fed with the latest information they need to keep you safe.

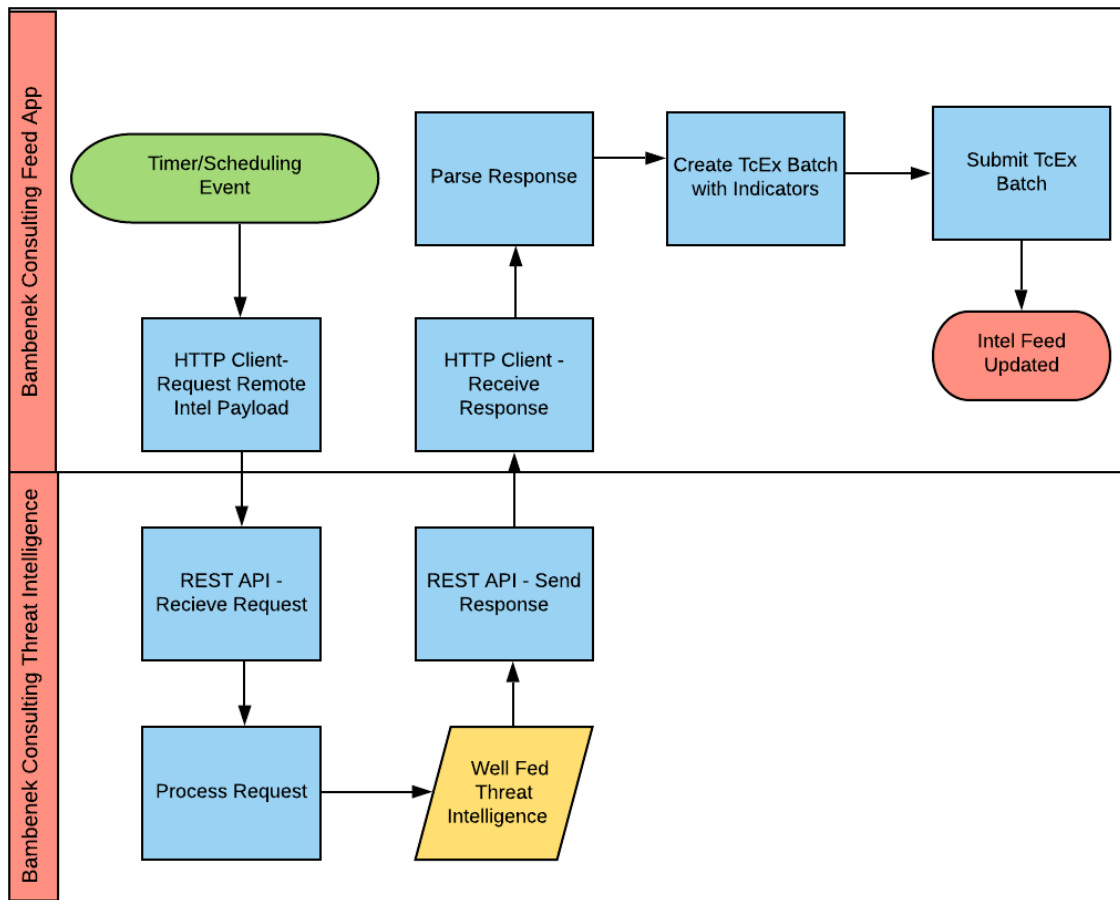
This system provides one of the largest repositories of curated threat intelligence that is publicly available. Approximately one million malicious domains are monitored every hour and are curated and whitelisted to ensure that you have reliable information you need to protect yourself from cybercriminals. With Well Fed, your security tools are more effective.

We offer both end-user organization licenses and licenses to security companies and MSSPs. Reach out today to learn how Well Fed can protect your digital assets today.

### Intelligence-services offered via this integration:

- **High-Confidence C2 IP Feed** - Master Feed of known, active, and non-sinkholed C&Cs IP addresses (high-confidence only).
- **High-Confidence C2 Domain Feed** - Master Feed of known, active, and non-sinkholed C&Cs domain names (high-confidence only).
- **High-Confidence DGA Domain Feed** - Domain feed of known DGA domains from -2 to +3 days (high-confidence only).
- **Sinkhole Feed** - Manually curated list of IPs known to be sinkholes.
- **Maldomainml Malware Feed** - Feed of current malware domains.
- **Maldomainml Phishing Feed** - Feed of current phishing domains.

This integration consists of consuming the Bambenek Consulting Threat Intelligence feed and importing the data as indicators into the ThreatConnect Platform as a Threat Intelligence feed. A high-level run of the Bambenek Consulting Threat Intelligence feed is shown below.



## Release Notes

App Version	Release Date	Details
1.0.0		Initial Release.

## Data Mapping

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

Bambenek Threat Intelligence Feed	ThreatConnect Field/Object	Possible Values	Description
ip_address	Address  Tags 1. "C2" 2. "Sinkhole"	Any valid Ip Address	Fetched from the following feeds  1) High-Confidence C2 IP Feed 2) Sinkhole Feed
hostname	Hosts  Tags 1. "C2", 2. "DGA" 3. "Malware" 4. "Phishing"	Any valid hostname	Fetched from the following feeds  1) High-Confidence C2 Domain Feed 2) High-Confidence DGA Domain Feed 3) Maldomainml Malware Feed 4) Maldomainml Phishing Feed
description	Description attribute	Any valid string	Description about who used the indicator
date_created	Description attribute	Any valid string	Created date of the feed
info	Source attribute	Any valid string	Link to the manual feed URL link
owner	Description attribute	Any valid string	Sinkhole Owner

## Configuration Requirements

1. Access to a ThreatConnect Platform Instance
2. ThreatConnect API user

## Job App Installation

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

## ThreatConnect Job Configuration

The ThreatConnect Platform allows customers to run jobs on a scheduled basis. Once the package has been installed, the customer can run the Bambenek Consulting Threat Intelligence feed as frequently as they desire. By default, the App will run daily.

**Note:** These steps are not necessary if the app was deployed using Feed Deployer as the job would have already been configured.

- Go to the gear in the top right corner in the ThreatConnect platform then **Org Settings > Apps**.
- Click on the + to create a new job

### Program Screen:

- Enter the Job Name (Ex: Bambenek Consulting Feed).
- Select the Run program as a Bambenek Consulting Feed from the dropdown.
- Click NEXT.

1 Program 2 Parameters 3 Schedule 4 Output

Job Name \*

Bambenek Consulting Feed

Run Program

Bambenek Consulting Feed

CANCEL NEXT

## Parameter Screen:

- For API User, click on the down arrow and select your organization
- For ThreatConnect Owner, click on the down arrow and select the source created by the Feed Deployer
- For Username and Password, please provide credentials received from Bambenek Consulting.
- For Services, please select any of or all the feeds to fetch the data from Bambenek.
- For Log Level, select it from dropdown default log level set to warning.
- Click NEXT

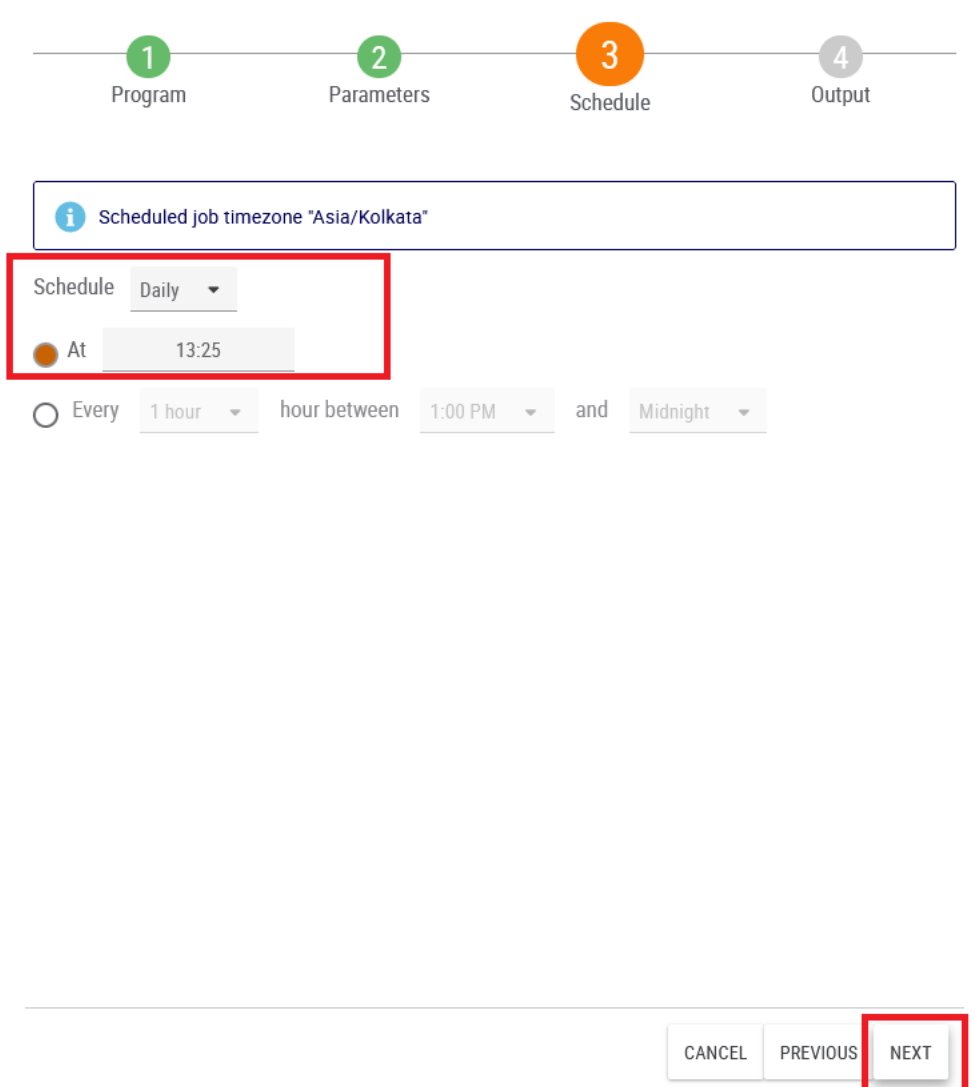
The form is titled 'Parameter Screen' and features a progress bar at the top with four steps: 1 Program, 2 Parameters (highlighted in orange), 3 Schedule, and 4 Output. Below the progress bar, the form contains several fields:

- Api User \***: A dropdown menu with a down arrow.
- ThreatConnect Owner \***: A dropdown menu with 'Bambenek Source' selected and a down arrow.
- Username \***: A text input field with a yellow background and a vertical ellipsis icon on the right.
- Password \***: A password input field with a yellow background, masked with dots, and a vertical ellipsis icon on the right.
- Services of Bambenek Consulting \***: A dropdown menu with 'High-Confidence C2 IP Feed, High-Confidence C2 Domain Feed, High-Confidence DGA' selected and a down arrow.
- Log Level \***: A dropdown menu with 'warning' selected and a down arrow.

At the bottom right of the form, there are three buttons: 'CANCEL', 'PREVIOUS', and 'NEXT'. The 'NEXT' button is highlighted with a red border.

## Schedule Screen:

- Depending on your environment, you can schedule the feed at daily hours, weekly etc., select the appropriate values from the dropdown menu.
- Click NEXT



1 Program 2 Parameters 3 Schedule 4 Output

*i* Scheduled job timezone "Asia/Kolkata"

Schedule Daily ▼

☒ At 13:25

☐ Every 1 hour ▼ hour between 1:00 PM ▼ and Midnight ▼

CANCEL PREVIOUS **NEXT**

## Output Screen:

- If you want to be notified on job results, click the box next to Enable Notifications, enter an email address for the notifications to be sent, and which notifications that you want and if you want a log file attached.
- Click SAVE



☐ Enable Notifications

Email Address

Notify on Job Result

☐ Success

☐ Partial Failure

☐ Failure

Attachments

☐ Include Log Files (1MB file size limit)

CANCEL PREVIOUS **SAVE**




- Once the Job has been saved, we can find our job on Jobs under Apps
- Click on the slider under Active to activate the job.
- Here we can observe the Start Time and Next Execution time and Last Execution Status as well if you want to run the job at this time click on the play button in options tab.

Bambenek - Organization Settings

Membership Communities/Sources Groups Invitations Variables Metrics Settings **Apps** Styling

Jobs

Search... [Clear](#)

Job Name	Start Time	Last Execution	Next Execution	Active	
Bambenek Consulting Feed	N/A	N/A	10-02-2021 14:03 IST	<input checked="" type="checkbox"/>	  

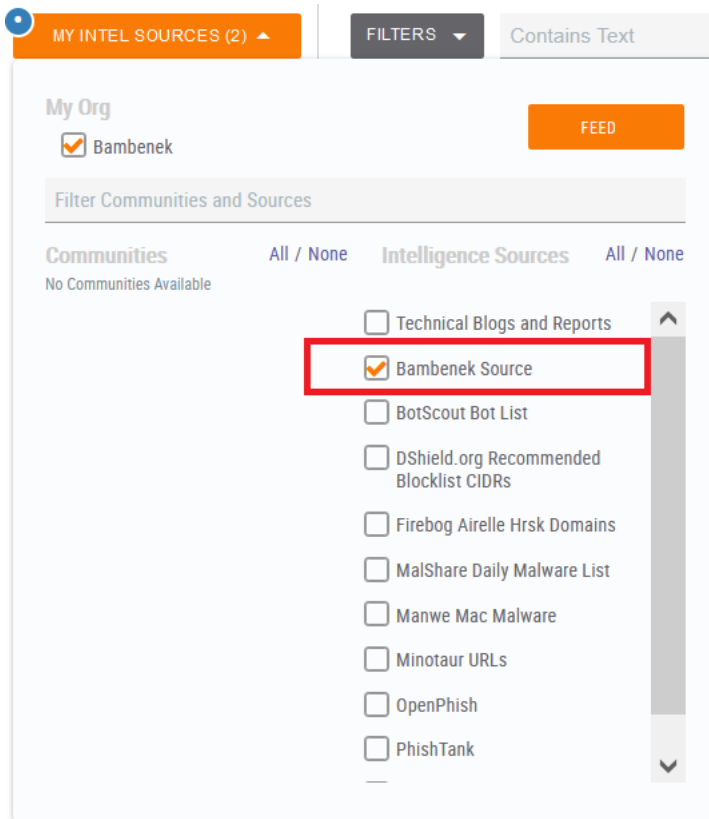


## Browsing Bambenek Consulting Feed

For guidance on general browsing of indicators and groups in the ThreatConnect Platform, please refer to the article below:

<https://training.threatconnect.com/learn/article/browse-kb-article>

Navigate to the browse page and check to make sure that the Bambenek Source Feed is checked.



## IP Address Feed

To browse **IP Address Feed** from Bambenek Consulting, select Address Indicator.

**ThreatConnect** Dashboard Workflow Posts Playbooks Browse Spaces Create Import

MY INTEL SOURCES (2) FILTERS Contains Text Clear All

**Indicators**

- Address
- E-mail Address
- File
- Host
- URL
- ASN
- CIDR
- Email Subject
- Hashtag
- Mutex
- Registry Key
- User Agent

Groups

- Adversary
- Campaign
- Document
- E-mail
- Event
- Incident
- Intrusion Set
- Report
- Signature
- Task
- Threat

1-10 of 1617 total results

Type T1	Summary T1	Owner T1	Version T1	Threat Rating T1	ThreatAssess T1	Obs T1	F/P T1	Added T1	Modified T1
Address	217.20.116.145	Bambenek	IPv4	High	281	--	--	10-01-2021	10-01-2021
Address	217.20.116.146	Bambenek	IPv4	High	281	--	--	10-01-2021	10-01-2021
Address	217.20.116.147	Bambenek	IPv4	High	503	--	--	10-01-2021	10-01-2021
Address	217.20.116.148	Bambenek	IPv4	High	503	--	--	10-01-2021	10-01-2021
Address	217.20.116.149	Bambenek	IPv4	High	503	--	--	10-01-2021	10-01-2021
Address	217.20.116.150	Bambenek	IPv4	High	513	--	--	10-01-2021	10-01-2021
Address	217.20.116.151	Bambenek	IPv4	High	503	--	--	10-01-2021	10-01-2021
Address	217.20.116.152	Bambenek	IPv4	High	503	--	--	10-01-2021	10-01-2021

**ThreatConnect** Dashboard Workflow Posts Playbooks Browse Spaces Create Import

MY INTEL SOURCES (2) FILTERS Contains Text Clear All

**Indicators**

- Address
- E-mail Address
- File
- Host
- URL
- ASN
- CIDR
- Email Subject
- Hashtag
- Mutex
- Registry Key
- User Agent

Groups

- Adversary
- Campaign
- Document
- E-mail
- Event
- Incident
- Intrusion Set
- Report
- Signature
- Task
- Threat

1-10 of 1617 total results

217.20.116.149

Status set by

Type Address Owner Bambenek Added 10-01-2021 Last Modified 10-01-2021

ThreatAssess

503 High

Recent False Positive Reported  
Impacted by Recent Observations

Threat Rating High Confidence Rating 95% Confirmed

Tags

C2

Attributes

Type	Last Modified	Value
Source	10-01-2021	http://osint.bambenekconsulting.com/manual/ramnit.txt
Description	10-01-2021	IP used by ramnit C&C

## Host Feed

To browse **Hosts Feed** from Bambenek Consulting, select Host Indicator.

1-10 of 596470 total results

Type	Summary	Owner	Threat Rating	ThreatAssess	Obs	F/P	Added	Modified
Host	www1.playhbogo.comcapitalone.com phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021
Host	www1.youtubebebe.com phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021
Host	www.ads.mawazo.host phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021
Host	www.aeon.cv.casrcd.com phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021
Host	www.alibaba.login.accutrack.co.za phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021
Host	www.business.laguestlist.nl phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021
Host	www.harti-info.flu.cc phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021
Host	www.janssencovid19vaccin.com phishing	Bambenek	High	—	—	—	10-01-2021	10-01-2021

ThreatConnect

Dashboard Workflow Posts Playbooks Browse Spaces Create Import ?

1-10 of 596470 total results

Type	Summary	Owner
Host	www1.playhbogo.comcapitalone.com phishing	Bambenek
Host	www1.youtubebebe.com phishing	Bambenek
Host	www.ads.mawazo.host phishing	Bambenek
Host	www.aeon.cv.casrcd.com phishing	Bambenek
Host	www.alibaba.login.accutrack.co.za phishing	Bambenek
Host	www.business.laguestlist.nl phishing	Bambenek
Host	www.harti-info.flu.cc phishing	Bambenek
Host	www.janssencovid19vaccin.com phishing	Bambenek

www.alibaba.login.accutrack.co.za

Status set by X

Type	Owner	Added	Last Modified
Host	Bambenek	10-01-2021	10-01-2021

DNS Not Active Whois Not Active

Threat Rating: High Confidence Rating: 90% Confirmed

Tags: phishing

Attributes

Type	Last Modified	Value
Source	10-01-2021	https://osint.bambenekconsulting.com/manual/maldomainml-phishing.txt
Description	10-01-2021	Hostname used by phishing

CAL™ Insights

Trends

7 days 30 days

## Support

For assistance with this App, to report a bug, or feature requests please contact us via the following.

Support Portal	<a href="http://www.bambenekconsulting.com/contact/">http://www.bambenekconsulting.com/contact/</a>
Email	<a href="mailto:support@bambenekconsulting.com">support@bambenekconsulting.com</a>