DEPLOYMENT GUIDE

Infoblox TIDE & MISP Integration

Table of Contents

Introduction.......... 2

Requirements.......... 2

Tested Hardware & Software.......... 2

Deployment Summary.......... 2

Deployment Instructions.......... 3

- CSP API Key Retrieval.......... 3
- TIDE Feed Filters.......... 5
- Limitations.......... 7
- MISP Configuration.......... 8
- MISP Events & Attributes with TIDE.......... 11

Additional Resources.......... 14

Introduction

This deployment guide demonstrates how to incorporate TIDE feeds into a MISP instance.

Infoblox Threat Intelligence Data Exchange (TIDE) leverages highly accurate machine-readable threat intelligence (MRTI) data to aggregate and selectively distribute data across a broad range of security infrastructure. The threat intelligence team curates, normalizes, and refines the high-quality threat data to minimize false positives. Our threat feeds begin with information gained from native investigations and harvesting techniques. We then combine them with verified and observed data from trusted partners including government agencies, academics, several premier Internet infrastructure providers, and law enforcement. The result is a highly refined feed with a low historical false-positive rate.

The MISP threat sharing platform is a free and open-source software for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or counter-terrorism information.

Requirements

The following items are required to incorporate the Infoblox TIDE feeds into MISP:

- Access to an Infoblox BloxOne Threat Defense Advanced subscription

- Access to a MISP instance

Tested Hardware & Software

- MISP version 2.4.130 installed on an Ubuntu 18.04 Virtual Machine

Deployment Summary

1. Retrieve your BloxOne Threat Defense Advanced API key from the Cloud Services Portal.

2. Observe TIDE filters offered by Infoblox and retrieve API call.

3. Configure MISP to connect to the Infoblox Cloud Services Portal and download TIDE feeds.

4. Demonstrate functionality of MISP with TIDE.

Deployment Instructions

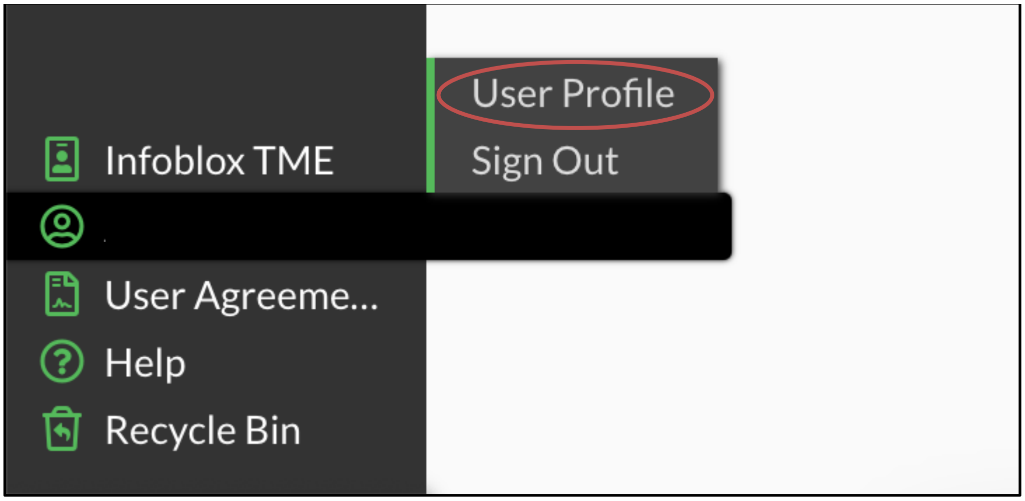
CSP API Key Retrieval

You will need a BloxOne Threat Defense Advanced API key to pull the TIDE feeds via the REST API in MISP. You can access this key through the Cloud Services Portal (CSP). API keys are unique identifiers found in many applications to both identify the application making the API calls and verify the application making the calls has access to do so.

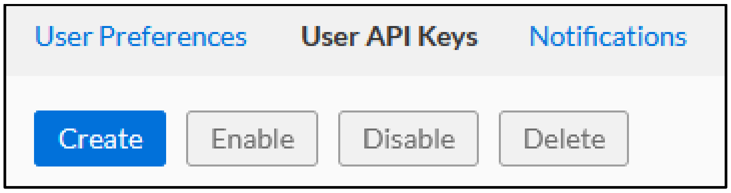
To access your API key:

1. Log into the CSP at https://csp.infoblox.com.

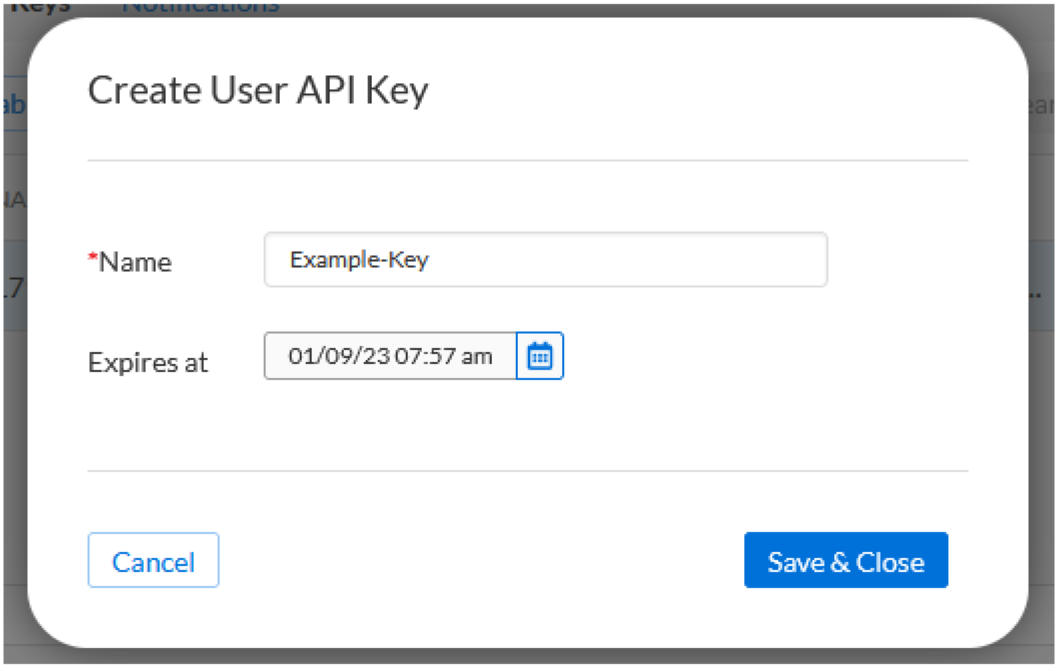
2. Upon logging in, hover over your username in the bottom-left corner and select **User Profile**.



3. Navigate to the User API Keys tab. Click **Create** to create a new API Key.



4. In the Create User API Key dialog box, input a **Name** and an **expiration date** for the API Key.



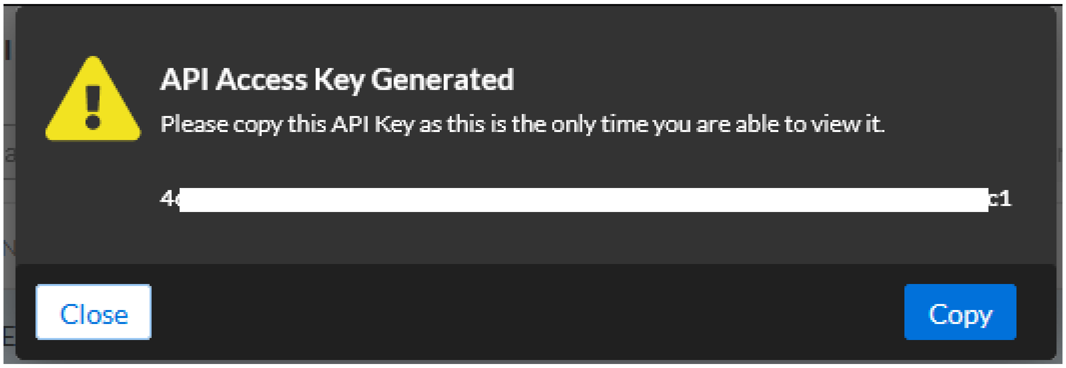
Create User API Key

*Name: Example-Key

Expires at: 01/09/23 07:57 am

5. Click **Save & Close** to confirm the creation of the API Key.

6. A dialog box containing the new API Key will be shown. Click **Copy** to copy your API key to your clipboard. Paste it somewhere you can easily access and then copy from later, such as Notepad.



API Access Key Generated

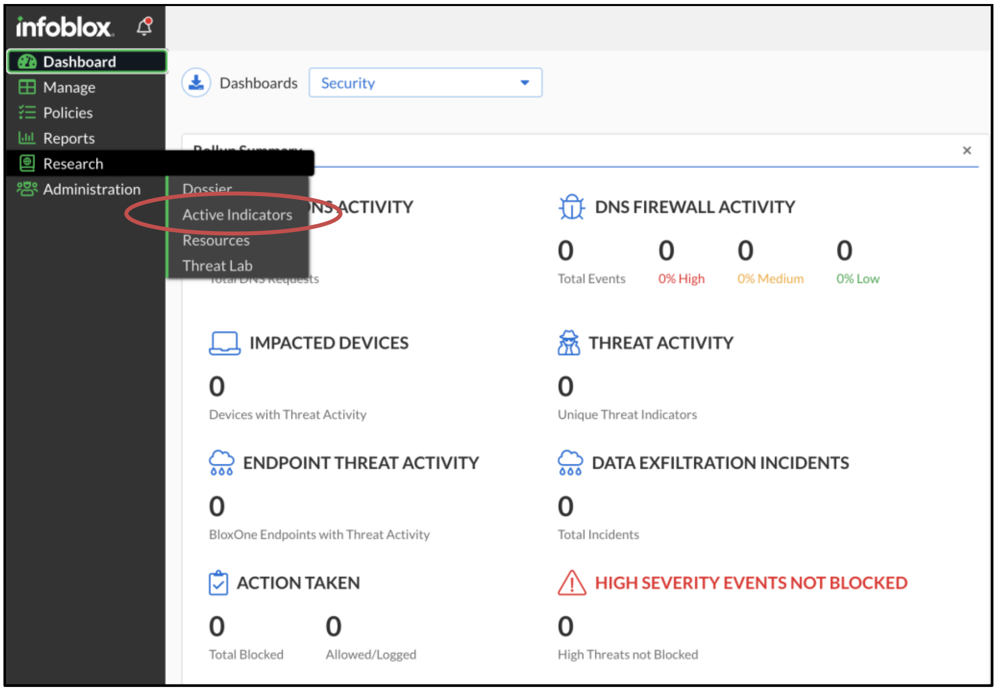
Please copy this API Key as this is the only time you are able to view it.

[redacted]

TIDE Feed Filters

Infoblox TIDE provides many filters to choose from depending on your needs. This section of the demo shows you an overview of the filters and how to retrieve the appropriate API call to grab these feeds in MISP based on the desired filters.

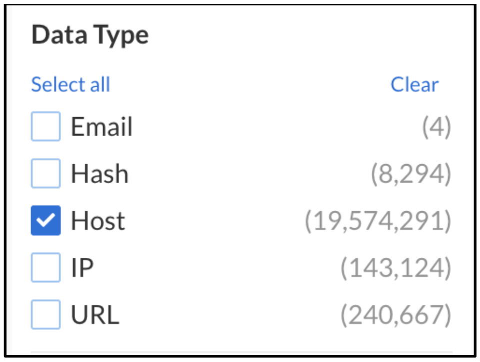
1. In the left side menu of the CSP, navigate to **Research** → **Active Indicators**.



2. Here you can see all active threat indicators based on Infoblox TIDE research. There are millions of indicators, so let's focus on incorporating only Host data types in the Phishing threat class.

   a. Under **DATA TYPE**, click **Clear** to deselect each checkbox.

   b. Select **Host**.



Data Type

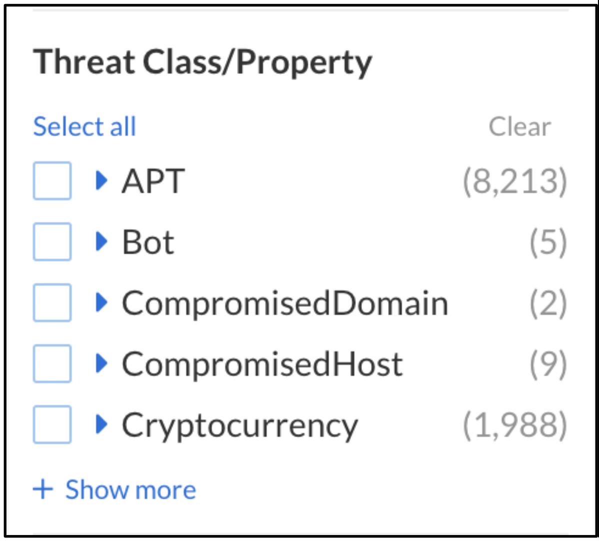
Select all Clear

□ Email	(4)
□ Hash	(8,294)
☑ Host	(19,574,291)
□ IP	(143,124)
□ URL	(240,667)

c. Under **THREAT CLASS/PROPERTY**, click **Clear** to deselect each checkbox.

d. Click **Show more**.

e. Select **Phishing**.

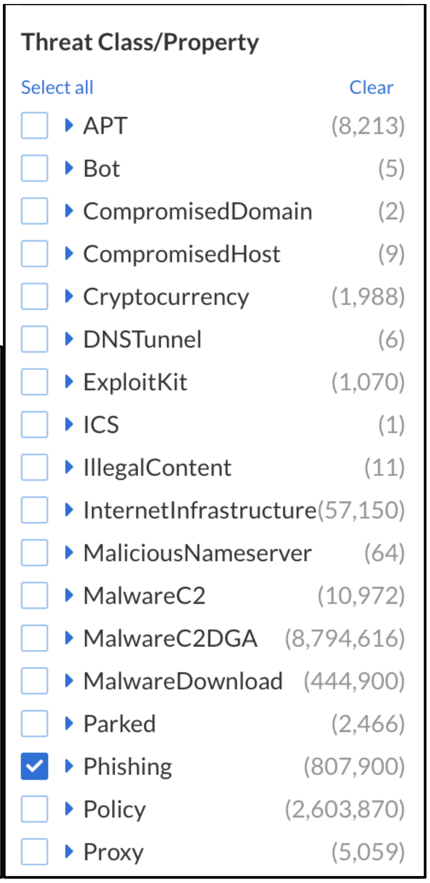


Threat Class/Property

Select all Clear

□	APT	(8,213)
□	Bot	(5)
□	CompromisedDomain	(2)
□	CompromisedHost	(9)
□	Cryptocurrency	(1,988)

+ Show more

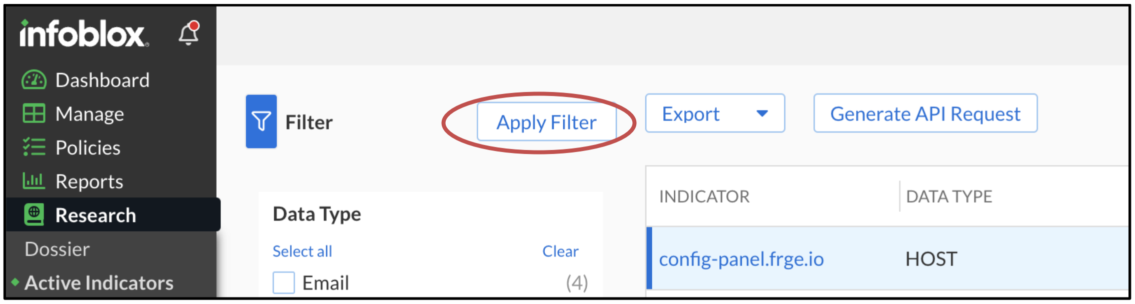


Threat Class/Property

Select all Clear

□	APT	(8,213)
□	Bot	(5)
□	CompromisedDomain	(2)
□	CompromisedHost	(9)
□	Cryptocurrency	(1,988)
□	DNSTunnel	(6)
□	ExploitKit	(1,070)
□	ICS	(1)
□	IllegalContent	(11)
□	InternetInfrastructure	(57,150)
□	MaliciousNameserver	(64)
□	MalwareC2	(10,972)
□	MalwareC2DGA	(8,794,616)
□	MalwareDownload	(444,900)
□	Parked	(2,466)
☑	Phishing	(807,900)
□	Policy	(2,603,870)
□	Proxy	(5,059)

f. Click **Apply Filter** at the top. Now you will only see Host data types of the Phishing class listed.



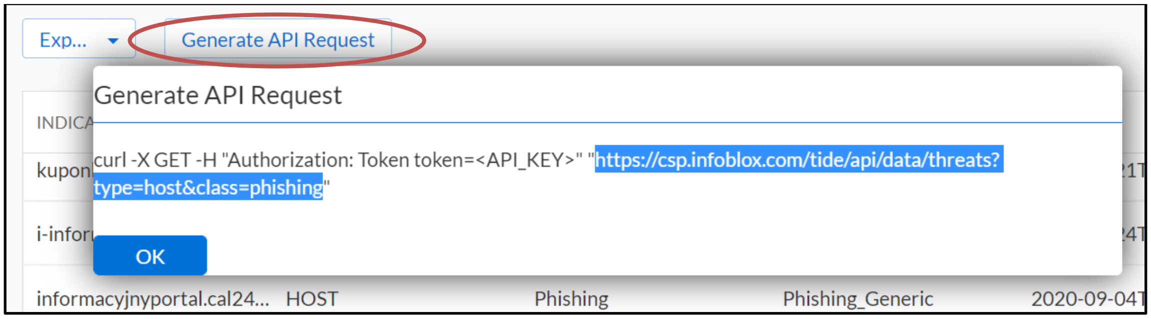
Data Type

Select all Clear

□ Email (4)

INDICATOR	DATA TYPE
config-panel.frge.io	HOST

3. Click **Generate API Request** to view the API request you will need to copy into MISP to grab this data. The necessary request is highlighted in blue below. Copy and paste it somewhere you can easily copy from later, such as Notepad. Click **OK** to close the popup.


Exp...
Generate API Request
Generate API Request
INDICA
kupon
i-infor
OK
informacyjnyportal.cal24... HOST Phishing Phishing_Generic 2020-09-04T

```
curl -X GET -H "Authorization: Token token=<API_KEY>" "https://csp.infoblox.com/tide/api/data/threats?type=host&class=phishing"
```

Limitations

There are several limitations to note when importing feeds into MISP.

1. Importing millions of records from TIDE into MISP can take a very long time, potentially hours or even days on low end systems. **It is highly recommended to use filters in your API calls, such as an *rlimit=100000* to reduce import time.**

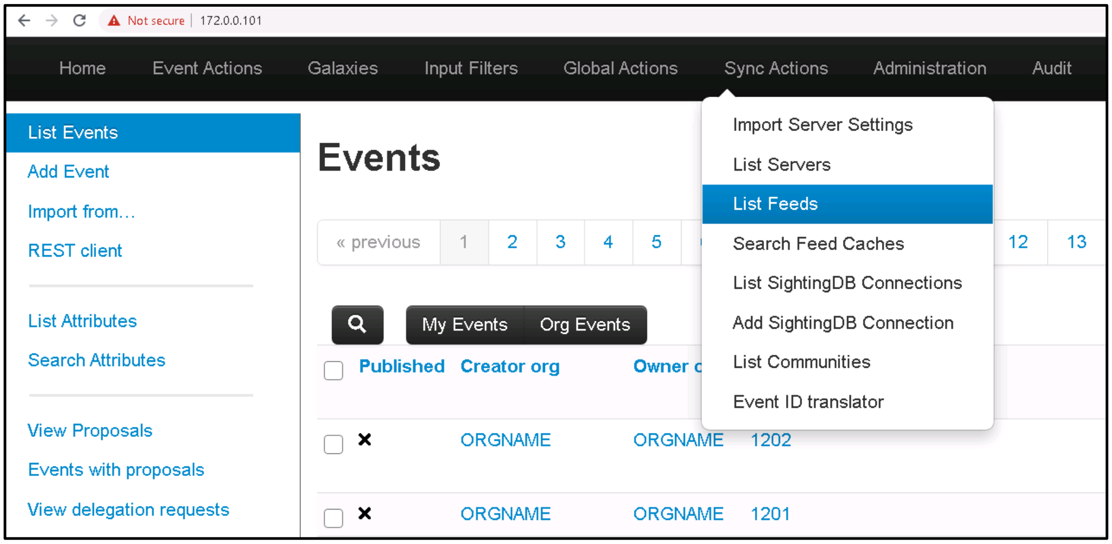
2. Importing multiple datatypes in the same feed can cause problems, including 400 errors returned by MISP. **It is highly recommended to import one datatype (host, url, ip, hash or email) at a time within the same feed.** If you want to use multiple datatypes, you can create multiple feeds in MISP that return each datatype, or use the *fields=* parameter in the TIDE call to return only one domain field from each datatype. This is due to the TIDE API returning different fields between datatypes. For example, hashes and ips do not have a 'domain' field like URLs, emails and hosts do; or that URLs contain an extra 'url' field for which the other types do not.

3. MISP has an easier time importing CSV over JSON. When using CSV, MISP parses the actual domains/hosts better without the extra characters returned by JSON. To return CSV, use the *data_format=csv* parameter in the TIDE call.

MISP Configuration

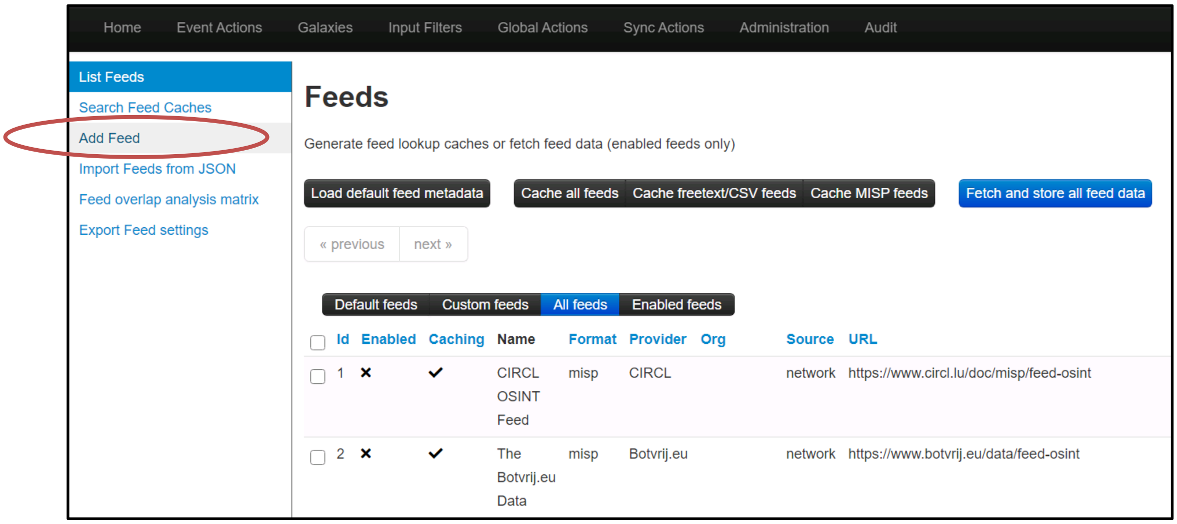
This section shows how to connect MISP to the Infoblox TIDE feeds.

1. Navigate to **Sync Actions** → **List Feeds**.



□	Published	Creator org	Owner o
□	✗	ORGNAME	ORGNAME 1202
□	✗	ORGNAME	ORGNAME 1201

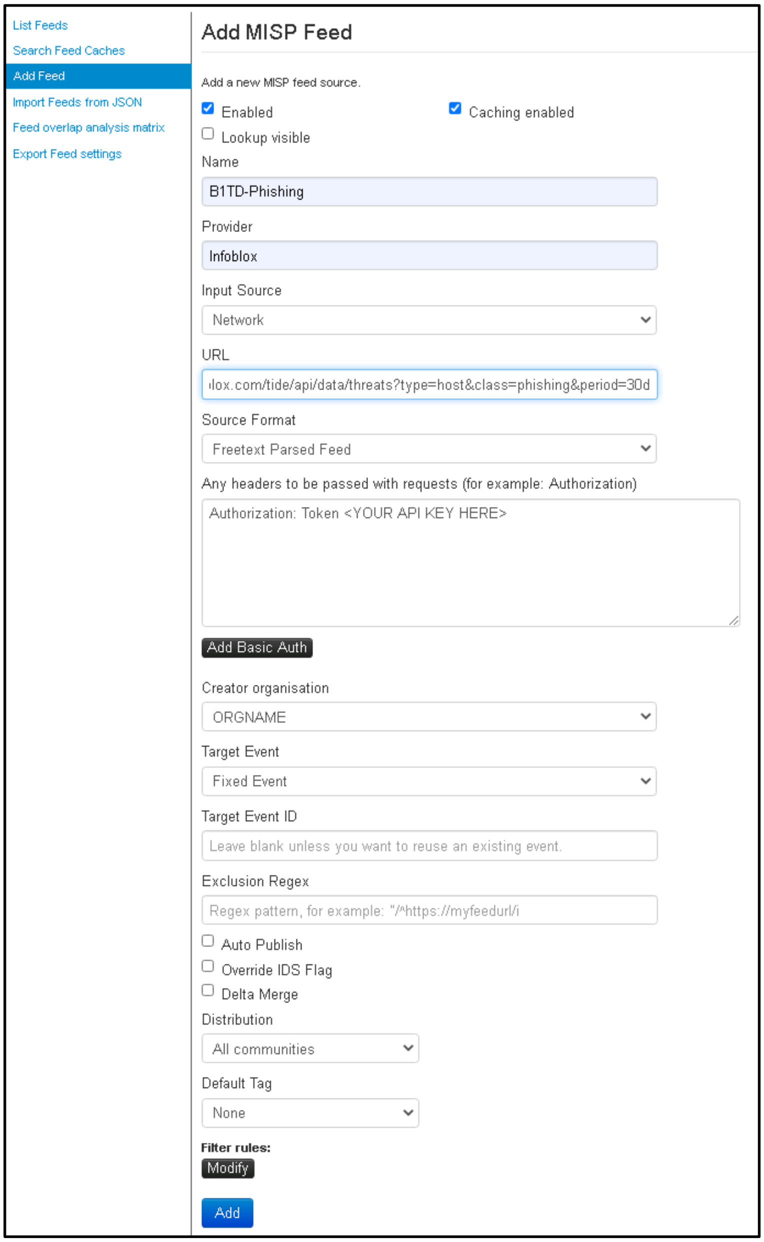
2. Click **Add Feed** in the left menu.



Generate feed lookup caches or fetch feed data (enabled feeds only)

□	Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL
□	1	✗	✓	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint
□	2	✗	✓	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint

3. Input the **parameters** for the new feed.



Add MISP Feed

Add a new MISP feed source.

☑ Enabled ☑ Caching enabled

☐ Lookup visible

Name: B1TD-Phishing

Provider: Infoblox

Input Source: Network

URL: lox.com/tide/api/data/threats?type=host&class=phishing&period=30d

Source Format: Freetext Parsed Feed

Any headers to be passed with requests (for example: Authorization): Authorization: Token <YOUR API KEY HERE>

Creator organisation: ORGNAME

Target Event: Fixed Event

Target Event ID: Leave blank unless you want to reuse an existing event.

Exclusion Regex: Regex pattern, for example: "/^https://myfeedurl/i

☐ Auto Publish

☐ Override IDS Flag

☐ Delta Merge

Distribution: All communities

Default Tag: None

Filter rules:

Check **Enabled** and **Caching** enabled.

Name: Enter a recognizable name.

Provider: Enter a recognizable provider.

Input Source: Select Network as we are accessing our source (the TIDE feeds) non-locally.

URL: URL of the TIDE feeds desired. You copied this URL from the CSP in the TIDE Feed Filters section in step 3. Copy that URL here, or as a reminder, input:

```
https://csp.infoblox.com/tide/api/data/threats?type=host&class=phishing&period=30d
```

*Note the appended **&period=30d** at the end. This limits the dataset to the last 30 days, but you can omit it if you want to use all data from all time. You can also append **&rlimit=100** if you wish to limit the dataset to the first 100 entries, for example. Setting a limit will significantly shorten the time MISP will need to fetch this feed later.*

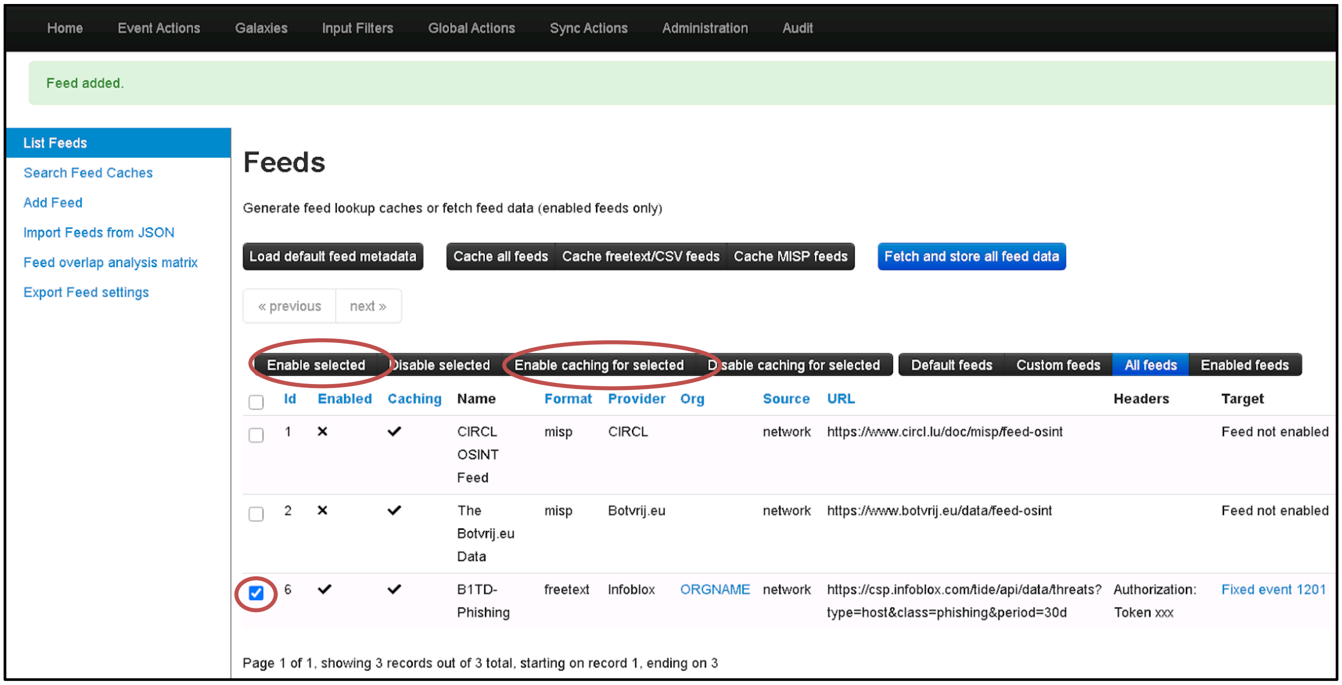
Source Format: Select Freetext Parsed Feed.

Headers: This is where your API key is input. Enter "Authorization: Token <YOUR API KEY>" into the textarea. Do not include the <> symbols or quotes.

Creator Organization: Select a recognizable organization. You can add new organizations to MISP later.

4. Click **Add** when done.

5. If the feed is not already, **enable** it.
    a. Click the **checkbox** on the left of the newly created feed.
    b. Select **Enable selected**.
    c. Select **Enable caching for selected** if you desire caching.



Feed added.

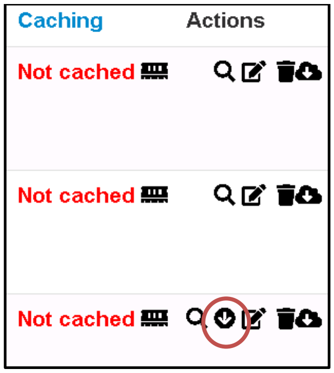
Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

□	Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target
□	1	✕	✓	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled
□	2	✕	✓	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled
☑	6	✓	✓	B1TD-Phishing	freetext	Infoblox	ORGNAME	network	https://csp.infoblox.com/tide/api/data/threats?type=host&class=phishing&period=30d	Authorization: Token xxx	Fixed event 1201

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

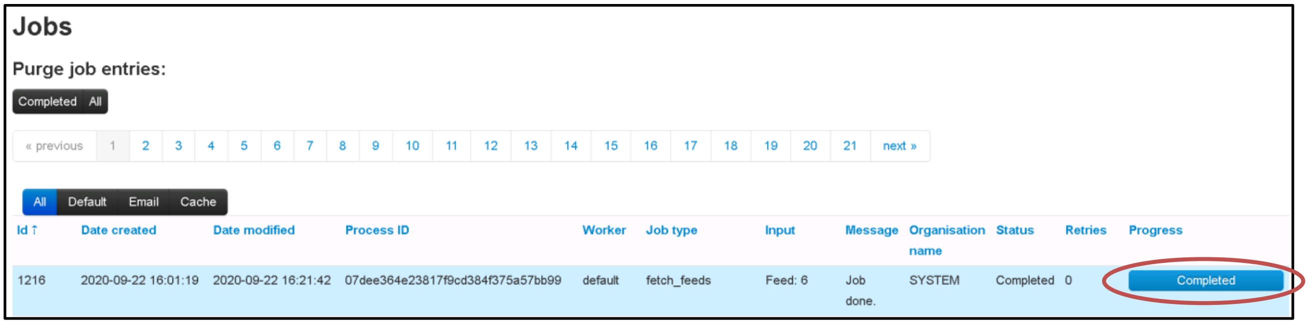
6. **Fetch** the feed.
    a. On the right end of the feed row, **click** the ⬇ icon to fetch all feed events.



Caching	Actions
Not cached	
Not cached	
Not cached	

7. Verify the feed fetch was executed.

    a. In the top bar, navigate to **Administration** → **Jobs**. Verify the fetch Completed.



Jobs

Purge job entries:

Id ↑	Date created	Date modified	Process ID	Worker	Job type	Input	Message	Organisation name	Status	Retries	Progress
1216	2020-09-22 16:01:19	2020-09-22 16:21:42	07dee364e23817f9cd384f375a57bb99	default	fetch_feeds	Feed: 6	Job done.	SYSTEM	Completed	0	Completed

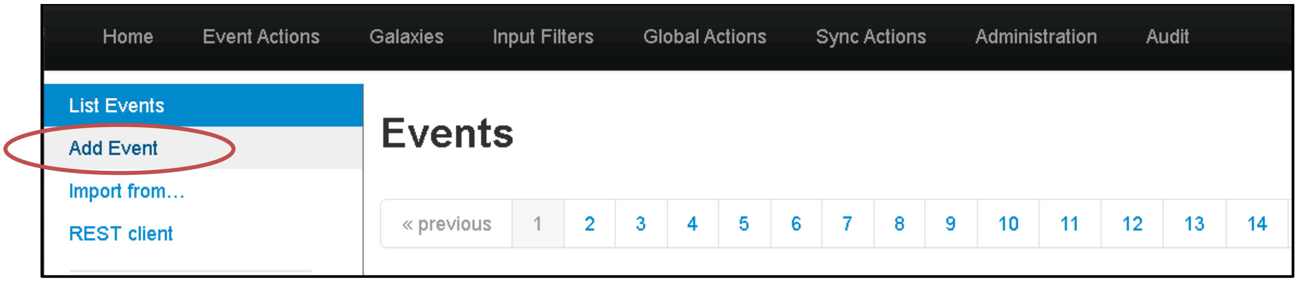
MISP Events & Attributes with TIDE

Here is where we will add a new MISP event and attribute to demonstrate they are being checked against our new TIDE feed.

1. Navigate to **Home**.

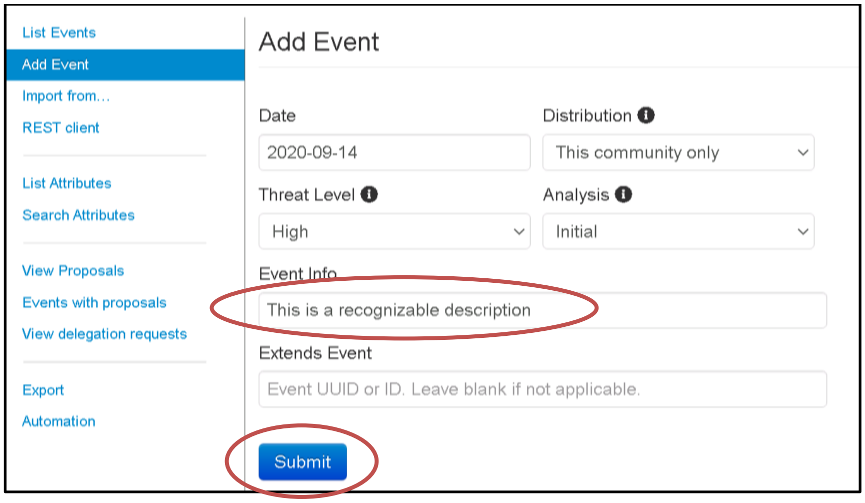
2. Add a new **Event**.

    a. Click **Add Event** in the left menu.



    b. Give the event **recognizable Event Info**. This could be a name, description, or anything otherwise distinguishable.

    c. Click **Submit** when finished.

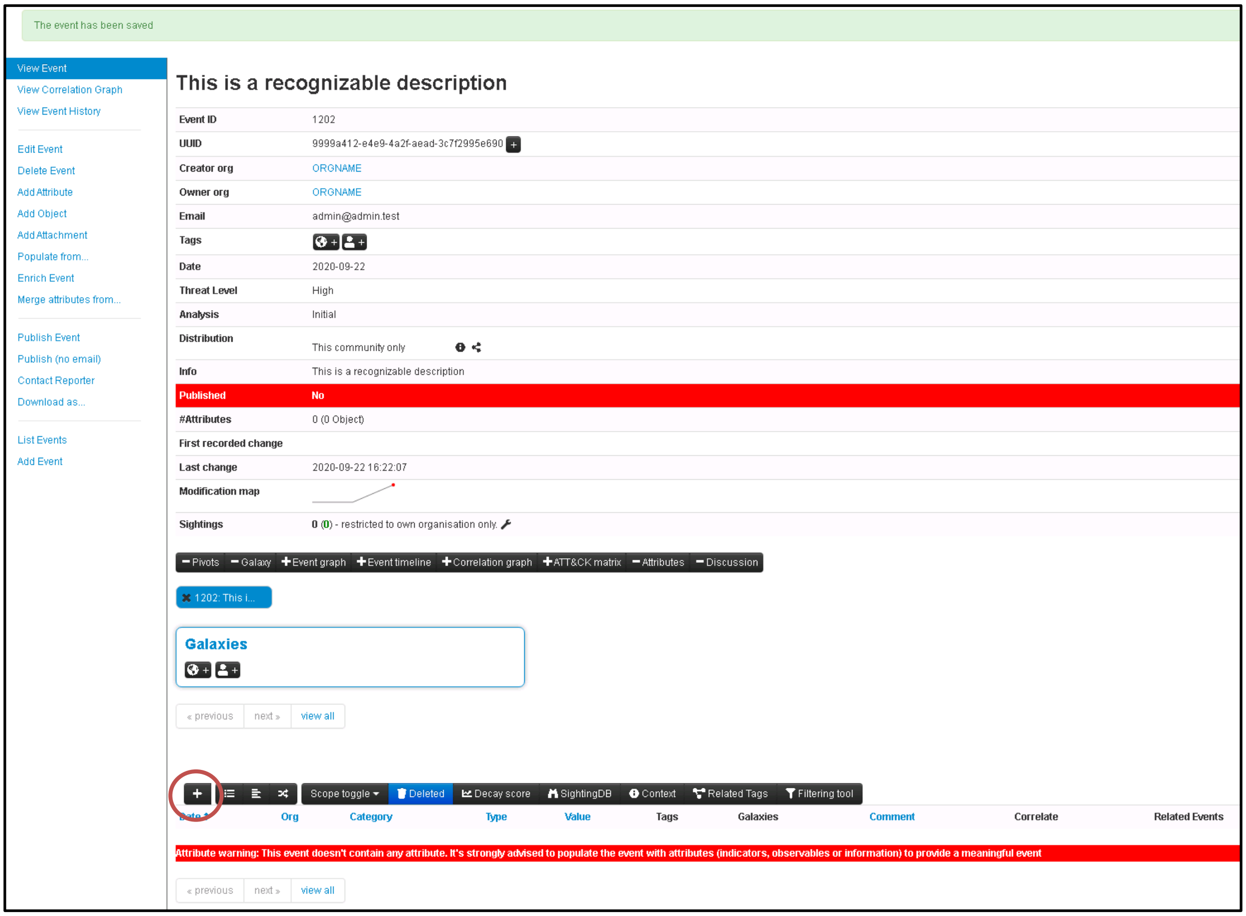


Add Event

Date	2020-09-14
Distribution	This community only
Threat Level	High
Analysis	Initial
Event Info	This is a recognizable description
Extends Event	Event UUID or ID. Leave blank if not applicable.

3. MISP will automatically open the new event for you. MISP events are populated with attributes, such as domain names, IPs, indicators, etc. **Add** a new attribute to the event.

   a. Scroll down and **click** the Plus button + to add a new attribute. A popup will appear.



The event has been saved

This is a recognizable description

Event ID	1202
UUID	9999a412-e4e9-4a2f-aead-3c7f2995e690
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	
Date	2020-09-22
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	This is a recognizable description
Published	No
#Attributes	0 (0 Object)
First recorded change	
Last change	2020-09-22 16:22:07
Modification map	
Sightings	0 (0) - restricted to own organisation only.

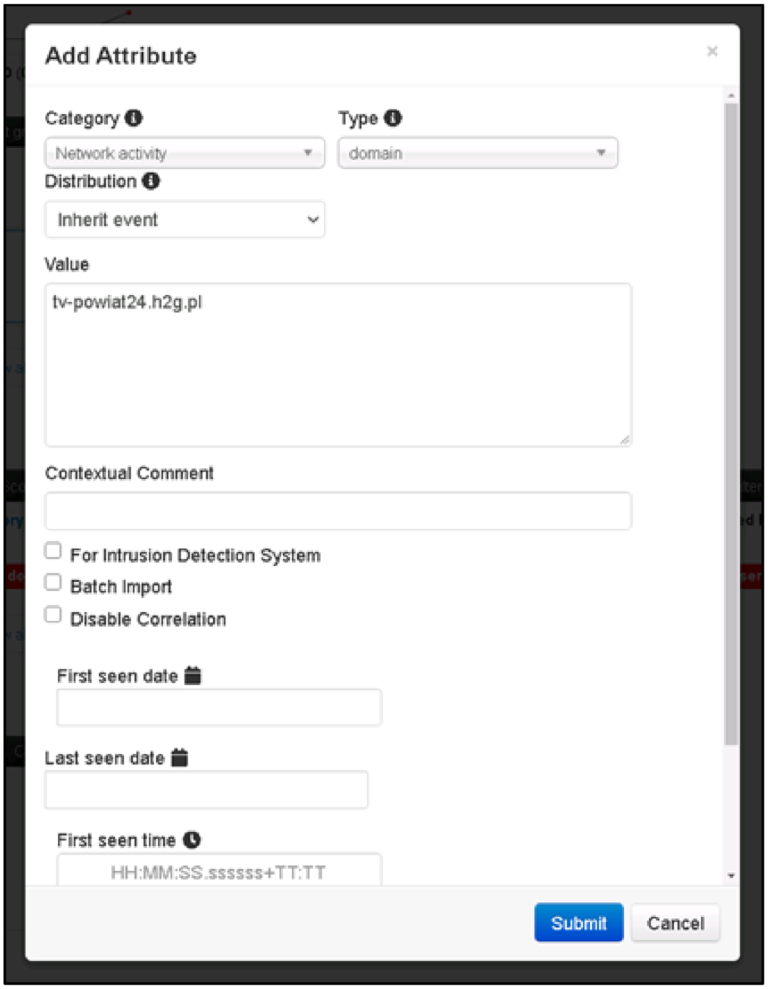
Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event

b. **Category**: Select Network activity.

c. **Type**: Select domain.

d. **Value**: Enter “tv-powiat24.h2g.pl”. This is a known malicious domain in the TIDE feed.

e. Click **Submit**.



Add Attribute

Category: Network activity

Type: domain

Distribution: Inherit event

Value: tv-powiat24.h2g.pl

Contextual Comment:

☐ For Intrusion Detection System

☐ Batch Import

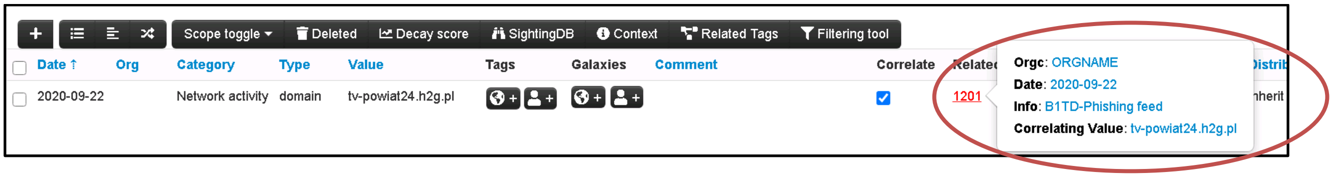
☐ Disable Correlation

First seen date:

Last seen date:

First seen time: HH:MM:SS.ssssss+TT:TT

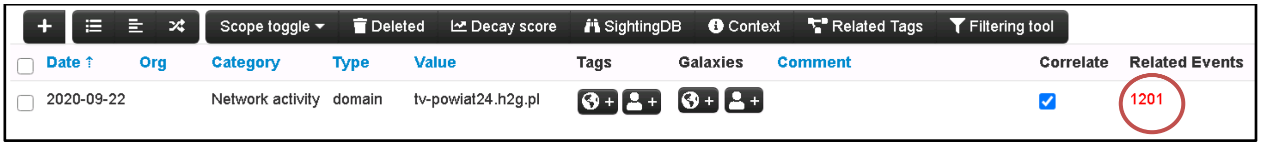
4. You will see the event ID of our new feed appears under Related Events for this attribute. Hover over the ID to verify.



☐	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related	Distrib
☐	2020-09-22		Network activity	domain	tv-powiat24.h2g.pl				☑	1201	nherit

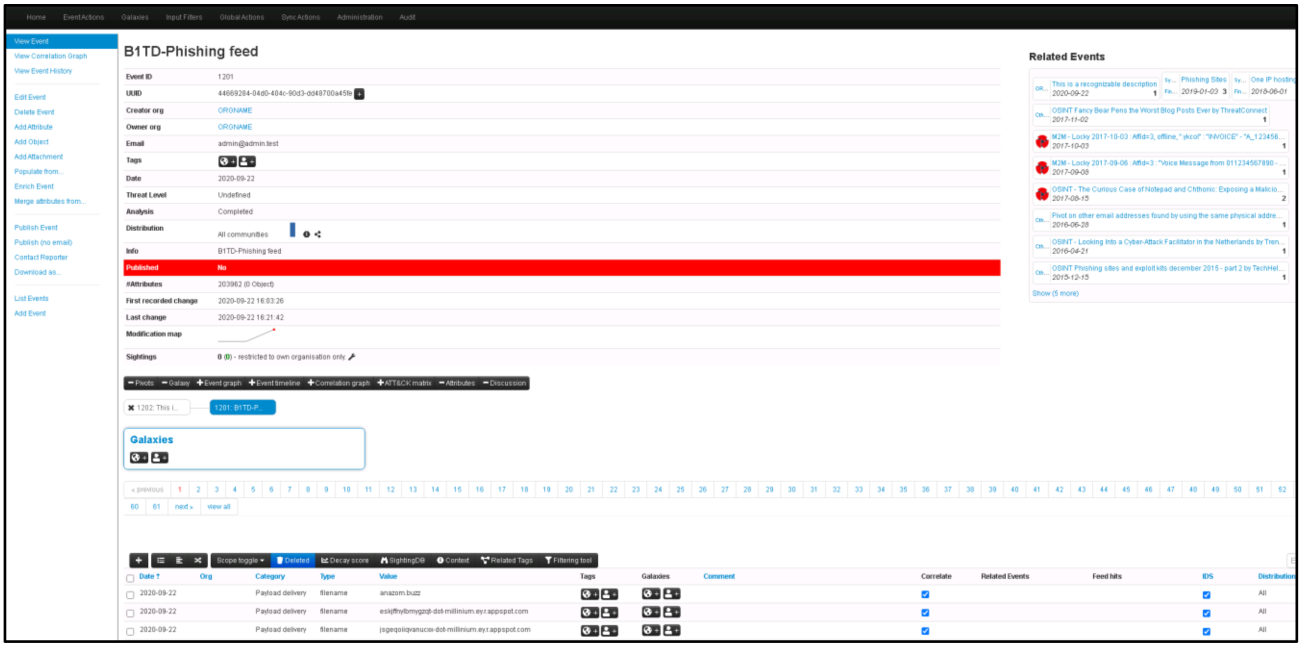
Orgc: ORGNAME
Date: 2020-09-22
Info: B1TD-Phishing feed
Correlating Value: tv-powiat24.h2g.pl

5. Click on the **ID** to view the feed event info.



□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
□	2020-09-22		Network activity	domain	tv-powiat24.h2g.pl				☑	1201

a. Shown is the feed event info.



B1TD-Phishing feed

Event ID	1201
UUID	44669284-04d0-404c-90d3-dd48700a45fe
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	
Date	2020-09-22
Threat Level	Undefined
Analysis	Completed
Distribution	All communities
Info	B1TD-Phishing feed
Published	No
#Attributes	203962 (0 Object)
First recorded change	2020-09-22 16:03:26
Last change	2020-09-22 16:21:42
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Related Events

OR... This is a recognizable description 2020-09-22 1
Sy... Fin... Phishing Sites 2019-01-03 3
Sy... Fin... One IP hosting 2018-06-01
Cth... OSINT Fancy Bear Pens the Worst Blog Posts Ever by ThreatConnect 2017-11-02 1
M2M - Locky 2017-10-03 : Affid=3, offline, ".ykcol" : "INVOICE" - "A_123456... 2017-10-03 1
M2M - Locky 2017-09-06 : Affid=3 : "Voice Message from 011234567890 - ... 2017-09-08 1
OSINT - The Curious Case of Notepad and Chthonic: Exposing a Malicio... 2017-08-15 2
Cth... Pivot on other email addresses found by using the same physical addre... 2016-06-28 1
Cth... OSINT - Looking Into a Cyber-Attack Facilitator in the Netherlands by Tren... 2016-04-21 1
Cth... OSINT Phishing sites and exploit kits december 2015 - part 2 by TechHel... 2015-12-15 1
Show (5 more)

□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
□	2020-09-22		Payload delivery	filename	anazom.buzz				☑			☑	All
□	2020-09-22		Payload delivery	filename	eskjffnylbmygzqt-dot-millinium.ey.r.appspot.com				☑			☑	All
□	2020-09-22		Payload delivery	filename	jsgeqoiiqvanucxi-dot-millinium.ey.r.appspot.com				☑			☑	All

Additional Resources

There are several ways to download MISP. Find instructions here.

MISP offers many optional modules for additional functionality. Find a summary of available modules and their installation instructions here.

For all things MISP, find the detailed administrative user guide here.

For more information about Infoblox's BloxOne Threat Defense, see the guide here.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com