AlienVault

Open Threat Exchange (OTX)™ User Guide

AlienVault Open Threat Exchange (OTX) User Guide

Table 1. Revision Table

Revision No.	Date	Revision Description
4	January 20, 2016	Added information about the API tab on the OTX Activity feed. See Connecting to the OTX API SDK.
3	October 22, 2015	• Added information about the new Activity tab. See Viewing the Activity Feed. • Added information that Whois domain look-up service is free from DomainTools at `domaintools.com` for the first 15 lookups per day, per customer, but that customers exceeding this number should subscribe to `domataintools.com`. See Table 6.
2	September 8, 2015	• Corrected the description of the data collected by OTX from USM/OSSIM users who opt into sharing IP Reputation-relevant information. See Information Collected by AlienVault. • Added the procedure, Updating or Adding a New Email Address. • Added the procedure Signing Up for OTX Using a Social Media Account. • Updated the definitions of URI and URL indicators of compromise in Table 2. Indicator of compromise (IOC) types.

Contents

About Open Threat Exchange (OTX)™

With this release, AlienVault introduces a new generation of its Open Threat Exchange (OTX)™ platform. Designed to engage the security and IT communities to collaboratively develop and easily use open threat data, OTX offers benefits regardless of level of expertise.

OTX allows security researchers and threat data producers to share research and investigate new threats.

Anyone interested in threat intelligence—not just AlienVault customers—can take advantage of OTX.

OTX enables you to accomplish the following:

- Receive new information about online threats by means of OTX "Pulses," composed of Indicators of Compromise (IOC). These IOCs describe the components that make up a threat. IOCs may, for example, consist of IPv4 or IPv6 addresses, CIDR, file hashes (MD5, SHA256), URLs, or Domains. (See About Pulses.)
- Verify their threat research findings through the OTX community, consisting of researchers from AlienVault Labs, strategic partners, and community developers.
- Benefit from the advanced research tools available from the OTX platform.
- Download OTX pulse information in commonly used file formats, for example, *CSV, OpenIOC 1.0* and *1.1, and STIX* to export pulse information to a variety of devices.
- Educate themselves on the latest threat research findings.
- Subscribe to information about specific threats in the form of pulses and track their evolution over a time.
- Subscribe to individuals in the OTX community, whose research contributions you particularly value.
- Publish their own findings in the form of OTX pulses about new threats they uncover, including new IOC instances.
- Comment on or add information to the pulses or IOCs published by other OTX community members.
- Instrument their security tools through the OTX DirectConnect API, which pulls the raw threat data from pulses into the security tools to allow data correlation and immediate notification of threat activity within their systems. The DirectConnect API is free to OTX users for any non-commercial use. Commercial partners use the API under the conditions described in a license agreement.

About Pulses

The OTX community reports on and receives threat data in the form of pulses. An OTX pulse consists of one or more indicators of compromise (IOCs) that constitute a threat, a campaign, or an infrastructure used by a malicious actor. IOCs act as vectors for active threats to networks and computers.

About Indicators of Compromise

An Indicator of Compromise (IOC) is an artifact observed on a network or in an end point judged with a high degree of confidence to be a threat vector.

Table 2 lists the different IOC types associated with pulses. Each pulse may contain one or more IOCs.

Table 2. Indicator of compromise (IOC) types.

IOC Type	Description
IPv4	An IPv4 address used as the source/destination for an online server or other computer suspected of malicious activity.
IPv6	An IPv6 address used as the source/destination for an online server or other computer suspected of malicious activity.
domain	A domain name for a website or server suspected of hosting or engaging in malicious activity. Domains encompass a series of hostnames.
hostname	The hostname for a server located within a domain, suspected of malicious activity.
email	An email address associated with malicious activity.
URI	A uniform resource identifier (URI) describes the explicit path to a file hosted online, which is suspected malicious activity.
URL	Uniform resource locations (URLs) summarizes the online location of a file or resource associated with suspected malicious activity.
filepath	Unique location in a file system of a resource suspected of malicious activity.
FileHash-MD5	An MD5-format hash that summarizes the architecture and content of a file deemed suspicious.
FileHash-SHA1	A SHA1-format hash that summarizes the architecture and content of a file deemed suspicious.
FileHash-SHA256	A SHA256-format hash that summarizes the architecture and content of a file deemed suspicious.
Imphash (import hash)	An imphash-format hash that summarizes the architecture and content of a file deemed suspicious.
PEhash	A PEhash-format hash that summarizes the architecture and content of a PE-executable file deemed suspicious.

IOC Type	Description
CIDR (classless inter-domain routing)	Description of both a server IP address and the network architecture (routing path) surrounding that server, suspected of malicious activity).
mutex	Name of a mutex resource describing the execution architecture of a file, which may be malicious.
CVE (Common Vulnerabilities and Exposures)	CVE reference to network exhibiting malicious behavior.

Creating an OTX Account

This topic describes how to sign up to use the new OTX platform.

If you previously signed up for an OTX account, you must still complete the OTX signup process to access the enhanced OTX platform. In this case, it is important that you provide the same email address that you previously used when you registered for an OTX account. This allows OTX to identify your existing account record.

Note: USM and OSSIM users must explicitly connect their instances to OTX to receive its benefits. For information, see *Using USM and OSSIM 5.1 with OTX* on the AlienVault Documentation Center (`https://www.alienvault.com/documentation`).

To create an OTX account

1. Go to `https://otx.alienvault.com`.
2. On the upper-righthand corner of the home page, click **Sign Up** (Figure 1).

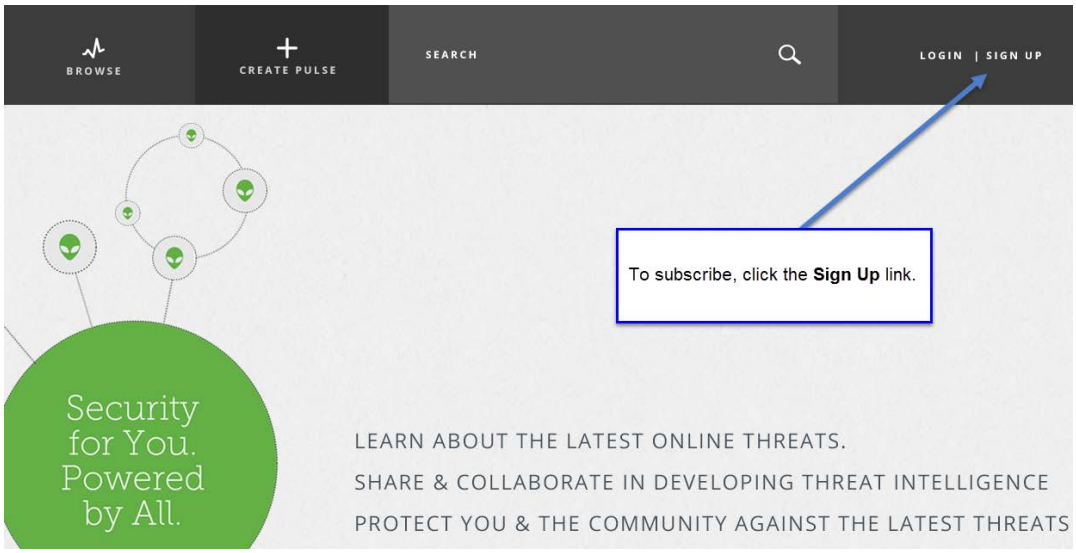

Figure 1. Open Threat Exchange home page.

3. Fill out the form that appears, entering the following data:

   a. Username

   Note: Make sure to select a username that protects your anonymity, in other words, a social media "handle." OTX identifies you to other users in the community based on this handle.

   b. Email address.

   c. Password of your choosing.

   d. Retype the password to confirm it.

4. Click **Sign Up.**

   A page appears informing you that a verification email with a link to OTX was sent to the email address you provided.

   Note: If you do not receive the email, contact `otx@alienvault.com`.

5. After you receive the email, click the link that takes you to the confirmation page; and click **Confirm.**

   This takes you to the Activity feed in OTX (**https://otx.alienvault.com/activity/new**) where you immediately see pulse activity.

Signing Up for OTX Using a Social Media Account

Users can sign up for OTX using their social media accounts, such as Facebook, Twitter, Google+, or LinkedIn.

OTX then authenticates users through their social media credentials, and in the case of Twitter, prompts you to enter your email address.

To sign up with one of your social media accounts

1. Go to `https://otx.alienvault.com.`
2. On the upper-righthand corner of the home page, click **Sign Up** (Figure 1).
3. Click on the appropriate social media icons at the top of the page.
4. Authorize AlienVault to use your social media account credentials to create an OTX account either by clicking **Sign In** or **Accept.**

   Note: The exact wording and submission action differs depending on the social medium.

5. On the **Sign Up** page, confirm that you intended to sign up using your social media account.
   a. Review the pre-filled username.
   b. Type the email address associated with your social media account.
   c. Click **Sign Up.**

   A page appears informing you that a verification email with a link to OTX was sent to the email address you provided.

   Note: If you do not receive the email, contact `otx@alienvault.com`.

6. After you receive the email at the address you provided, click the link to go to the confirmation page.
7. On the **Confirmation** page, verify that the email is valid for your username on the social media account you used; then click **Confirm.**

   This takes you to the Activity feed in OTX (**https://otx.alienvault.com/activity/new**) where you immediately see pulse activity.

Reviewing Your Account Settings

The Settings page contains your OTX account data. On this page, you can perform the following tasks:

- Change your OTX password.
- Control the types of notifications you receive as email.

- Access your OTX account key, used to connect
  - OTX to USM/OSSIM

  or
  - OTX DirectConnect API, or one of its plug-ins, such as the Bro-IDS.
- Update or add an email address. See Updating or Adding a New Email Address.
- Personalize your OTX avatar. See Personalizing Your OTX Avatar.

To go to the OTX Settings page

1. Click on your username in the upper right-hand corner of any OTX page, next to the gear icon (Figure 2).

   

   Figure 2. Link to your account information on the Settings page.
2. Click **Settings.**

Connecting to the OTX API SDK

Engineers who want to take advantage of the OTX threat intelligence within their intrusion detection monitoring tools, including USM or OSSIM, can integrate it using our DirectConnect agents. In addition to USM and OSSIM, AlienVault currently provides the following connectors:

- OTX-Apps-Bro-IDS
- OTX-Apps-TAXII

If you don't find a connector for your product, you can develop one of your own, using the OTX Direct Connect SDK, available in the AlienVault Labs GitHub library, and written in JAVA and Python.

To connect to the OTX DirectConnect agents

1. Click the API tag at the top of the OTX Activity feed.
2. Click the label of the connection agent you want to use.

   This takes you to the GitHub page for your connector selection.

   If you want to connect to USM or OSSIM, follow the instructions provided when you click their respective labels and copy your OTX key, displayed on the right-hand side of the page.

To access the SDK

1. Go to **Settings > Account > Settings**.
2. Click **Use the OTX API SDK.**

   This takes you to GitHub for AlienVault Labs, where you can make your selection.

Updating or Adding a New Email Address

This procedure describes how to update or add an email address, and how to make a new one primary.

To change your email address or to add a new one

1. Within OTX, click the gear wheel at the upper-right and select **Settings.**
2. Under **Account Settings,** click **ADD E-MAIL.**
3. In the **Enter New Email Address** field, type the new or corrected email address.

   OTX sends an email to the email you typed that contains a confirmation link.
4. Click the link to go to a confirmation page.
5. Click **CONFIRM.**

   This takes you to the OTX Activity feed.
6. Go to Settings > **Account Settings**, where you now see the new email address in addition to the previous one.
7. (Optional) To remove the previous email address, or just make it primary, click **MAKE PRIMARY** *next to the email you just added.*

   The previous email address moves on top of the newly added email address, and two buttons, MAKE PRIMARY and REMOVE, display next to it.

   `Verified Primary` now displays under the new email address.
8. (Optional) To delete the previous email address, click **REMOVE.**

Personalizing Your OTX Avatar

AlienVault OTX creates a default avatar for all new users. If you want to change your avatar, you may upload an image of your choosing.

To change your OTX avatar image

1. From the OTX Activity feed, click on your name at the upper right-hand corner of the page and select **Settings.**
2. Hover with your cursor over your avatar image to display the word “Edit,” then click it.
3. On the Change Avator popup, under **Upload Avatar,** click **Browse** and navigate to a JPG or PNG file to upload.
4. Select the file and click **Open,** then **Save.**

Managing Pulse Subscriptions

All OTX members receive pulse information through their OTX Activity feed, as well as updates about pulses through email. This information appears as soon as you open an OTX account.

OTX users automatically receive all pulses, and any updates to them, that originate from AlienVault.

USM and OSSIM users optionally contribute data to IP Reputation.

You may also subscribe to OTX community members, thereby subscribing to all of the pulses they create and update.

USM and OSSIM OTX subscribers, and others whose security tools use agents such as Suricata or Bro can be configured to use raw OTX data can to enhance their threat detection capabilities.

Note: OTX data may not be used for commercial purposes. However, commercial users can apply to AlienVault through otx@alienvault.com for a license.

Subscribing to a Pulse

Subscribing to a publicly created pulse allows automatic export of its raw data to your security tools.

To subscribe to a pulse

1. Launch the OTX from `https://otx.alienvault.com` and log in.
5. From the OTX **Activity** feed, perform either of the following to locate a pulse:
   - Scroll through the list to find the pulse you want to subscribe to
   - Perform a search for the pulse from the **Browse** page, if you know its name.
6. Click the pulse.

   A detailed view of the pulse appears in the section at the right (Figure 3).

Figure 3. Pulse Details page in OTX, showing Subscribe/Unsubscribe toggle.

7. Click **Subscribe,** located under the pulse name.

Unsubscribing from a Pulse

When you unsubscribe from a pulse, you still receive information about the threat in your OTX Activity feed in the web UI, but no raw data is pulled for that pulse into your security tools for correlation.

To unsubscribe from a pulse

1. Locate the pulse you want to unsubscribe from in one of the following ways:
   - Scroll through the list to find the pulse.
   - Perform a search for the pulse, using its name, a key word, or an indicator.
8. Click the pulse.
9. On the **Pulse Details** page, click **Unsubscribe.**

Subscribing to or Following Other OTX Contributors

You may subscribe to or follow public OTX contributors. The difference between subscribing to and following a contributor consists of the following:

- ***Subscribing*** tells OTX DirectConnect to pull all of the contributor's pulses or IOCs into your security tools, in the case of USM/OSSIM, this occurs in 15-minute increments.

  Their pulse and IOC contributions also automatically appear in your OTX Activity feed. You also receive emails every time they update one of their pulses or when they create a new pulse.

- ***Following*** tells OTX to show that person's pulses within your Activity feed, but not to pull raw data from their contributions into your security tools through DirectConnect. Following someone is the right approach if you only want to see their pulses in that location.

To subscribe to an OTX contributor

1. Click the username of the OTX contributor to whom you want to subscribe from any of the following locations:
   - One of their pulses (Figure 4).

Figure 4. Subscribing to a contributor from one of their pulses.

   - Their username on the **Recommended People to Follow** section of the OTX Activity feed (Figure 5).

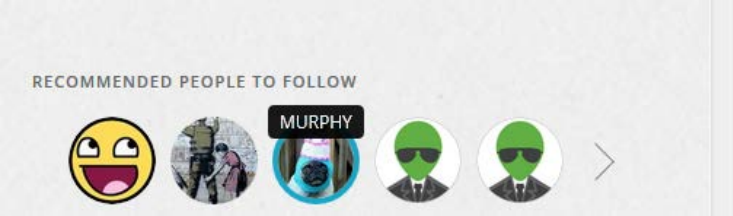

Figure 5. Recommended People to Follow section of the Activity feed.

Note: OTX populates the section in your Activity feed called **Recommended People to Follow,** based on the number of pulses that they have created and the number of people who have subscribed to them.

This takes you to an activity feed for that contributor, displaying all of their pulse and IOC contributions.

2. Click **Subscribe,** located under the contributor username (Figure 6).

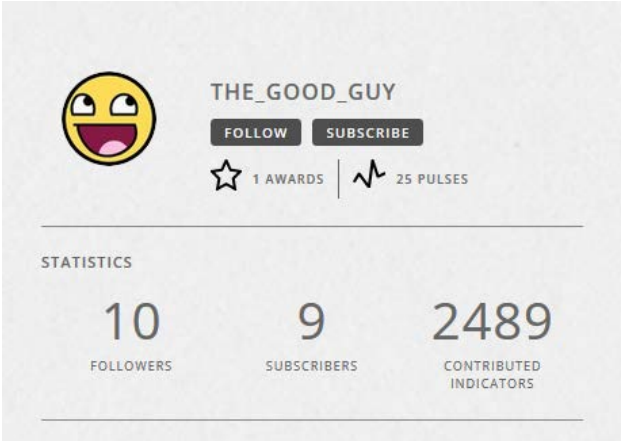

Figure 6. Subscribing to a user from their Activity feed.

To unsubscribe from an OTX contributor

- From the **Activity** feed for the contributor, click **Unsubscribe.**

Note: When you click **Unsubscribe** next to where their name appears on one of their pulses, you unsubscribe only from that pulse.

To follow an OTX contributor

- From the **Activity** feed for the OTX contributor, click **Follow.**

Note: You can only follow an OTX contributor from their Activity feed.

To unfollow an OTX contributor

- From the **Activity** feed for the OTX contributor, click **Unfollow.**

About Contributing Threat Data to OTX

OTX community members can contribute threat data to OTX in the following ways:

- When they create or comment on pulses.
- When they opt into allowing OTX to access any IP Reputation data generated within their own system environment.

Voluntary and Anonymous Data Contribution

All data contributed to OTX are completely voluntary and anonymous. No data submitted to OTX through USM can be used to identify any of the following:

- Any individual
- Any individual system's data
- Any individual system's internal IP traffic

Information Collected by AlienVault

When you contribute to OTX, AlienVault collects only the following information:

- External IP addresses that try to or succeed in communicating with your system.
- Any traffic patterns.
- Any timestamps, for example, security identifiers (SIDs) and counts from intrusion detection system (IDS) signatures.
- Any alarms generated based on observed traffic.
- IOC activity data within your environment for analysis against pulses.

Viewing the Activity Feed

The OTX Activity feed consists of two tabs:

New Pulses

Activity

New Pulses

The New Pulses tab of the Activity feed consists of two primary sections, described in Table 3:

- A pulse activity feed
- Your OTX user profile

Table 3. OTX Activity feed sections and fields.

Section/Field	Description
Pulse activity feed	• Displays all of the pulses identified by the OTX community and AlienVault Labs with or without subscribers, including the pulse creation or modification date. • Displays only the pulses from the activity feed that have subscribers.
Profile	Profile data appears on the Activity feed, as well as on a profile page you can link to from here.
• Username	Your OTX username or “handle.”
• Awards	Details about any OTX awards you win. For example, OTX beta program participants receive an award.
• Pulses	Number of pulses you created. For information about creating pulses, see Creating a Pulse.
Statistics	Contains the following elements, which also appear on your profile page:
• Followers	See description below.
• Subscribers	See description below.
• Contributed indicators	Number of indicators of compromise you identified, whether in one or multiple pulses.
Recommended People to Follow	Contains the following elements:
• Followers/Following	Number of OTX community members who follow you or whom you follow. See Subscribing to or Following Other OTX Contributor.
• Subscribers/Subscribing	Number of OTX community members who subscribe to you or to whom you subscribe. See Subscribing to or Following Other OTX Contributor.

Activity

When you click the Activity tab, you can see these important notifications:

- Comments by an OTX member on one of your pulses.
- Creation of a new pulse by an OTX member you subscribe to or follow.
- New comments by a subscriber to one of your pulses.

Viewing Pulses

You can view OTX pulses in two formats:

Concise View

Detailed View

Concise View

The pulse section of the OTX Activity feed shows all active pulses in concise format by date created or updated, with the latest activity always top-most (Table 4).

The concise view of each pulse shows:

- Avatar of the user who created the pulse.
- Creation date of the pulse or the date it was last updated with new information.
- A concise description of the pulse.
- Up to four tags (**Detailed** view shows tags in excess of four) that OTX analytics tools or the pulse creator uses to categorize activities related to a pulse.
- Number of pulse subscribers.

Table 4. Pulse concise view, sections and fields.

Section/Field	Description
Avatar	Located at far-left, the avatar of the user who created the pulse. If the pulse is from AlienVault Labs, the avatar is the Alien.
Created/Modified	Time elapsed since pulse creation or pulse modification occurred, in either hours or days.
Username	Username of pulse creator.
Description	Fragment of pulse description. To see more, click the description.

Section/Field	Description
Tags	Up to four tags (**Detailed** view shows any tags in excess of four) that either OTX analytics tools or the pulse creator used to categorize possible indicators. These are not necessarily threat vectors, however.
Subscribe/Unsubscribe	Number of subscribers to this pulse. You can also use the link to subscribe to the pulse displayed.
Like/Unlike	Similar to the Facebook "Like" thumbs-up icon, a clickable link that you can use to show appreciation of or dissatisfaction with the pulse displayed.

Detailed View

The Pulse Details view provides a detailed analysis of the pulse and any associated IOCs.

To get details about a pulse

- Click the pulse.

  Pulse Details appears, with the Activity feed displaying in a navigation pane at left.

Table 5 describes the elements of a pulse in Pulse Details view.

Table 5. Pulse Details, sections and fields.

Section/Field	Description
Closure icon	Consists of an "X." Clicking this icon returns you to the Activity feed in concise view.
Clone icon	A time-saving device that allows you to create a duplicate of the pulse as a starting point to creating a new pulse sharing many of the same features. See **Figure 7.**
Facebook, Twitter, Google+, and LinkedIn icons	Links to share a pulse with your communities on these social networking sites. See **Figure 7.**
List of formats available for file downloads	Expanding this list allows you to select a download format compatible with any third-party applications you may use. See **Figure 8.**
• CSV	Comma Separated Values format that can be easily imported, exported, and parsed by multiple applications and scripting languages.

Section/Field	Description
• OPENIOC 1.0 and OPENIOC 1.1	Extensible XML schema used to describe the technical characteristics identifying a known threat, attacker methodology, or other evidence of compromise. See http://www.openioc.org.
• STIX	A collaborative, standardized language to represent structured cyber threat information. See https://stix.mitre.org.
Statistics dashboard	Displays high-level statistics about the pulse (Figure 8):
• Related Pulses	If available, number of pulses related to this pulse. For example, this may consist of pulses with one or more of the same IOCs.
• Indicators	Number of associated indicators.
• TLP Classification	Traffic light protocol color as appropriate to U.S. Department of Homeland Security guidelines. For more information about these, see Creating a Pulse.
• Privacy Setting	Pulse creators have the ability to make a pulse public (viewable by the OTX community) or private (viewable only to themselves or a select group). For more information about these, see Creating a Pulse. An open eye means that the pulse is Public, in other words, it may be viewed without restrictions.
• Subscribe/Unsubscribe	See description in Table 4.
• Like/Unlike	See description in Table 4.
Tags	Tags associated with the displayed pulse. Tags identify possible IOCs. These are not necessarily threat vectors, however. These are added at pulse creation time, either manually by the pulse author or automatically by OTX analytics tools.
Reference	Link to the web page used to extract information on the pulse, such as when it was first seen and other details.
Pulse description	Description of the pulse by the pulse creator.
Threat Infrastructure	(Optional) When available, national flag and name of one or more geographic locations for indicators associated with the displayed pulse. The number shown at the right represents the number of indicators observed for that location.

Section/Field	Description
Indicator Type list	Displays indicator types associated with the pulse, as well as the actual indicator, such as IP address, domain, or the actual hash, if a hash file such as MD5 or SHA-1 (Figure 10).
Targeted Software	When the pulse contains CVE entries, these refer to a network exhibiting malicious behavior.
Comments	Any comments OTX community members may have left about this pulse, including new information.

Figure 7. Clone icon, social networking icons, and tags in Pulse Detail view.

Figure 8. Pulse file download list.

Figure 9. Pulse Details (top half), showing Threat Infrastructure and Targeted Products.

Adjusting the Number of Indicators Displayed in Pulse Details

This topic describes how to change the number of indicators displayed in the indicator list of the Pulse Details page (Figure 10).

To adjust the number of indicators in the display

- Click the **Show Indicators** list to view more, and select a new value in increments of 25, 50, or 100.

  The default number for display is 10.

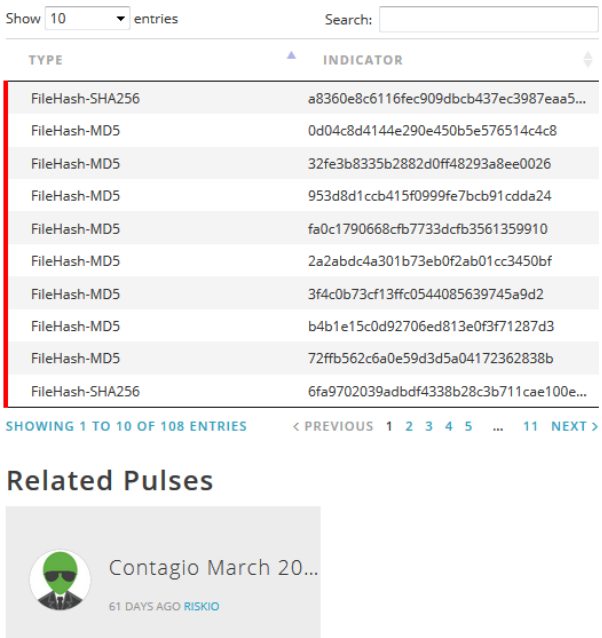

Figure 10. Indicator Type list and Related Pulses.

Submitting a Pulse Comment

You can add any comments you might have on a pulse to the **Comments** field. For example, you might want to share any experience you have had with the same indicators.

To submit a comment about a pulse

1. Type your comments within the **Comments** field at the bottom of Pulse Details.
2. (Optional) To remain anonymous, select **Comment Anonymously.**
3. Click **Submit.**

   Your comment appears at the bottom of the page with your avatar and the time when you created the comment.

Note: If you elected to comment anonymously, OTX displays the default avatar.

4. To remove a comment, click **Remove.**

About Indicator Details

The Indicator Details pages can provide a wealth of background information on any given indicator. This information is based on both analysis by the OTX analytics engine, as well as data from third-party security databases like Google Safe Browsing, URL Void, or VirusTotal. This helps you to better recognize it and assess its threat potential if it communicates with assets in your environment.

Not all Indicator Details pages include the same amount of data and some have little to no data. When no data are present it can indicate that either of the following about the file:

- The file is not malicious
- Neither AlienVault nor its partners have yet analyzed the file.

The data appearing on the Indicator Details page is based on the analysis of the indicator by AlienVault or its research partners.

Viewing Indicators

You may access Indicator Details pages by either searching on an indicator, if you know its IP, domain, or hash, or by clicking it from within the **Indicator Type** list of the Pulse Details page.

To get details about an indicator

1. Go to **Pulse Details,** and from the **Indicator Type** list, click the indicator you want more information about.
2. To get detailed information about the particular indicator, click **Details,** located under **References,** as shown in Figure 11.

Figure 11. Sample References data.

This displays the **Indicator Details** page (Figure 12).

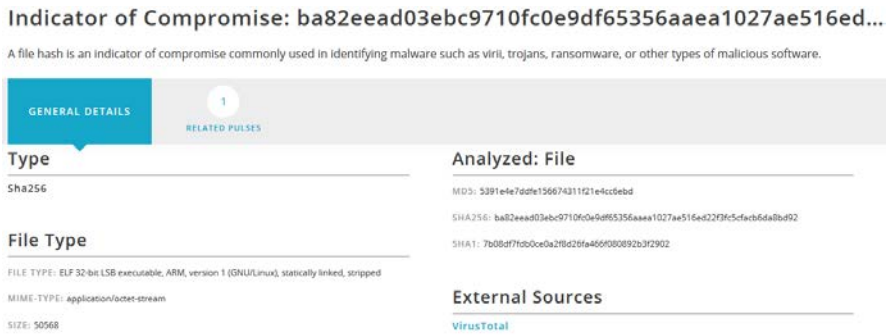

Figure 12. Sample Indicator Details page, **General Details** section.

Depending on the particular indicator of compromise, the **Indicator Details** page can be very simple or it can include a great deal of research results. The following pages describe these categories of information in order of their appearance on the page.

Header Information

The Indicator of Compromise Details page always identifies the Indicator of Compromise IP, domain, or hash in its heading (Figure 12), followed by a description of the threat posed by the indicator.

General Details

This section of the Indicator Details page (Table 6) provides basic reference information for all indicator types.

The information displayed under this heading depend on the indicator type and also on how much research data is available for any given indicator at any given time from AlienVault or its partners.

Table 6. General Details information.

Information Category	Description	Example
Type	Type of indicator of compromise.	IPv4, IPv6, URL, URI, CVE, domain, and hash files. For a complete list, see **Table 2**.
Basics	If available, shows origin, ASN/Owner, date first seen, IP address and country of origin, if relevant.	
ASN/Owner	Registered owner of an IP address. Includes the city and country, including the national flag, associated with the IP.	AS3269 Telecom Italia S.p.a.
First Seen	Date and time the indicator was first reported.	
Last Seen	Date and time the indicator was last reported.	
Creation Date	Date the indicator was first seen by AlienVault	
Last Modified	Date indicator was last modified or opened, as applicable.	
External Sources	Data from the security research community.	This data can be helpful in analyzing indicators and potential threats from a variety of perspectives. This helps determine if malicious activity is present.
Whois	Whois is a registry service offered by third-party vendor, DomainTools at `domaintools.com`, which shows who owns a particular website, domain, or host name. This tells you when a website was created. **Note:** DomainTools offers 15 free Whois domain look-ups per day, per user to AlienVault customers. If you exceed 15 domain look-ups in a day, we recommend that you become a DomainTools subscriber. A DomainTools subscription is not part of your AlienVault license.	If many domains point to a web page, the web page may be acting as a server to multiple secondary pages hosting malware. One example of this might be the use of a URL for malicious intent that looks at first glance like a well-known legitimate site, for example, **www.goooogle**.com. It helps to examine the owner of a site in relation to its Geolocation.

Information Category	Description	Example
VirusTotal	When present, shows any results for the indicator on VirusTotal, a free virus, malware, and URL online scanning service. File checking is done with more than 40 antivirus solutions.	
Alexa	IPs affiliated with this indicator. Provides information on how long a site has existed, how many page views it receives per day, and similar information that contributes to the Alexa "popularity" ranking of a website.	In some cases, Alexa may not have enough information to rank a web site.
URLVoid	Analyzes websites through multiple blacklist engines and online reputation tools. Helps detect websites involved in malware incidents, fraudulent activities, and phishing.	
DNSBL	DNS-based black hole list. This is a list of locations on the Web responsible for spamming.	
Potential Risk	Seen for IPv4, IPv6, domain, URL, and URI indicators.	
Google Safe Browsing	Google-provided list of URLs for web resources that contain malware or phishing content. The Google Chrome, Apple Safari and Mozilla Firefox web browsers use the Google Safe Browsing service to check pages against potential threats.	An indicator with a Google Safe Browsing checkmark, signifies that the indicator is listed there.
References	Textual references to this hostname.	`https://info.publicintelligence.net/FBI-HackToolsOPM.pdf`
Threat Summary		Seen with IPv4, IPv6, domain, URL, and URI indicators.

Information Category	Description	Example
Threat Score	OTX IP Reputation ranking of threat, based on its ranking criteria of IP reliability and priority.	**IP reliability ranking—**Based on the relative number of reports on a malicious IP in relation to others reported. If, for example, OTX receives 10 reports on a given IP address versus 20 on another, it gives the IP with 10 reports a lower reliability ranking than the IP with 20 reports. **IP priority ranking—**AlienVault ranks IP address priority, based on the behavior associated with each IP address listed. For example, an IP address used as a scanning host receives a lower priority than an IP address known to have been used as a Botnet server
	Malicious host activity associated with this IP, as defined by OTX IP Reputation.	Information might include whether or not the IP was previously malicious. Malicious host activity examples: • Scanning host • Malicious host • Spamming • Command and Control (C&C) • Malware domain • Malware distribution • Malware IP
Threat Findings	Displays a graph line with date range, starting with the date the IP was first reported seen. Findings may consist of any of the malicious host activities described under Threat Score. **To see the findings** • Click **See Findings.**	If the activity were C&C, for example, the threat findings might describe a command and control server hosting the malware. Command and control servers transmit instructions remotely to the malware on infected hosts. Any interaction with a known command and control server signals a system compromise. The risks associated with C&C servers include widespread malware infection (potentially beyond a single system), service disruption, session hijacking, information leakage, and more.
Server Response	Sometimes noted with malicious URLs.	URLs can be used to define the location of a malicious file or a watering hole attack hosted from a website.

Information Category	Description	Example
		If a well-known site is supposedly down it may be a bad sign. Server response tells you if the server is reachable and working as it should.
Date	Date server response received.	
Content-Length	HTML files: Size of the page denoted within the Content-Length metadata. Entity-header field indicating size of entity-body sent to recipient in OCTETs.	If size is longer than expected for the type of file, the file may be hiding a large amount of source code. This might be an indication of a drive-by download attack, a malware delivery technique that is triggered simply because the user visited a website.
Server	The operating system, web server or application that presents the page to the Internet.	Microsoft-IIS/6.0
Content-Type	Header field that specifies the nature of data in an email.	Text/html
X-Powered by	Server-side Web application framework.	ASP.net
CVE Overview	Common Vulnerabilities and Exposure. A dictionary of publicly known information security vulnerabilities and exposures.	Includes specifics such as software versions considered vulnerable. See `http://cve.mitre.org.`
CVSS Severity	Common Vulnerability Scoring System criteria for assessment of CVE severity.	Based on U.S. Department of Homeland Security National Vulnerability Database describes the nature of vulnerabilities hackers seek to exploit in commonly used software, such as Java Runtime Environment. See `https://nvd.nist.gov/CVSS-v2-Calculator#score`.
Generated-on-Datetime	When the CVE was logged with mitre.org.	2013-02-04T10:22:00.000-05:00
Access-Vector	Part of Base Score Exploitability Metrics for CVSS v2 vector.	Local, Adjacent Network, Network.
Integrity-Impact	Refers to how well-constructed the vulnerability is.	None, Partial, Complete.
Access-Complexity	Level of difficulty to exploit the vulnerability.	High, Medium, Low.

Information Category	Description	Example
Availability-Impact	Ease with which malware can be repurposed for other goals.	None, Partial, Complete.
Authentication	Pervasiveness of the vulnerability within the application.	Multiple, Single, None.
Score	CVSS/CVE score. Consists of Base, Temporal, Environment, and Overall scores. See https://nvd.nist.gov/CVSS-v2-Calculator#score.	Scores are from 0 through 10.0
Confidentiality-Impact	Special knowledge required to exploit the vulnerability.	None, Partial, Complete.
File Type	Describes indicators consisting of hash files.	Risks posed by hash files include viruses, Trojans, and ransomware.
File type	Type of file, including details of the operating system it is intended to exploit, including the location in the OS where it resides.	PE32 executable; DLL; Intel80386, for MS Windows
MIME type	MIME headers describe for browsers how to execute certain types of code or files.	Application/Octet-stream
Subsystem	Location where the file operates.	Windows GUI
Size	File size in bytes	49152 bytes
File Classification	Format for classifying executables, object code, DLLs, FON-Font files and others used in 32-bit and 64-bit versions of Windows operating systems.	PEXE (Portable Executable)
Analysis Date	Date on which static, dynamic, and network analyses performed by AlienVault or its partners.	June 16, 2015, 4:35 pm
Communications Samples	Any malicious files that open a connection to the IP address, domain or hostname.	

Information Category	Description	Example
Analyzed: File	Different hashes of a file.	MD5: 2518be42bb0713d29b60fd08d3b5fed4 Sha256: a893eee6e2518037f0db513700f4600f98e8329a63aa31476ae367cab24d640b Sha1: 6c4d8ee10bf07beb7c8eeacf95611ee2e67d04e0 IMPHASH: 5238a22fdc55fe3e5c44a175ce3a6765 PEHASH: e1851cc0e517cef201cbf92d31d519d26c977f90
Yara Tools	Tools aimed at helping malware researchers to identify and classify malware families. Descriptions of malware families come from textual or binary information contained in samples of those families.	

Related Pulses

This section, where present, provides an overview of any other pulses that contain the same indicator.

To get information about the related pulse

- Click the pulse.

File Analysis

Under the **Related Pulses** section of the Indicator Details page for a malware file, OTX displays the file analyses it or its partners conducted on specific malware-containing files. These analyses types appear as tabs, which themselves offer insight into the analysis specifics:

Static Analysis

Dynamic Analysis

Network Analysis

Static Analysis

Static analysis deals with the composition of the file, for example, if it is an executable, analysis includes:

- Operating system on which one could execute it, including architecture, for example, whether specialized for x84 or x64 bit.
- File size

- Malware file classification, if known, for example, Trojan or spyware. This also includes the explicit anti-virus signature of the file, if available.

All file types undergo static analysis whether by OTX or by its research partners.

When a static analysis has been performed, OTX displays antivirus results consisting of the information shown in Table 7.

Table 7. Sample static analysis information categories

Information Category	Description	Example
Antivirus Results	Any findings available about the indicator from leading antivirus packages, including the file name and whether it is malware.	AVG, a family of anti-virus and Internet security software for the Windows, Linux, Mac OS X, and FreeBSD operating systems.
Vendor	Entity conducting analysis.	AVG
Finding	Results of the finding. If malicious, usually represented as `<filename.type>` and its classification according to the vendor format for reporting malware.	`Atros.BEZB`
Notes	Concise result of antivirus analysis.	Malware infection
ExifTool	Used to parse metadata of a digital image, because these can be threat vectors.	Metadata supported by ExifTool include IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP, ID3, and manufacturer-specific metadata formats of many digital cameras.
Character_set	Character set the malware targets.	Unicode
Code_Size	Size of code within a file versus multimedia amount when bundled.	166400
Company_Name	Name of company whose software the malware targets.	Microsoft Corporation
Entry_Point	Location in the operating system stack or the Registry where code executed.	0x14179
File_Flags	How the file reports flags to the operating system.	rw, r

Information Category	Description	Example
File_Flags_Mask	Translated flags sent to the operating system for review in binary, machine code, or hexadecimal format.	0x003f
File_OS	Operating system the malware file targets.	Windows NT 32-bit
File_Subtype	Operating system-specific numerical instructions on how to execute the file.	0
File_Version	Sub-version of the file, denoting a usually smaller update to the `File_Version_Number`.	4.11.0603.3
File_Version_ Number	Version of the file, as reported by its vendor.	4.11.603.3
Image_Version	Modified image version.	
Initialized_Data_ Size	Amount of memory, in KB, the file reserves when first opened or executed.	45568
Internal_Name	Full file name within the operating system when the operating system permits file renaming. In some cases, hackers hide malware in what appears to be a legitimate application. For this reason, the ability to read the file name that the operating system sees is important.	EXTRAC32.EXE
Language_Code	Language that the file reports its text to be in. If a file was edited by someone, their operating system automatically places a language code in the file. If the language code is not the language of the software developer or that of the intended user, it can be a sign that the file was tampered with.	English (U.S.) The Sony Entertainment Pictures malware attack of 2013 contained Korean-language code that contributed to discovery of its source.

Information Category	Description	Example
Legal Copyright	Trademarked copyright of the software development company.	© Microsoft Corporation. All rights reserved.
Linker_Version	Assembler version responsible for file creation. Some assembler processes are vulnerable to exploitation.	9.0
Machine_Type	Processor type that the malware targets.	
MIME_Type	MIME header of a digital file. MIME headers describe for browsers how to execute digital files.	Application/octet-stream
Object_File_Type	Type of file, based on execution format, in other words, what the file does. Hackers routinely give files names intended to deceive users about the nature of the file. This information cannot be falsified. Knowing the Object_File_Type helps you avoid this type of hack.	Dynamic link library
Original_Filename	Original name of the file at creation date. Sometimes hackers try to rename a file to hide that it is an executable or known malware. Original_Filename cannot be falsified.	EXTRAC32
OS_Version	Operating system version targeted by the indicator.	5.0
Processor_Type	Processor type that the malware targets.	
Product_Version	Version of the file, denoting a usually smaller update to the `Product_Version_Number`.	4.11.0603.3

Information Category	Description	Example
Product_Version _Number	Version number of the file, as reported by its vendor.	4.11.603.3
PE_Type	Portable executable type targeted by the indicator.	PE32
Subsystem	Part of the software platform targeted by the indicator.	Windows GUI
Subsystem_ Version	Subsystem version should in most cases be identical to the OS version.	4.11.0603.3
Time_Stamp	Stamped date and time the file was last accessed in any way.	2014:12:16 10:13:13+01:00
Uninitialized_ Data_Size	Amount of disk space the file uses before execution, in other words, space needed for its storage.	0
PE Sections	Relates to Windows file sections, for example, PE32.	
Section Name	File type.	.data, .rdata, .rsrc, .text
Size (raw, bytes)	Unexecuted file size.	5632
Entropy	The expected average value of information contained in the file, in a scale from 0-8. The closer the number is to zero (0), the more orderly, or non-random the data. The closer the number is to 8, the more random, or non-uniform the data.	6.22
Virtual Address	When executed, where does the file enter within the execution stack.	212992
Virtual Size	Size of the executed file.	21276
PE Import	Relates to Windows import files.	
Imported From	Which dynamic link library (DLL) calls a file.	KERNEL32.dll

Information Category	Description	Example
Name of Import	System action called to execute the file.	Sleep, Open a URL, Set Alarm,
Start Address	Place in memory a file enters the operating system stack.	0x42a024
PE Version Information	PE analyzer information.	
Name	Name the PE analyzer used to gather information.	
Value	Details about the PE analyzer specific to its version.	
PE Anomalies	File or file behavior determined by dynamic analysis to be suspicious.	checksum_header_zero entropy_based
PE Packers	"Packers" used to compress or obfuscate the file.	.NET executable

Dynamic Analysis

Dynamic analysis studies the behavior of an executable file at run time, in other words, what it does inside of your system. Where appropriate, dynamic analysis includes network analysis.

When a dynamic analysis yields results, OTX displays analysis results consisting of the information shown in Table 8.

Table 8. Sample dynamic analysis information categories

Information Category	Description	Example
Alerts	Any alerts that exhibit suspicious/malicious behavior when the file is executed in a sandbox environment.	
Name	Name, if any, of the file containing the indicator, as reported by antivirus packages.	antivirus_virustotal

Information Category	Description	Example
Description	Any details known about the file named, for example, any information reported on eit by antivirus packages.	File has been identified by at least one AntiVirus on VirusTotal as malicious
Severity	Severity of the threat attributed to the file. Scale is from 1 through 10, with 10 confirmed as extremely malicious. File severity ranking is based on the following: • Potential for damage or compromise of a system. • File pervasiveness and potential for exploitation on the Internet. Any supplemental information known about common file usage or threat actors.	3
Data	Raw data of the alert.	MicroWorld-eScan: Trojan.GenericKD.2480984 VIPRE: Trojan.Win32.Generic!BT Symantec: W32.Duqu.B Kaspersky: HEUR:Trojan.Win32.Duqu2.gen Sophos: Troj/Duqu-H McAfee: Artemis!3F52EA949F2B AVware: Trojan.Win32.Generic!BT
Families	Associated malware families, if known.	Cryptolocker
References	A reference specific to that file.	
Registry		
Key	Location in the registry of an operating system to which the indicator writes, reads, deletes an entry.	

Information Category	Description	Example
Mutexes	Any mutex that the file creates when executed. Mutexes are often used by malware as a mechanism to detect whether a system has already been infected or not.	
Name	Mutex name.	4fe35d934eed65422a4637ab151f28d9
File Behavior		
File	File location.	C:\Documents and Settings\Mike\Local Settings\Temp\7316a6e4-117a-11e5-8a75-001e67afb360.dll
Status	Job of the executable, in other words, whether it reads, writes to, or deletes a file in a specific Registry location/path.	Read
Alert	If present, value is true or false.	True
Description	If present, any details known about the file named, for example, any information reported on it by antivirus packages.	
Severity	Severity of the threat attributed to the file. Scale is from 1 through 10, with 10 confirmed as extremely malicious. File severity ranking is based on the following: • Potential for damage or compromise of a system. • File pervasiveness and potential for exploitation on the Internet.	2

Information Category	Description	Example
	• Any supplemental information known about common file usage or threat actors.	
Data	If data included with the file, information about the size and constitution of the data, such as images loaded.	
References	References to .pdf or text about the file behavior.	http://morphick.com/blog/2015/7/14/bernhardpos-new-pos-malware-discovered-by-morphick

Network Analysis

As part of dynamic analysis, AlienVault analyzes malware for its potential to communicate outside of your system. This is referred to as *network analysis.*

Network analysis looks at whether and how a file within your system communicates with the network. However, although a malware file may wreak havoc within your system, it may never communicate outside of it.

When a network analysis yields results, OTX displays analysis results consisting of the information shown in Table 9.

Table 9. Sample network analysis information categories.

Information Category	Description	Example
IDS Signatures		
Name	Name of the triggered Intrusion Detection Signature.	ETPRO TROJAN BACKDOOR.EMDIV Checkin
SID	Numeric identifier of the Intrusion Detection Signature.	2809110
Source	Source of the intrusion detection alert.	192.168.56.104
Destination	Destination of the intrusion detection alert.	125.206.115.72
Protocol	If available, the protocol used for Internet transport.	IPv4, ICMP, HTTP

Information Category	Description	Example
HTTP Request	Information about the outbound connection over HTTP a file is making.	
URL	Fully qualified URL of the connection target.	http://www.iandeye.co.jp/blog/2014/index.php
Host	Server target of the connection.	www.iandeye.co.jp
Port	Port used to contact your system by file. For known protocol types, such as `80:web page`, this indicates the type of activity likely over the connection.	Port 80 signifies that connection probably used to send HTML files.
Method	Downloading or uploading content over HTTP, usually in the context of a REST or SOAP transaction.	Post = uploading data; Get = downloading data.
User Agent	If a webpage, information about the browser.	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
HTTP Body	Raw data sent over HTTP.	1rD36tTi=%28%24%26%3B%3E%3F.9%14za%7F%
Domain Contacted	Any domain contacted.	
Domain	Contacted domain name.	google.com
Hostname	Subdomain of the domain contacted.	mail.google.com
IP	IP address of the contacted domain.	125.206.115.72
External Host	External hosts of communications.	
Host	IP address of host for the malware.	125.206.115.72
DNS Query		
Query Type	Alpha code for type of interaction file has with the DNS when the file contacts it.	A = A host address. NS=An authoritative name server. SOA = Marks the start of a zone of authority.

Information Category	Description	Example
Answers	Response to file from DNS.	DATA: 125.206.115.7 TYPE: A
ICMP Requests	Any Internet Control Message Protocol traffic launched by a file.	0x0xf22
Adobe Malware Classifier	Findings from Adobe's command-line antivirus tool, which detects malware in binary files	
IRC Activity	Internet Relay Chat activity, a legitimate chat protocol sometimes misused as a command and control mechanism for botnets. Also used for infiltrating data (data extrusion), consisting of the unauthorized transfer of data from a computer (a data breach). Sometimes used for clandestine communications.	
SMTP Requests	Simple Mail Transfer Protocol relays can be used for sending unauthenticated emails, for example, spam. Can also be used for data exfiltration (data breach).	Delivered-To: MrSmith@gmail.com Received: by 10.36.81.3 with SMTP id e3cs239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST) Return-Path: Received: from mail.emailprovider.com (mail.emailprovider.com [111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb.2005.03.29.15.11.46; Tue, 29 Mar 2005 15:11:47 -0800 (PST) Message-ID: <20050329231145.62086.mail@mail.emailprovider.com> Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST

Passive DNS

These data relate to a hostname of a domain that is stored consistently by the consortium of DNS servers. Table 10 illustrates the information provided for a passive DNS.

Table 10. Sample Passive DNS information categories.

Information Category	Description	Example
Hostname	Registered URL for that domain/hostname.	a-masato.jp
Address	IP address resolved.	125.206.115.72
First Seen	Date and time first reported.	Oct. 31, 2014, 3:18 am
Last Seen	Date when last report received.	Oct. 31, 2014, 12:22 pm

You can expand the list at the upper-left corner to show up to 100 passive DNSs at a time.

Associated URLs

When present, this consists of a list of URLs associated with this indicator, consisting of the information in Table 11.

If an IP, hostname, or domain, this information references any URLs logged by OTX as connected to the data.

Table 11. Sample Associated URLs information categories.

Information Category	Description	Example
Date Checked	Last time OTX analyzed the data.	Jul. 2, 2015, 8:10 pm
URL	An associated URL.	http://online.matisse.co.jp/navi/q_a.jpg%2
Hostname	Actual hostname of URL. This may or may not be what is on file with WHOIS or the DNS server.	online.matisse.co.jp
Server Response	HTML response code.	Examples: 200, 404, or “Connection Error” (if the server sends no response at all).
IP	IP address associated with the URL.	Not Present.
Google Safe Browsing	Whether or not indicator is in the Google Safe Browsing database. Value is either present or not present.	Not Present.

Information Category	Description	Example
Antivirus Results	A file at the URL location that reports antivirus information.	

Creating a Pulse

You can create a pulse in multiple ways:

- Using the OTX extraction wizard to pull IOCs from your favorite sources. These can be blogs, emails, a .pdf file, log files, or any other malware sources—any file that has a textual description of a threat. You can also import Open IOC 1.*x* and STIX files.
- Adding indicators of compromise manually.
- Copying and pasting them onto the page.
- Cloning an existing pulse possessing the characteristics of a pulse you want to create, then editing it.

For details about the different indicators of compromise, see Table 2.

To add a source for OTX extraction

1. From the OTX primary navigation bar, select **Create Pulse.**
2. In the **Extract from Source (AlienVault Indicator Extractor)** section of the **Create New Pulse** page, do one of the following, depending on the type of indicator:
   - Type the URL of a website or blog.
   - Drag and drop a text file (for example, a .pdf, .txt, plaintext log, STIX, or OpenIOC file).
   - Paste the text.
3. Click **Next.**

   The program processes the request and displays a new Create New Pulse page. The page then displays the type of IOC you added on the previous page, for example, domain if it is a URL.

   If this information is available, the page also displays a list of IOCs related to the one you added, available either through AlienVault or other sources.
4. If available, review the list of IOCs for appropriateness.
5. If you see an IOC for which you want more information or that you want to delete, click it.

   If the IOC is a URL, for example, clicking it exposes three icons:
   - An “a”—Launches a popup window of Alexa.

     Alexa can provide information on how long a site has existed, how many page views it receives per day, and similar information that contributes to the Alexa “popularity” ranking of a website.

     In some cases, however, Alexa may not have enough information to rank a web site.

- A balloon—Launches a Whois registration record popup.

  Whois is a third-party registry service that shows who owns a particular website, domain, or host name. This tells you when a website was created.

  It can also tell you how many domains point to the web page. If many domains do point to it, that web page may act as a server to multiple secondary pages hosting malware.

- (All IOCs) An “x”—To delete an IOC that you think is incorrect from the list, click the **x**.

Note: Deleting an IOC from the list of IOCs moves it to the Excluded IOCs tab.

6. If available, review the list of Excluded IOCs.

   This list includes items that OTX determined were unlikely to pose threats. However, it is good practice to scan the list anyway, in case you see something about which you do not agree. For example, you may feel that an IOC was mischaracterized.

   The mischaracterization may have been a simple error, or it may hide malicious intent. You remain the best judge.

7. If you see something suspicious on the list, transfer it to the list of Included IOCs by selecting it and clicking **x.**

8. Click **Next.**

   The specific indicator you created on the last page and its type (for example, domain) appear on the right-hand side of the page in a table.

9. On the next **Create a Pulse** page, provide information that helps other OTX users benefit from the pulse you created:

   a. **Name—**Give the pulse a name to help identify it.

      Make the name concise, but pick a name that characterizes the threat uniquely. This could consist of where the threat was found or what type of malware it represents.

      Example:

      New PoSeidon spotted.

   b. **Description—**Describe the pulse in terms of where you found it, the type of threat it poses, and any other facts that may link it to other threat indicators.

      Example:

      While researching network infrastructure related to PoSeidon malware, Damballa was able to find information related to this campaign and its operators.

   c. **TLP—**Indicate the traffic light Protocol (TLP) for the threat.

      Developed by the U.S. Department of Homeland Security, the TLP consists of designations used to help ensure that sensitive information is shared with the correct audience. Its four colors indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s). For guidance, see **https://www.us-cert.gov/tlp**.

Note: If you make a pulse any other TLP than white or green, it automatically becomes private.

d. **Private—**Indicate whether or not you want to share the pulse with others or make it private.

To share or not share the pulse

Click the eye at the center of the page, or click the blue circle next to it, to toggle its setting to the desired status.

e. **Tags—**If your IOC is a URL. OTX creates relevant tags, based on analysis of the URL.

You can review any of these tags, and delete them, or you can add a new tag you feel is relevant.

10. Add a new tag:
    a. Click inside the **New Tag** field, at the bottom of the pulse description.
    b. Type the tag name, and press **Enter.**
11. Click **Submit**.

OTX returns you to the Activity feed.

Here you see the pulse you just created, along with its associated tags, appears in a concise format at the top of the **New** column, at left.

The pulse also appears at right, with details on the pulse creator, available from their profile.

To add indicators manually to create a pulse

1. Access the **Create New Pulse** page.by selecting **Create New Pulse** from the OTX primary navigation bar.
2. Click the **arrow** to the left of **Manually Add Indicators.**

   A new data entry section appears.
3. From the **Choose Type** list, select the applicable IOC type.
4. Paste the indicator into the **Indicator** field and, if you see one listed, paste or type the source.
5. Click **Add.**
6. Refer to the foregoing procedure for information about how to add a source for OTX extraction.

To add indicators to one of your existing pulses, using the extraction tool

1. Access your pulse in OTX.
2. Click **Add Indicators.**
3. On the **Add Indicators to Pulse** page, select **Extract from Source (AlienVault Indicator Extractor)** to automatically pull indicators from the source:
4. Take one of the following actions within the **Enter source here** field:

- Enter source URL
- Drag and drop file
- Paste text

5. Click **Next.**

   The page now shows the indicator that you previously added to the source field in the Included IOCs tab.

   It displays the indicator type, the indicator itself, and an excerpt from the source.

> **Note:** If you need to delete the indicator, hover over the indicator row to expose an “x” and click it.

6. Click **Submit.**

   The indicator and any related pulses now appear on the Details page for your pulse.

Adding Indicators to an Existing Pulse

You can add new indicators to one of your existing pulses when new data becomes available.

To add indicators to one of your existing pulses, using the manual method

1. Access your pulse in OTX.
2. Click **Add Indicators.**
3. On the **Add Indicators to Pulse** page, select **Manually Add Indicators.**
4. Paste indicator, its reference, and enter its type into the corresponding fields.
5. (Optional) If you want to add more than one indicator, click **Add.**

> **Note:** If you need to delete the indicator, hover over the indicator row to expose an “x” and click it.

6. Click **Submit.**

   The indicator and any related pulses now appear on the Details page for your pulse.

Searching for Pulses

This task describes how to successfully search for a pulse.

To search for a specific pulse

1. Type the pulse name; the name of an associated tag, like bitcoin or China; or another of the search parameters (Table 12) into the **Search** field (Figure 13) on the **OTX Browse** page.
2. Click **Search.**

Note: You can also type your search parameter into the Search field in the primary navigation bar.

To clear the Search field

- Click **Clear.**

Table 12. Pulse search parameters.

Parameter	Example/Description
Keyword	bitcoin
Pulse name	Dyre infrastructure May 2015
Indicator of compromise type	Examples: FileHash-SHA256, hostname, CVE
Description of the pulse.	*China, banking, finance*…

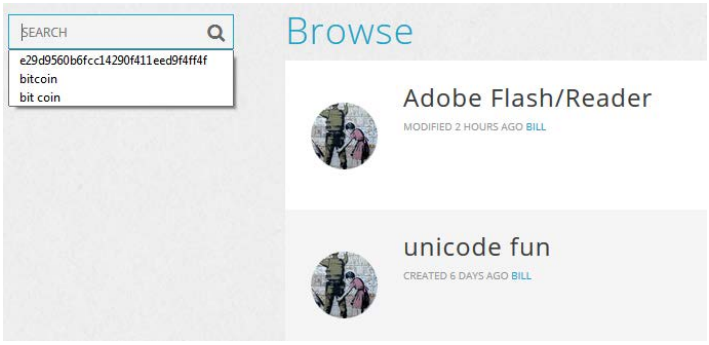

Figure 13. Search field on the OTX Browse page.