AT&T Cybersecurity

AT&T Business

Open Threat Exchange®

User Guide

Updated May 15, 2024

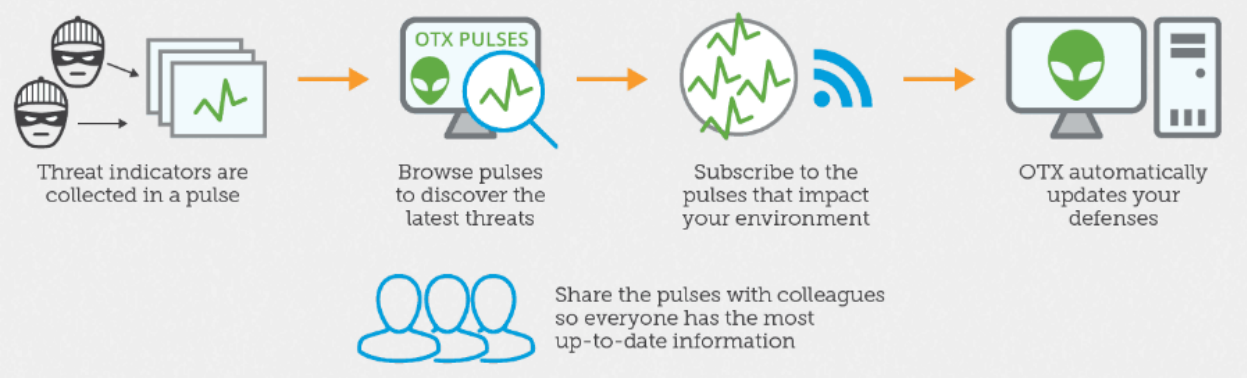
Contents

About Open Threat Exchange (OTX)

The LevelBlue Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network. OTX provides access to a global community of threat researchers and security professionals, with more than 100,000 participants in 140 countries, who contribute over 19 million threat indicators daily. OTX allows anyone in the security community to actively discuss, research, validate, and share the latest threat data, trends, and techniques.

Note: LevelBlue also provides a free global threat dashboard powered by OTX, available at https://cybersecurity.att.com/open-threat-exchange#/threats/top, which showcases some of the threat data sourced from the OTX community. Here, you can view a live feed of malicious activity recorded by OTX from around the world and see the top active threats.

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 or define a sequence of actions that could be used to carry out attacks on networks devices and computers. OTX pulses also provide information on the reliability of threat information, who reported a threat, and other details of threat investigations.



All OTX members receive pulse information through their OTX Activity feed, as well as receive updates about pulses through email. This information appears as soon as you open an OTX account. OTX data can be used to enhance the threat detection capabilities, not only of security monitoring systems such as LevelBlue USM Appliance™ and the open source LevelBlue OSSIM® platform, but also of other third-party security monitoring and management systems.

Topics covered in this guide include the following:

- Setting Up and Managing Your OTX Account
- Getting Started with OTX
- Subscribing, Following, and Contributing to OTX
- OTX Data with External Security Monitoring Systems

Setting Up and Managing Your OTX Account

You can sign up and set up an OTX account based on an email address, or you can use your existing Twitter or Google+ account.

Topics covered in this section include

Creating an OTX Account Using Your Email Address

This topic describes how to sign up to access the OTX platform using your email address as the OTX system login.

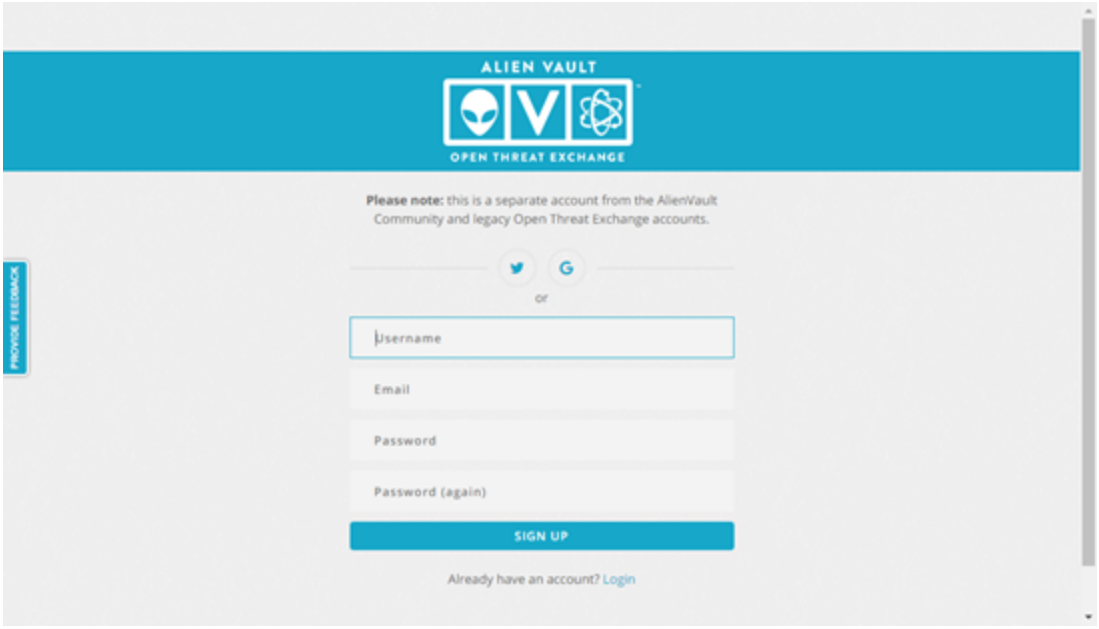
To create an OTX account

1. Go to OTX Home page.
2. In the upper-right corner of the home page, click **Sign Up**

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

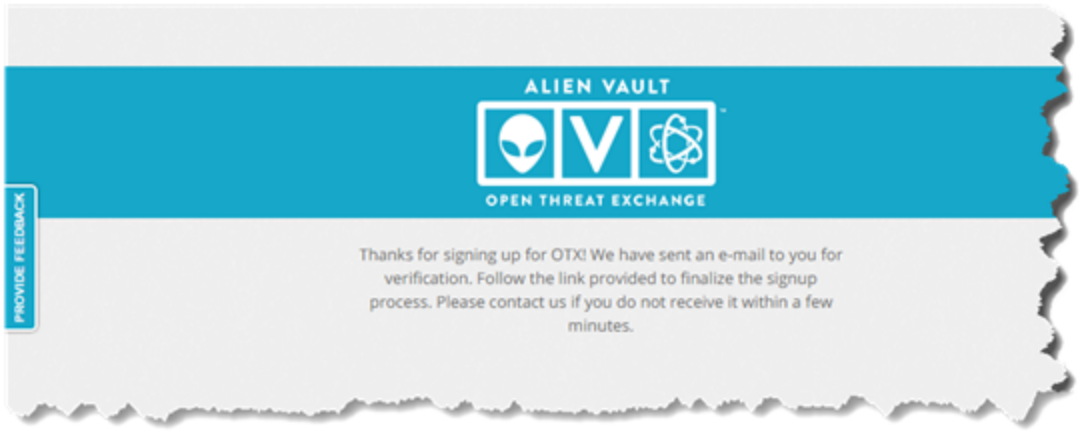
     Note: Your username will be displayed in OTX for any responses or information you provide to OTX, such as new pulses, indicators of compromise, and responses to other OTX members.

   - Email address.
   - Password of your choosing.
4. Retype the password to confirm correct entry.



5. Click **Sign Up**.

   OTX displays a web page informing you that a verification email message with a link to OTX was sent to the email address you provided.



> **Note:** If you do not receive the email message, send an email message to otx-support@alienvault.com.

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

   This takes you to the OTX Home page (https://otx.alienvault.com) where you will see all current pulse activity.

Signing Up for OTX Using a Social Media Account

You can also sign up for OTX using an existing Twitter or Google+ account. In that case, OTX authenticates your login using your social media credentials and, in the case of Twitter, prompts you to enter your email address.

Note: When you sign up to use OTX using a social medial account, you may be prompted to update the version of Java running on your machine, if you have an older installed version.

To sign up with one of your social media accounts

1. Go to https://otx.alienvault.com.
2. In the upper right-hand corner of the home page, click **Sign Up**.
3. Click the appropriate social media icon at the top of the page.

   Authorize LevelBlue to use your social media account credentials to create an OTX account.

   - For a Twitter account, click **Sign In**.
   - For a Google+ account, click **Allow**.
4. On the OTX Sign Up page, confirm that you want to sign up using your social media account.

   - If you signed up through Google+, your email address is automatically entered and you need only type a username.
   - If you signed up through Twitter, your username is automatically entered. Check that it is correct, and then enter your email address.
5. Click **Sign Up**.

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

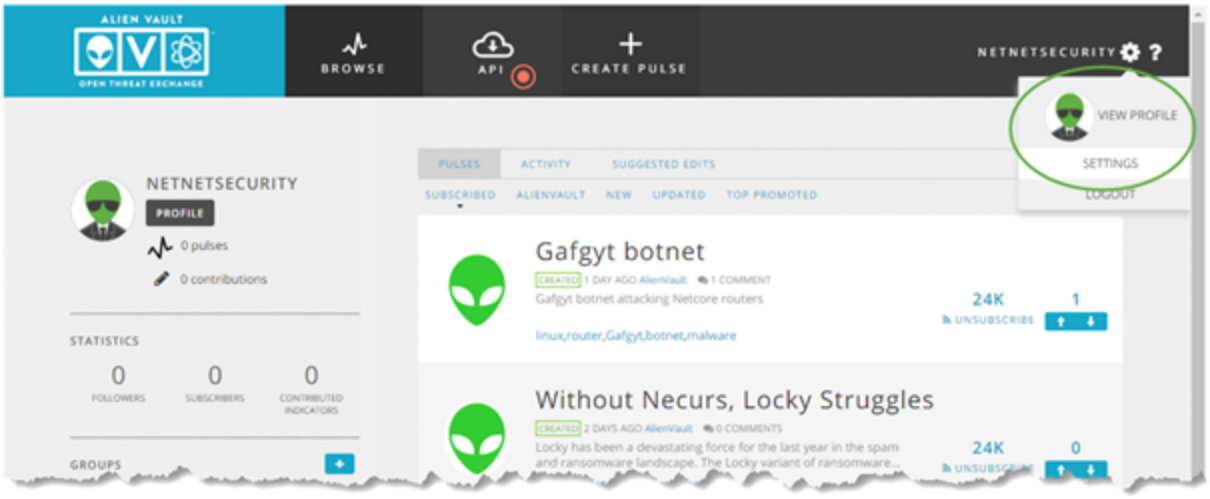
   Note: If you do not receive the email message, send an email message to the OTX Endpoint Security Technical Support.
6. Open the email message and click the link it contains to go to the confirmation page.

7. On the Confirmation page, verify that the email address is correct and click **Confirm**.

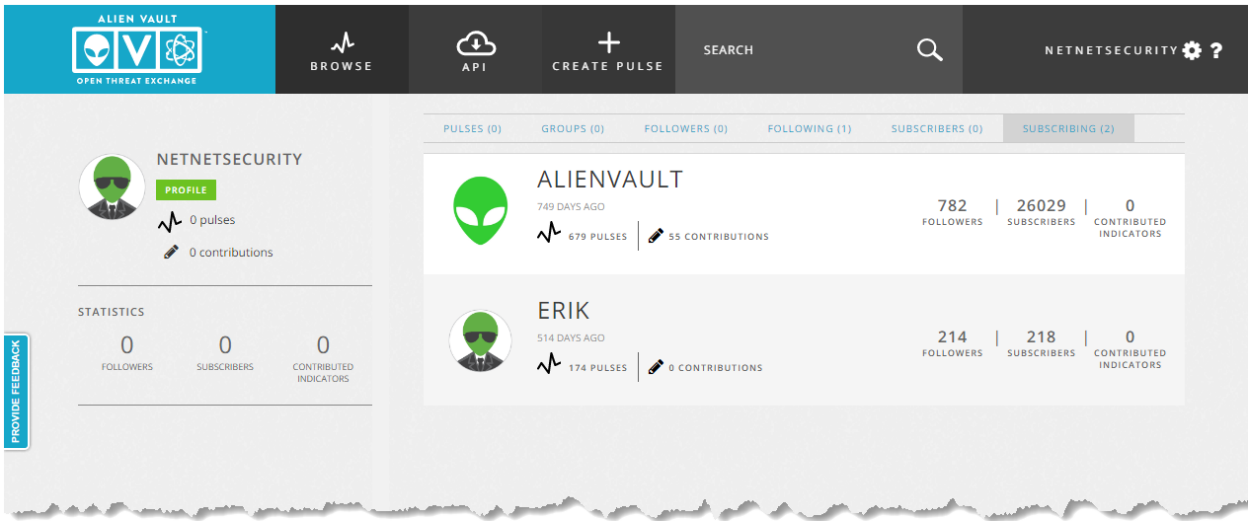
   This takes you to the OTX Home page (https://otx.alienvault.com/) where you will see all current pulse activity.

Reviewing Your Account Settings

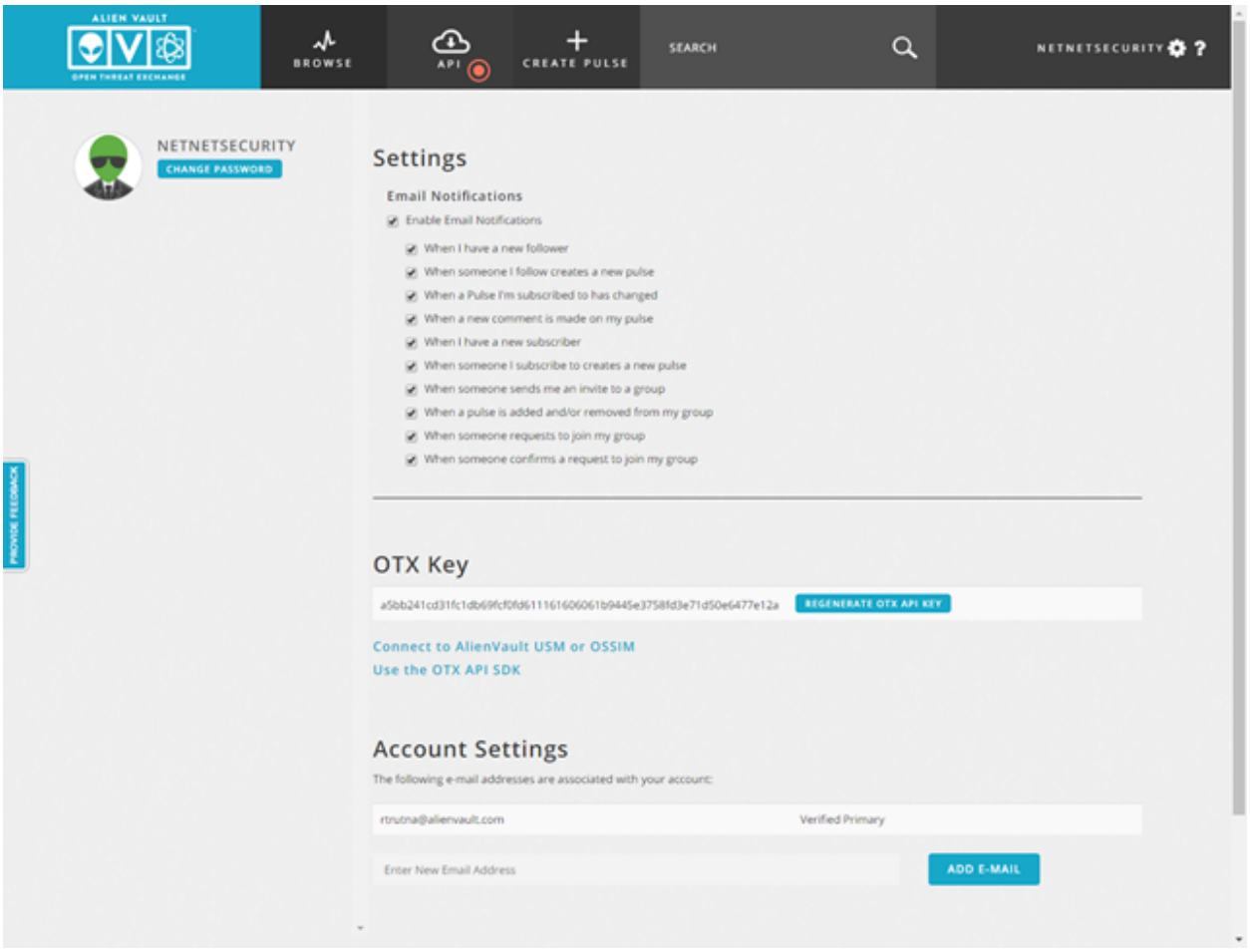
Once you've logged into the OTX user interface, you can click the Settings ( ) icon to view your user profile and also access the Settings page, which contains your OTX account data.



Selecting the **View Profile** option displays a web page in which you can see information about pulses you've viewed or contributed. You can also see the interaction you've had with other group members and subscribers, members you are following, and members who are following your pulse contributions.



Selecting the **Settings** option displays the **Settings** page.



From this page, you can perform the following tasks:

- Change your OTX password.
- Control the types of notifications you receive in email.
- Access your OTX account key, used to:
  - Connect OTX to your USM Appliance or LevelBlue OSSIM installation.
  - Establish connections with the OTX DirectConnect API, or one of its plug-ins, such as the DirectConnect Bro-IDS Agent.
- Update or add an email address. See Updating or Adding a New Email Address.
- Personalize your OTX avatar. See Personalizing Your Avatar.

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. Click the **Settings** () icon at the upper-right and select the **Settings** option.

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 message, which contains a confirmation link, to the email address you just entered.

4. Click the link to go to the confirmation page.

5. Click **Confirm**.

   You will now see the new email address in the Account Settings display, in addition to previous email addresses.

6. (Optional) To remove the previous email address, or just make a new entry the primary email address, 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.

7. (Optional) To delete the previous email address, click **Remove**.

Personalizing Your Avatar

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

To change your OTX avatar image

1. Click the **Settings** () icon at the upper-right and select the **Settings** option.

2. Move your cursor over the avatar image and click **Edit** when that link appears just below the image.

3. In the Change Avatar pop-up dialog box, click **Choose File**, then click **Browse**, and navigate to a new JPG or PNG file to upload.

4. Select the file and click **Open**, then click **Save** in the **Change Avatar** dialog box.

The updated avatar icon will now be displayed in your user profile and included in any comments and activities you participate in, when logged into OTX.

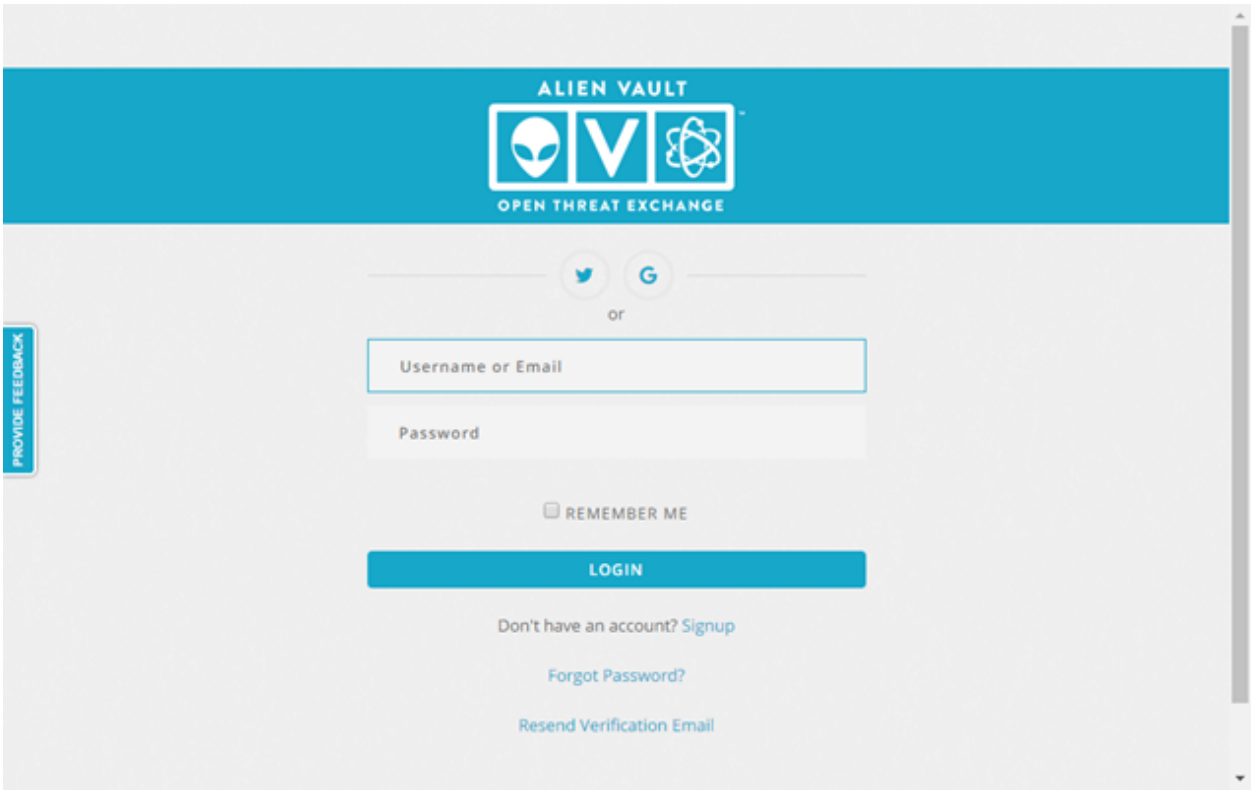
Getting Started with OTX

After logging in to the OTX user interface, you can begin examining the current threat activity being reported by various contributing members and groups. OTX lets you browse and search all current threats being reported, track updates on specific threat pulses, and follow or subscribe to the contributions of specific pulses, members, and groups.

Topics covered in this section include

Logging in to the OTX User Interface

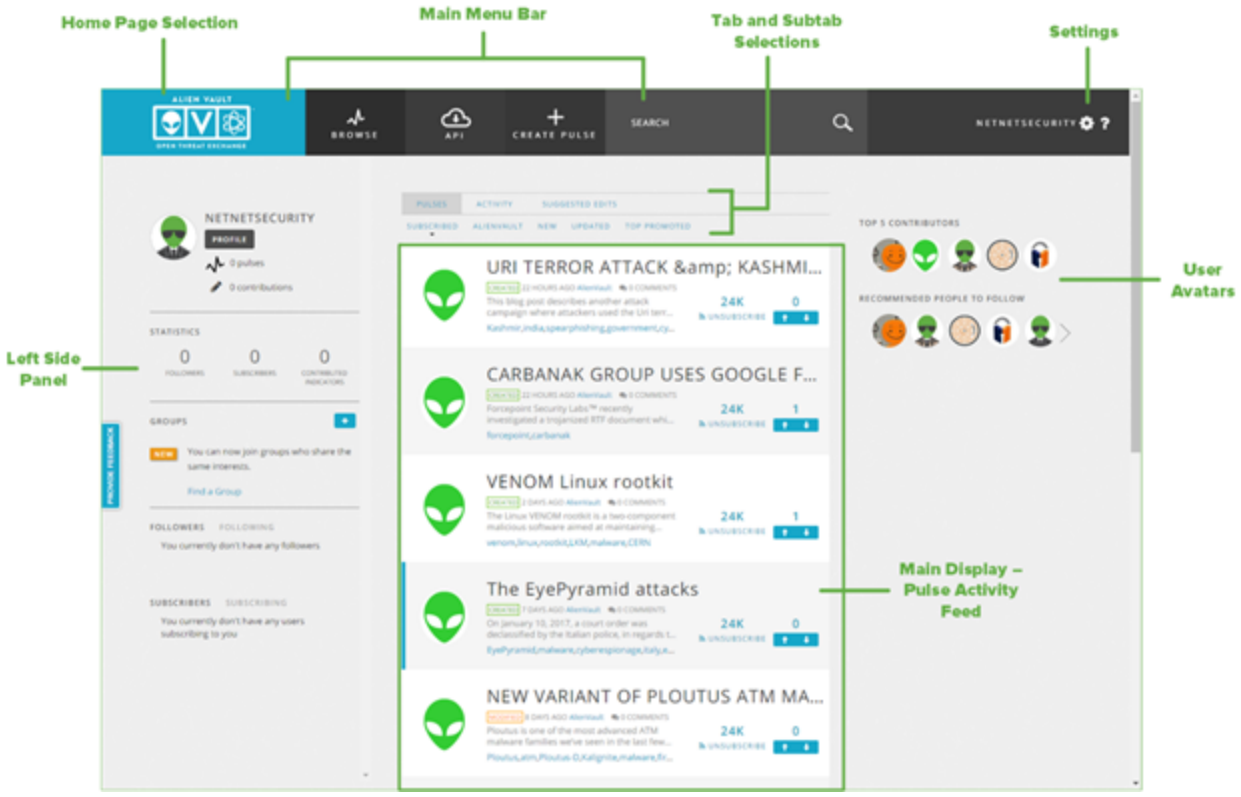
If you have logged out, or have been away from OTX for a while, you will need to log back into the OTX UI to resume looking at the current threat intelligence that OTX has collected from participating members. You can access the OTX login page by going to https://otx.alienvault.com/accounts/login/.



Log into the OTX user interface using the account information you defined during signup.

The OTX Home Page Pulse Activity Display

After successfully logging in, OTX displays the OTX Home page as shown below.



The OTX Home page provides a top row of main menu selections, **Home** ( ), **Browse**, **Create Pulse**, and **Search** ( ). On the far-right side of the menu bar, the OTX UI displays your username and two additional menu choices, **Settings** ( ) and **Help** ( ).

Main Activity Feed

The main, middle portion of the display provides an activity feed or stream of OTX pulses. At the top of this stream, the OTX user interface provides three main tab selections to display results for **Pulses**, **Activity**, and **Suggested Edits**.

Tab Selection Descriptions

Tab	Description
PULSE	Default selection. Displays current pulses based on selected filter criteria: **SUBSCRIBED** — Displays pulses to which you've already subscribed. (See Note below.) You are automatically subscribed to all pulses contributed by LevelBlue. **ALIENVAULT** — Displays only pulses contributed by LevelBlue Labs™. **NEW** — Latest pulses added to the threat activity feed (from all contributors). **UPDATED** — Latest updates to all pulses previously reported to OTX. **TOP PROMOTED** — Top promoted pulses added to the system by all contributors. Promotion or demotion indicates relative popularity and value of pulses, as voted on by OTX members.
ACTIVITY	Displays updates and events related to your pulse activities: • 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.
SUGGESTED EDITS	Displays suggested edits on pulses you've contributed and suggested edits on other members' pulse contributions.

By default, OTX displays all OTX pulses and contributions from members you've already been following or have subscribed to, plus those originating from the LevelBlue Labs, LevelBlue's internal threat research team. Besides the short results displayed for each pulse, you can click on a specific pulse in the results list, to view more detailed information about the pulse, additional attributes, and indicators of compromise (IOCs) for the pulse.

Note: The Home page activity feed displays pulses both for contributors you are following, as well as pulses you are subscribing to. When you subscribe to a contributor's pulse contributions, all of the subscribed contributors' pulses and IOCs are also downloaded into your local security monitoring environment, such as USM Appliance or LevelBlue OSSIM (when you have configured the OTX API for such integration). See OTX Data with External Security Monitoring Systems for more information on integrating OTX with specific USM Appliance, LevelBlue OSSIM, or other third-party security platforms using the LevelBlue DirectConnect API.

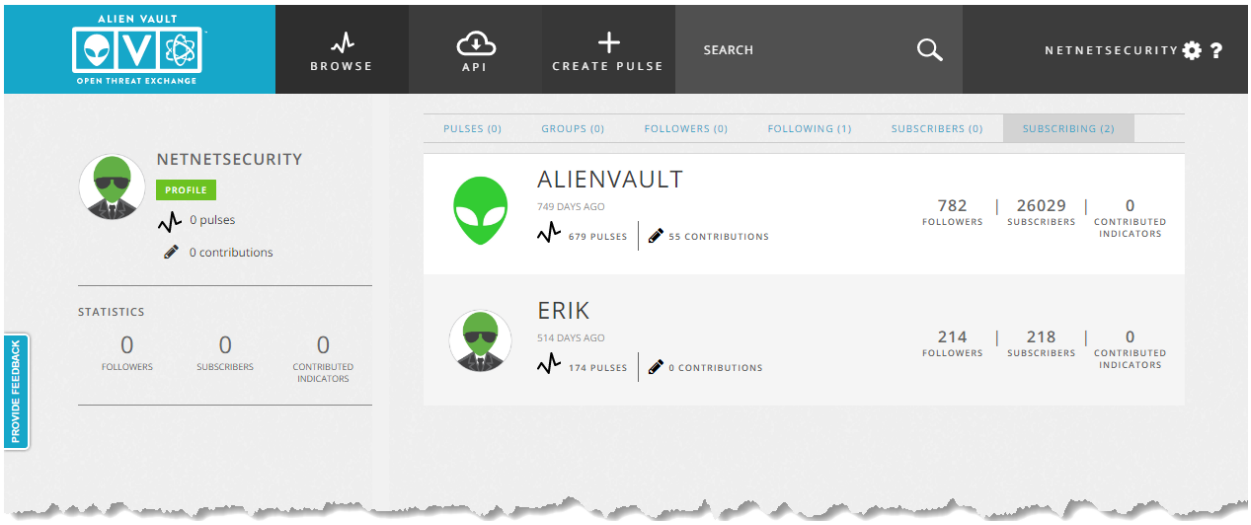
Home Page — Left Side Panel

A left side panel provides a summary of your current user profile including basic statistics on pulses you are monitoring, OTX members and groups whose contributions you have subscribed to or are following, members who are following your contributions, and so on.

In this panel, you can click the **Find a Group** link or the Plus ( ) button to find and join other groups of OTX users that you may share interests with. You can choose options to **Join an Existing Group**, **Join a Private Group**, or **Create a Group**.

Note: Joining groups means you will get alerts when pulses are added, and you can retrieve pulses more easily into a SIEM solution using the OTX DirectConnect API. Some groups are private, so pulses contributed from those groups can only be viewed if you are a member.

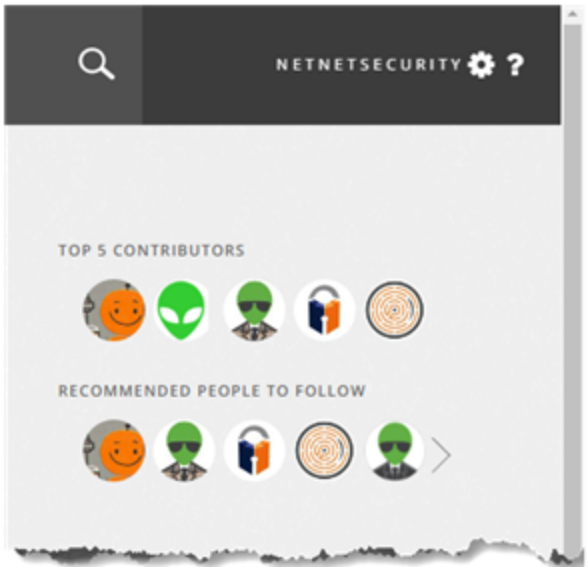
In the left-side panel, you can click the Profile ( ) button to view pulses sorted, in order, by different categories.



By default, the result list shows pulses across all categories. From the tab menu bar, you can select to view pulses by categories such as by **Groups (N)**, **Followers (N)**, **Following (N)**, **Subscribers (N)**, and **Subscribing (N)**.

Home Page — Right Side Panel

The right-side of the main display provides some quick selection options to display pulses for either top or recommended OTX contributors.

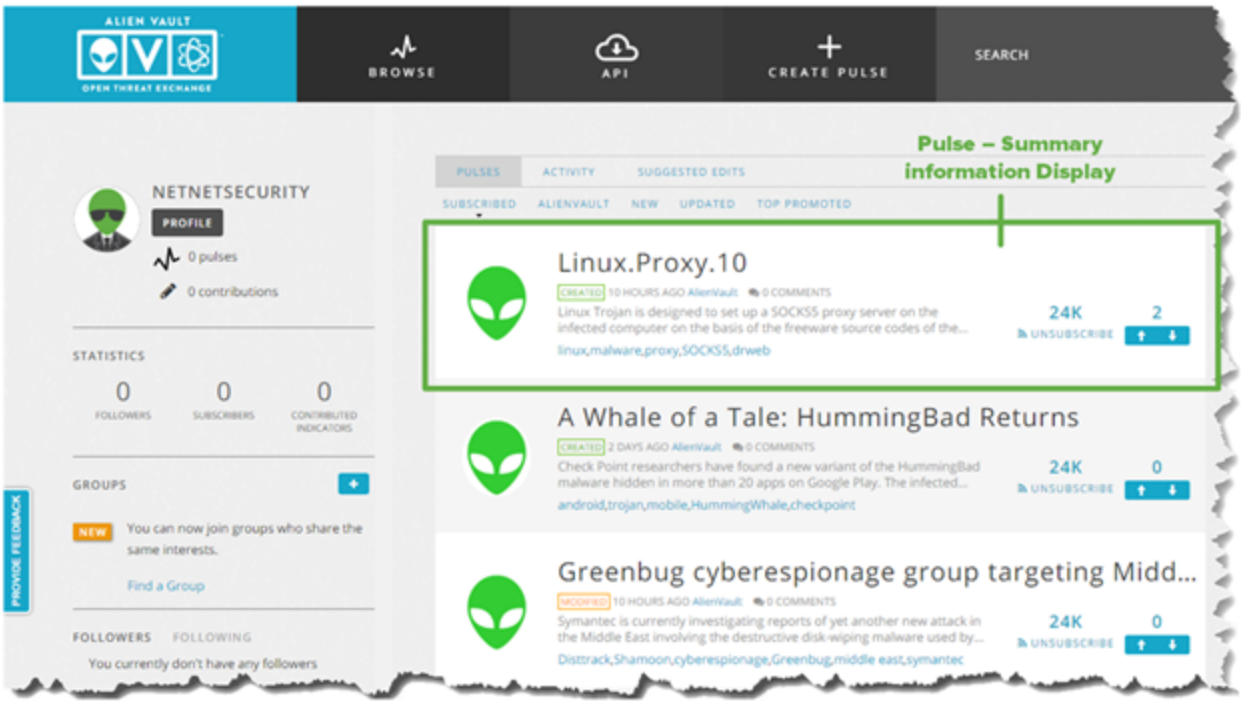


You can mouse over the contributor avatar icons to see the name of individual contributors. Clicking on any avatar brings up a display of the pulses submitted by the contributor you selected.

Viewing Pulse Information and Detail

Returning to the pulse activity feed displayed on the Home page, OTX provides a continuous stream of pulses, in reverse chronological order (latest is first), based on when a pulse was created or modified. By default, with the **Pulses** tab selected, OTX only displays pulses you've **Subscribed** to, plus pulses from other OTX members you have subscribed to.

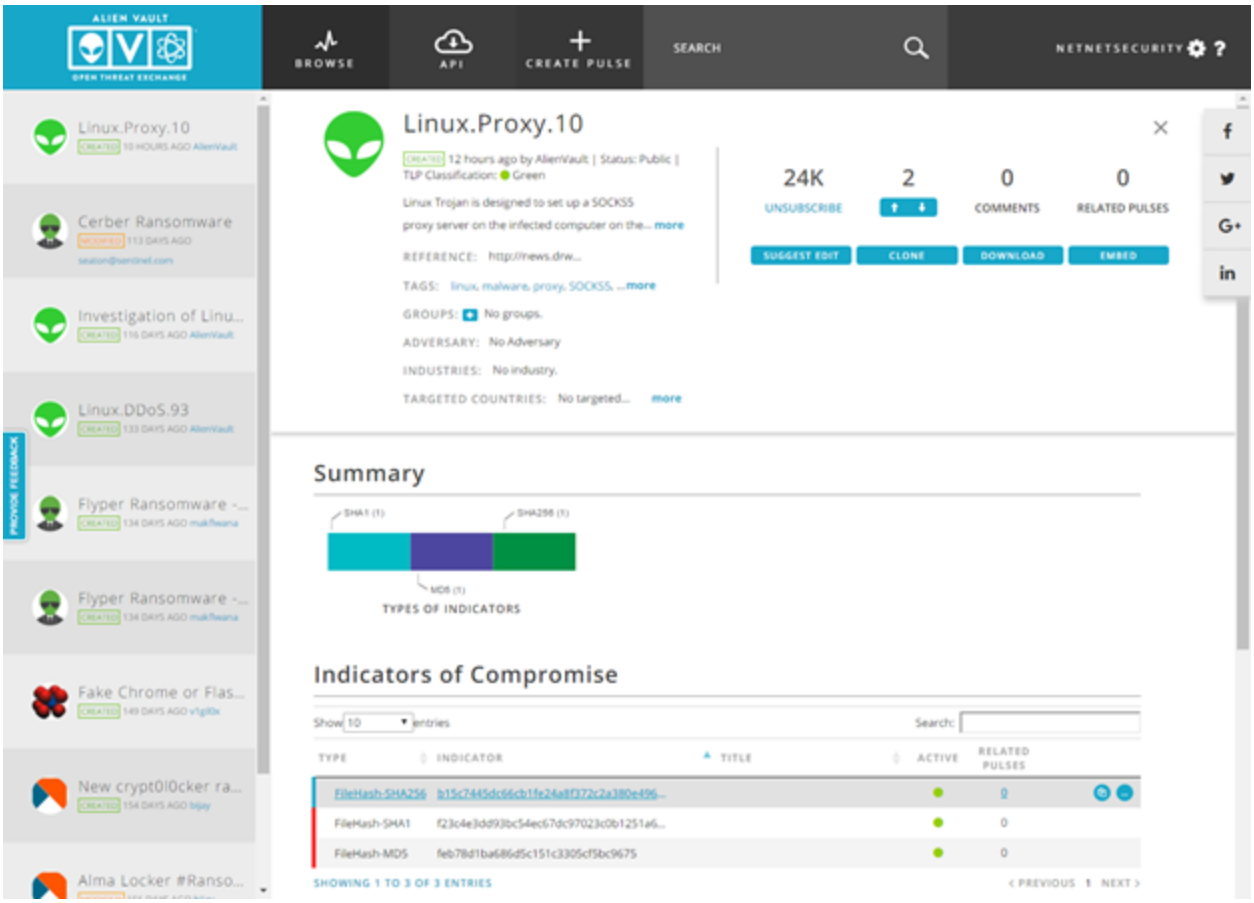
Note: The default pulse activity feed only shows pulses to which you've already subscribed, or those contributed by LevelBlue Labs™. To view all new pulses, select the **New** subtab option from the list of Pulse menu options.



The summary description for each pulse provides information such as the following:

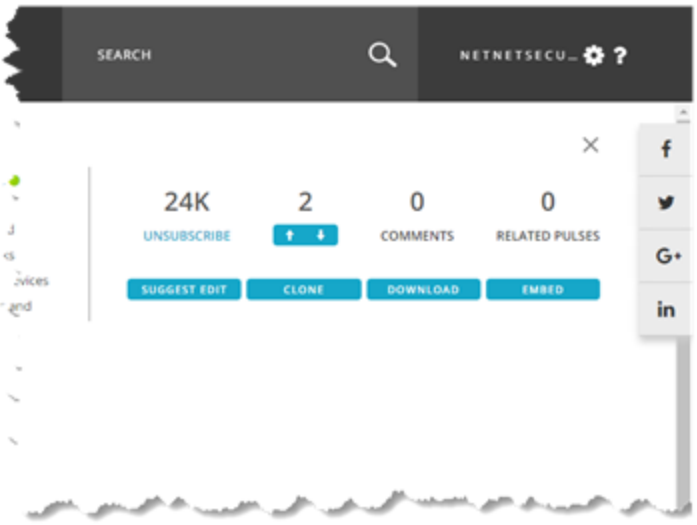
- Avatar of the user who created the pulse.
- Creation date of the pulse or the date it was last updated with new information.
- Number of comments on the pulse.
- A short description of the pulse.
- Up to four tags that OTX analytics tools or the pulse creator uses to categorize activities related to a pulse. (The Detailed view shows additional tags beyond four.)
- Number of pulse subscribers and whether you are subscribed to the pulse or OTX member.
- Number of votes ranking promotion or demotion of the pulse.

To get more details about a pulse, click on its name or summary description. OTX expands the display to show additional details about the pulse, along with a listing of Indicators of Compromise (IOCs) related to the pulse, and additional options for operations such as subscribing to the pulse, providing comments or suggested edits, and downloading of pulse details.



After clicking on a pulse summary and clicking the **more** option, the middle portion of the display shows an expanded/detailed view of the information for a selected pulse.

Next to the expanded summary display, OTX provides a row of buttons to perform specific operations.

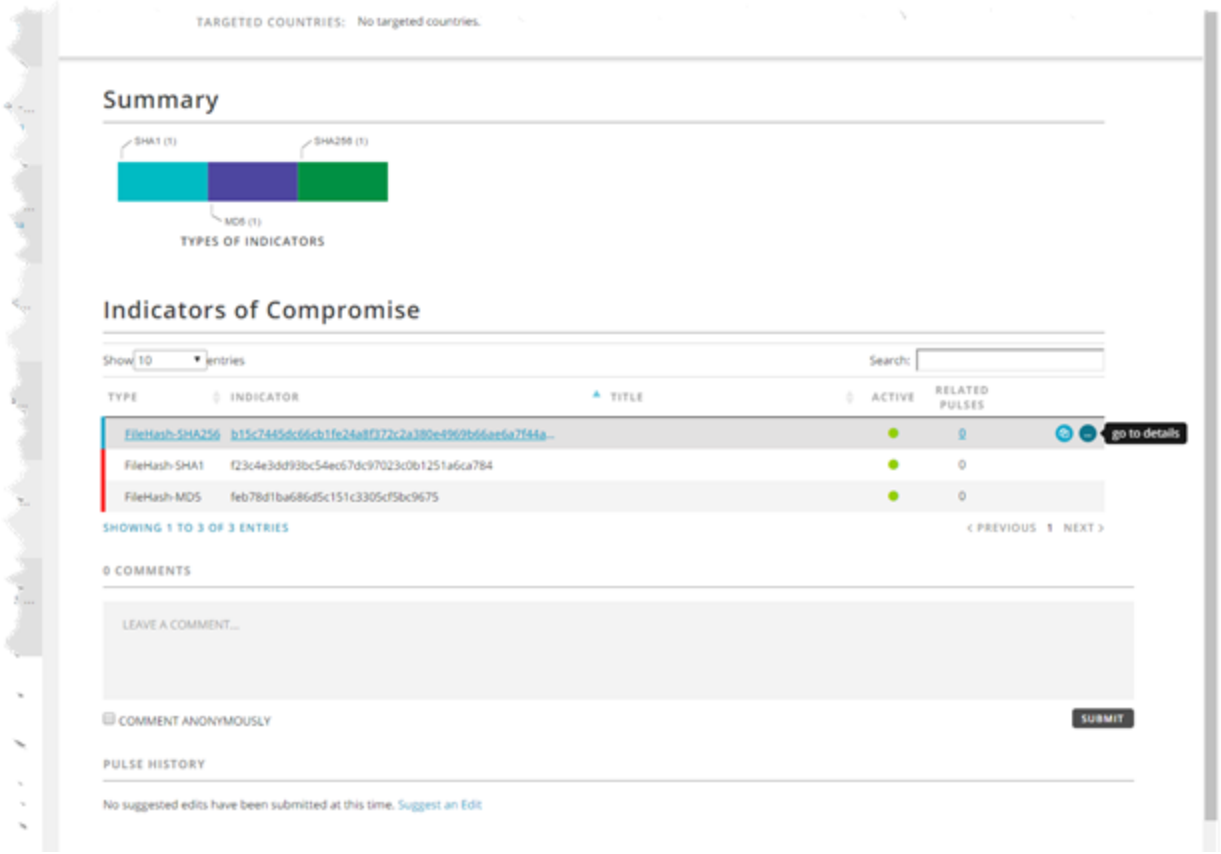


These options perform the following functions:

Pulse Option Description

Tab	Description
Subscribe/Unsubscribe	Toggle button to unsubscribe from subscribed pulses; or the reverse, subscribe to unsubscribed pulses.
↑ ↓	Vote to promote or demote opinion of pulse importance or value.
SUGGEST EDIT	Complete and submit a form with pulse editing suggestions such as new tags, targeted countries and industries, new references and indicators of compromise.
CLONE	Clone a pulse to create a template for a new related pulse.
DOWNLOAD	Download content of a pulse as a CSV, OpenIOC, or Stix format file.
EMBED	Copy contents of a pulse as a JavaScript file.

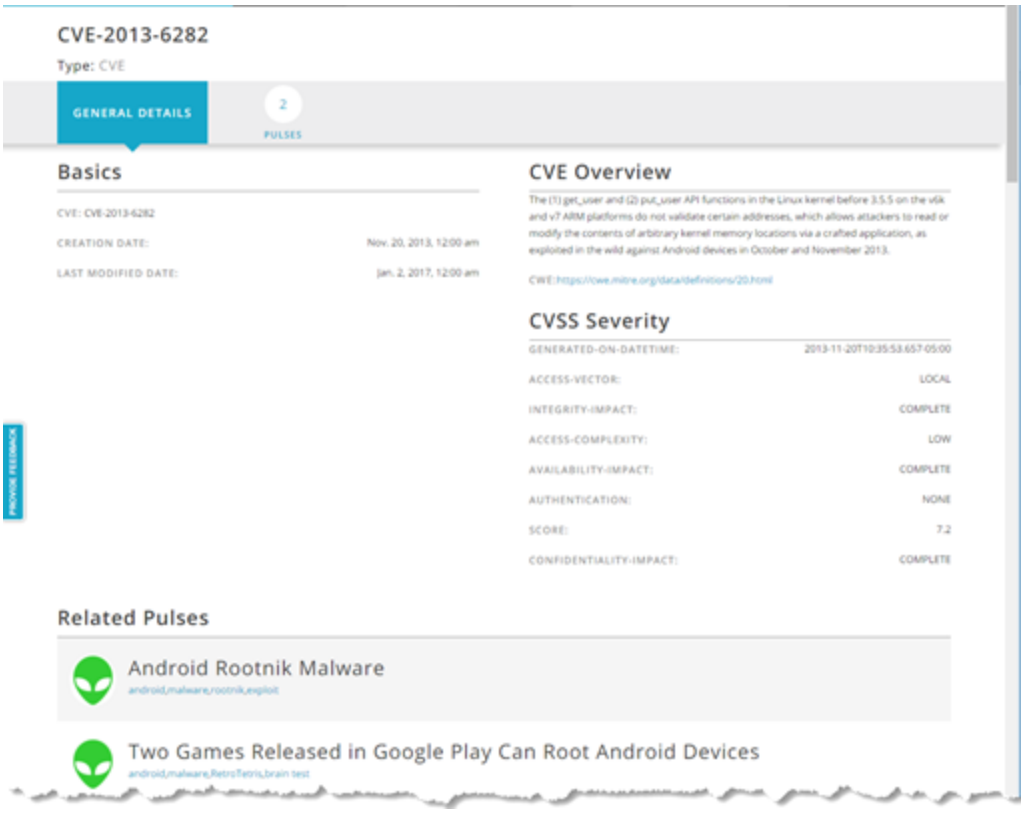
The lower portion of the pulse details display provides a comment section and information on Indicators of Compromise (IOCs) for the selected pulse.

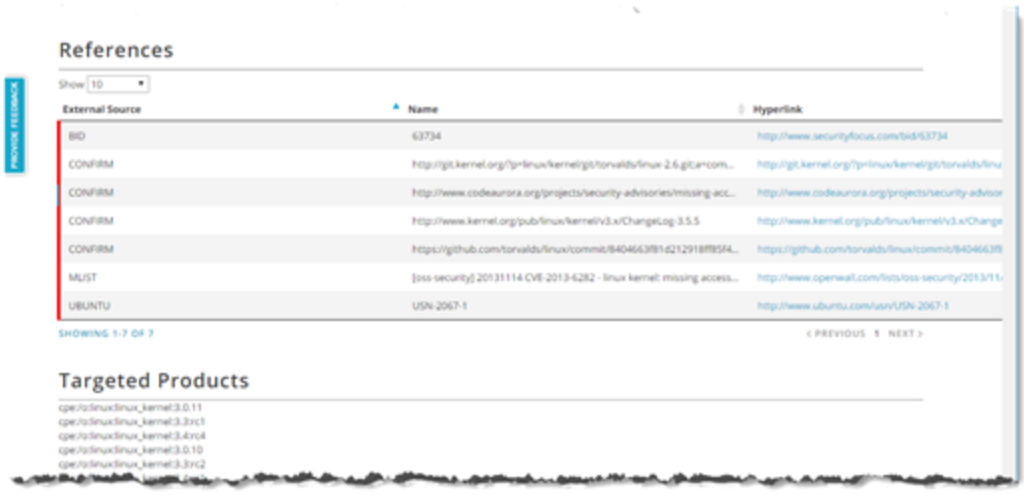


You can click on an individual Indicator in the list to expand the information displayed for the selected indicator. In addition, on the right side of each indicator row, the **Copy** ( ) button lets you copy the indicator information, which you may be able to use elsewhere in your security monitoring operation, and the **Go to Details** ( ) button, which displays an expanded detail view of the selected indicator on a separate page.

The Type column next to each indicator describes the type of each indicator associated with the pulse, such as IP address, domain, or file hash, such as MD5 or SHA-1. A file hash is an indicator of compromise commonly used in identifying malware such as viruses, trojans, ransomware, or other types of malicious software. For more information on IOC types, see Indicators of Compromise Types.

Depending on the particular indicator of compromise, the Indicator Details page can be very simple or it can include a great deal of information and research, based on how much information is available or known about the indicator at any given time. The following display shows an example:





Additional links on the page let you quickly jump to external reference data for a pulse, such as a CVE reference page, or detail on a particular exploit sequence.

At the very bottom of the page, OTX provides a comment page, so you can add any comments you might have on a pulse or share any experience you have had with the pulse threat or indicators of the pulse. You can enter a comment in which your name and avatar will appear next to your comment, or you can enter a comment anonymously.

Browsing and Searching OTX

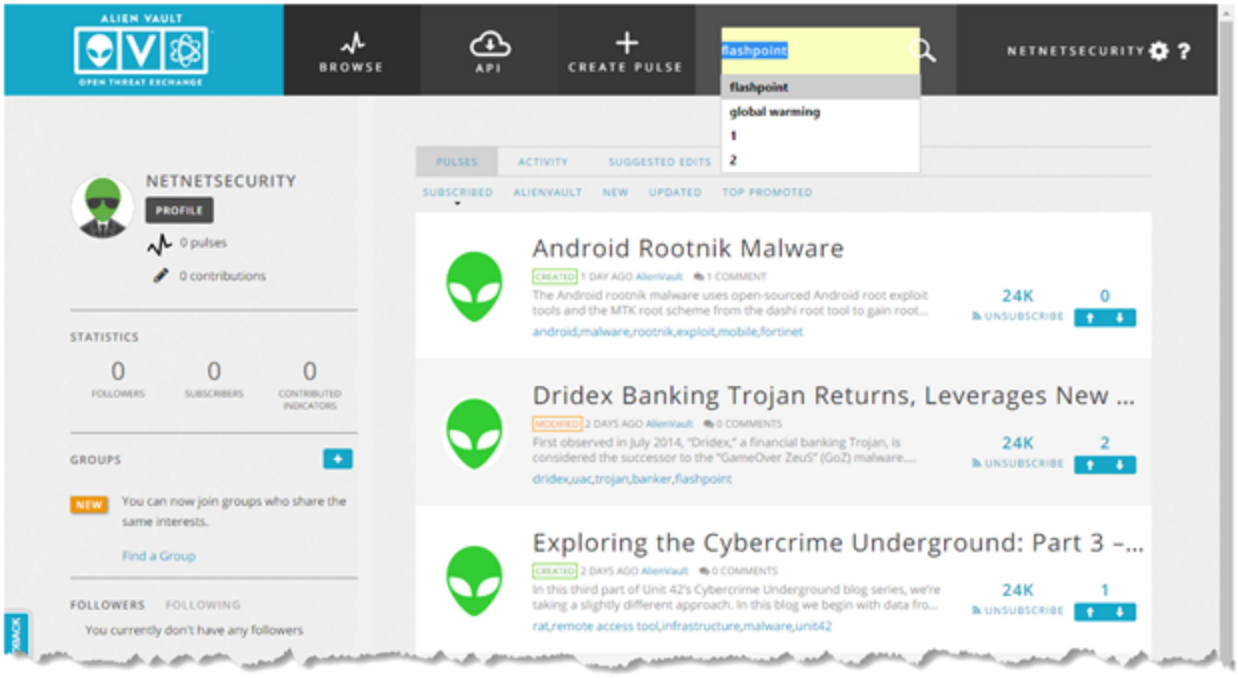
Beyond the Home page, the OTX user interface provides two other methods of browsing and searching threat information submitted by the OTX community:

Search ( ) — Available from the OTX Home page, lets you search for a text string included anywhere in pulse information, from the name and summary description, to fields and keywords.

Browse ( ) — lets you browse the OTX activity feed, choosing to view information by different categories: pulses, users, groups, or indicators of compromise. Within the display of results for information arranged by each of these categories, you can also perform a search, to further narrow the results that OTX displays of pulses, users, groups, or indicators.

Searching OTX

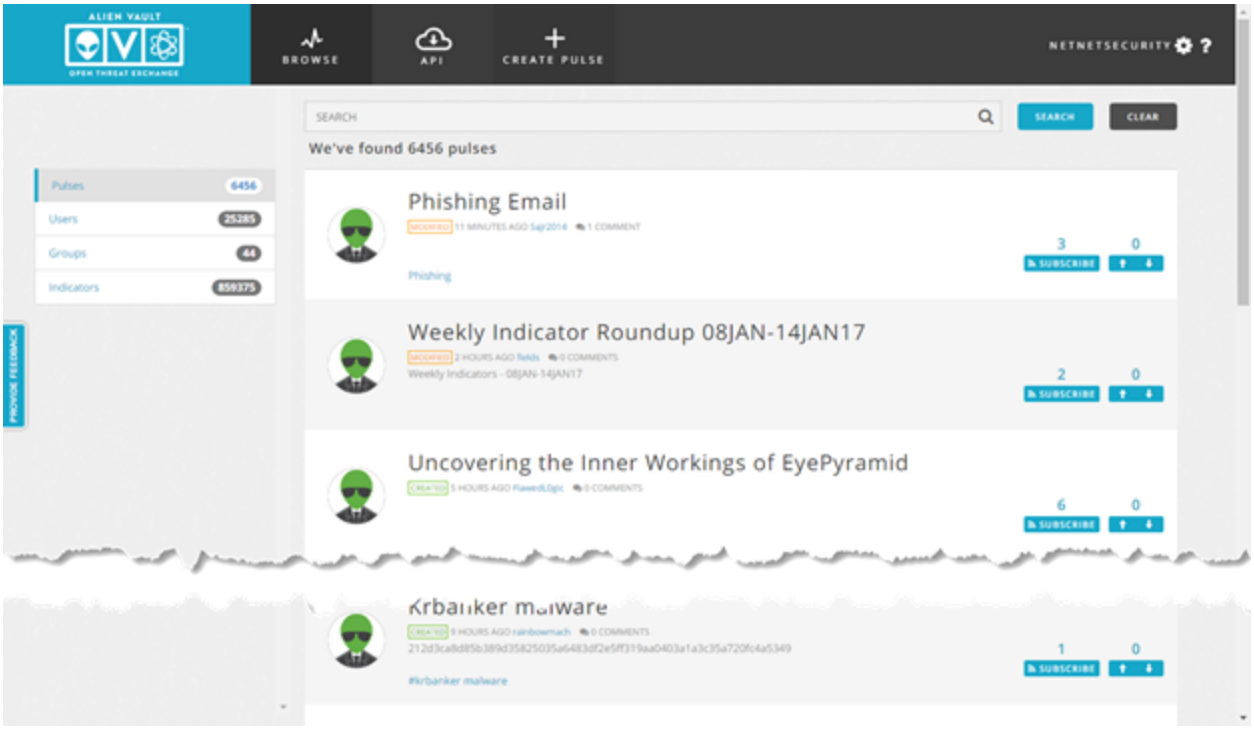
You can search for pulses from the Home page simply by entering a text search string in the Search field in the main menu bar, and then clicking the Search ( ) icon. OTX displays all pulses where the search text string you entered matches the name, description, or some other keyword or text information included in the pulse content.



After performing a search, you can navigate through the results, and view the detail of a pulse, just like you would from the normal Home page display.

Browsing OTX

When you select the Browse ( ) menu option, by default, the OTX user interface displays a chronological listing of pulses (latest on top), similar to the Home page. However, unlike the Home page, the Browse option displays all pulses (new, subscribed, and unsubscribed), not just those to which you've already subscribed.



Also different from the Home page, the left-side panel for the Browse display provides selections to view different aspects of OTX threat information, that is, pulses (the default), users, groups, and indicators:

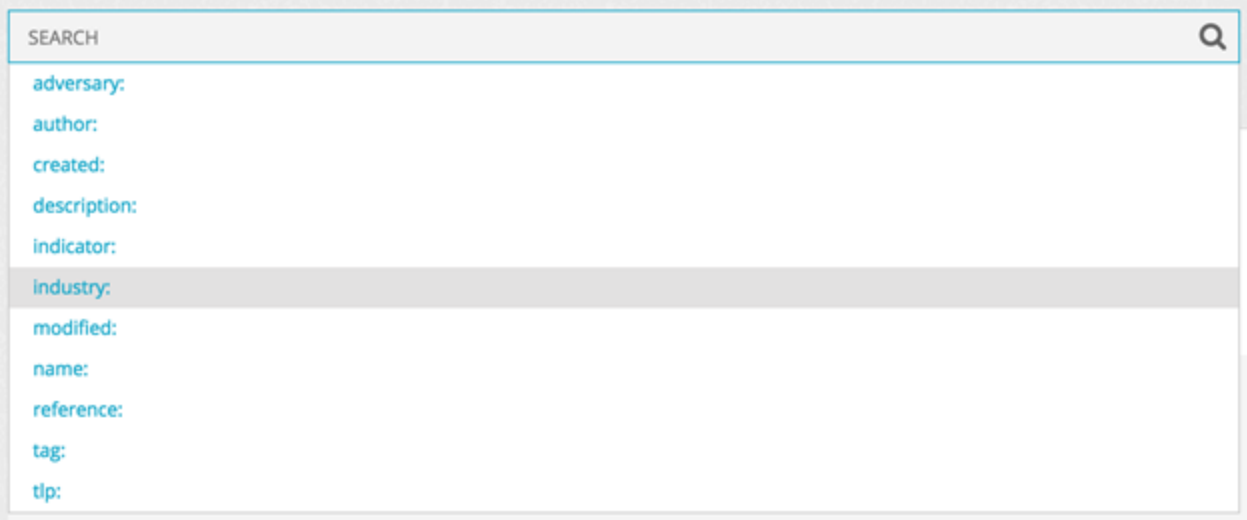
Panel Option Descriptions

Tab	Description
Pulses	Displays all available pulses, in chronological order (latest to earliest). Include existing, new, subscribed, and unsubscribed pulses.
Users	Displays summary information for every OTX member, in alphabetical order.
Groups	Displays a summary listing of all defined OTX groups, in alphabetical order.
Indicators	Displays a summary listing of indicators of compromise, in alphabetical order.

From the result set displayed for different types of OTX information, you can browse through and click on individual items in the list, and also drill down to view additional detail (when it is available).

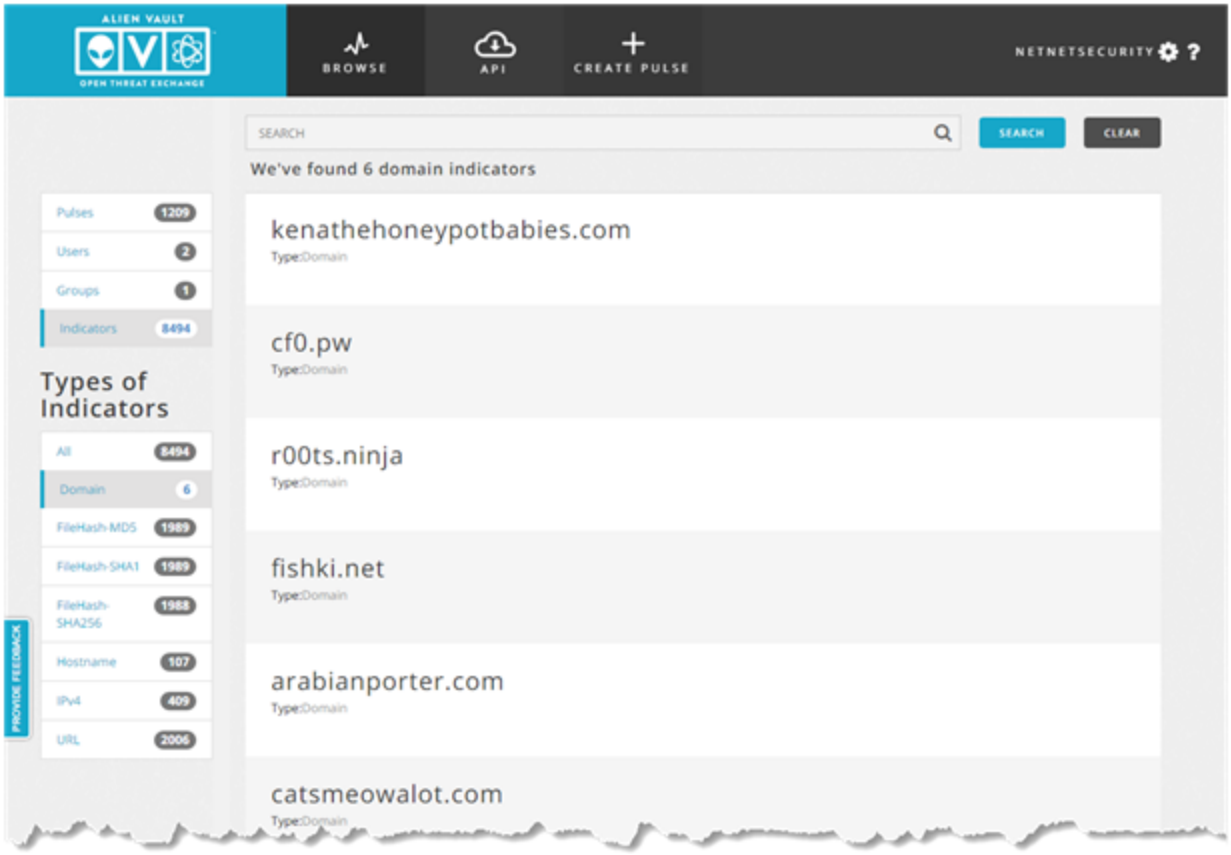
Within each result set, you can also narrow down the items displayed by entering a search text string in the Search field and clicking the **Search** ( ) button. The OTX user interface updates the results display to show only those items that include the search string text you specified. In addition, OTX updates the value displayed in the left side panel to show the number of items returned in the search results.

You can search by a number of fields within pulses. In the created and modified fields, search criteria is specified in the format **<***number* **ymd**. For example, **<1w** would search all pulses within the last week.



Indicators of Compromise Types

When you select the **Indicators** option in the left-side panel (for the Browse menu selection), the OTX user interface displays an additional set of menu options to specify the **Type of Indicator**. Clicking on any of the options restricts the display of indicators to only include those of a specified type, for example, **Domain**.



As previously mentioned, 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. The following table lists a number of different IOC types that are commonly associated with pulses.

IOC Type Descriptions

IOC Types	Description
CIDR	Classless inter-domain routing. Specifies a range of IP addresses on a network that is suspected of malicious activity or attack.
CVE	Standards group identification of Common Vulnerabilities and Exposures (CVEs).
domain	A domain name for a website or server suspected of hosting or engaging in malicious activity. Domains may also encompass a series of hostnames.
email	An email address associated with malicious activity.
FileHash (MD5, SHA1, SHA256, PEHASH, IMPHASH)	A hash computation for a file that can be used to determine whether contents of a file may have been altered or corrupted.
filepath	Unique location in a file system of a resource suspected of malicious activity.
hostname	The hostname for a server located within a domain, suspected of malicious activity.
IPv4, IPv6	An IP address used as the source/destination for an online server or other device suspected of malicious activity.
Mutex	Mutual exclusion object allowing multiple program threads to share the same resource. Mutexes are often used by malware as a mechanism to detect whether a system has already been infected.
URI	A uniform resource identifier (URI) that describes the explicit path to a file hosted online, which is suspected of malicious activity.
URL	Uniform resource locations (URLs) that summarizes the online location of a file or resource associated with suspected malicious activity.

Note: A file hash is an indicator of compromise commonly used in identifying malware such as viruses, trojans, ransomware, or other types of malicious software.

OTX IP Reputation Data

As part of the information that OTX collects on OTX pulses and the Indicators of Compromise they contain, OTX maintains an IP Reputation threat indicator, which is based on its ranking criteria of IP reliability and priority. OTX identifies IP addresses and domains worldwide that are submitted by the OTX community and verifies them as either malicious or, at least, suspicious until more data comes in to increase their threat ranking. Through its incoming IP data from all of these sources, IP Reputation supplements OTX data with valuable data about actively or potentially malicious activity appearing worldwide that could affect your own environment.

IP Reputation Data Sources

IP Reputation receives data from a variety of sources, including the following:

- Information security research forums
- Open-source intelligence — Public and private security research organizations.
- USM Appliance and LevelBlue OSSIM deployments — Consists of users who have voluntarily agreed to anonymously share information about external traffic into their network with OTX.

LevelBlue ensures that none of the data shared with OTX can be traced to the contributor, their USM Appliance, or LevelBlue OSSIM instance.

USM Appliance Access to IP Reputation Data

USM Appliance installations receive the benefit of IP Reputation data whether or not they sign up for an OTX account. However, LevelBlue OSSIM users must explicitly subscribe to OTX to have access to IP Reputation data.

When you open an OTX account for integration with USM Appliance, you may elect to share IP Reputation data with OTX, or opt out. Any data you contribute is anonymous and secure.

Note: You can configure USM Appliance to stop sharing IP Reputation data with OTX at any time by choosing that option from USM Appliance Open Threat Exchange Configuration page.

IP Reputation Ranking Criteria

IP Reputation provides a threat ranking based on IP Reliability and IP Priority values that OTX updates on an ongoing basis to calculate changing assessments to risk level.

IP Reliability

IP Reputation data derives from many data sources of differing reliability. Ranking in this case is based on the relative number of reports regarding 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

OTX 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.

Ongoing Ranking Reassessment

OTX constantly updates its IP Reputation data as new information emerges affecting IP reliability or priority criteria. Each update reprioritizes IP reliability and priority values and the threat level of an IP, accordingly.

Subscribing, Following, and Contributing to OTX

All OTX members receive pulse information through their OTX pulse activity feed, as well as receiving updates about pulses through email. This information appears as soon as you open an OTX account. Raw OTX data can be used to enhance the threat detection capabilities not only of security monitoring environments such as USM Appliance and LevelBlue OSSIM, but also other environments that can use the OTX DirectConnect API to synchronize with OTX threat intelligence information.

OTX users automatically receive all pulses, and any updates to them, that originate from LevelBlue. You may also subscribe to OTX community members, thereby subscribing to all of the pulses they create and update.

Topics covered in this section include

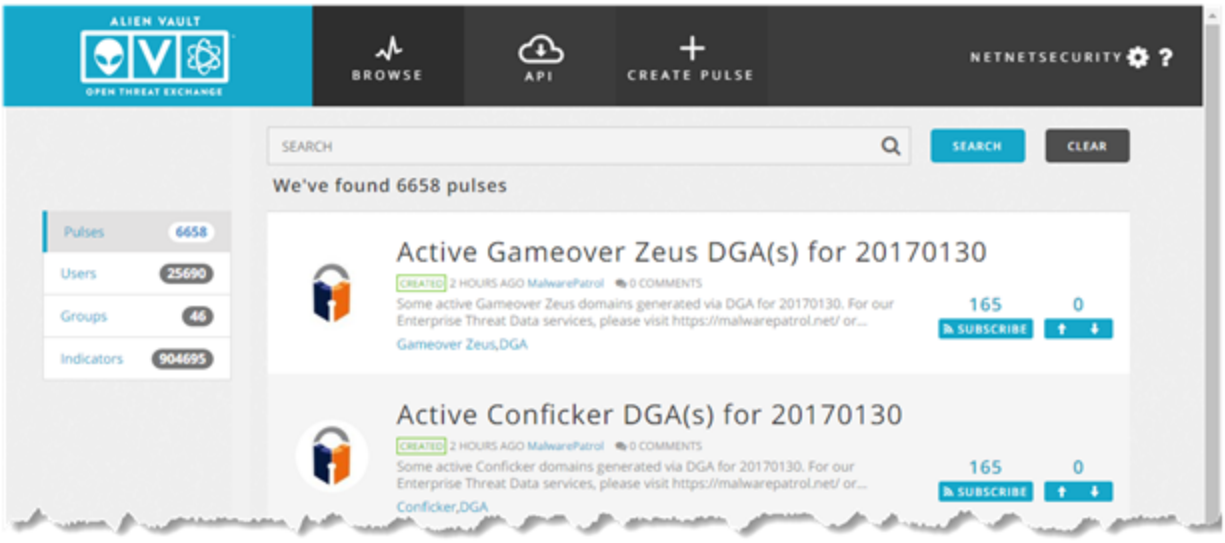
Subscribing and Unsubscribing to a Pulse

Subscribing to a publicly-created pulse allows automatic export of its raw data to the security tools you use to monitor security in your environment (provided you have configured your security tools to connect with OTX). To subscribe to a pulse:

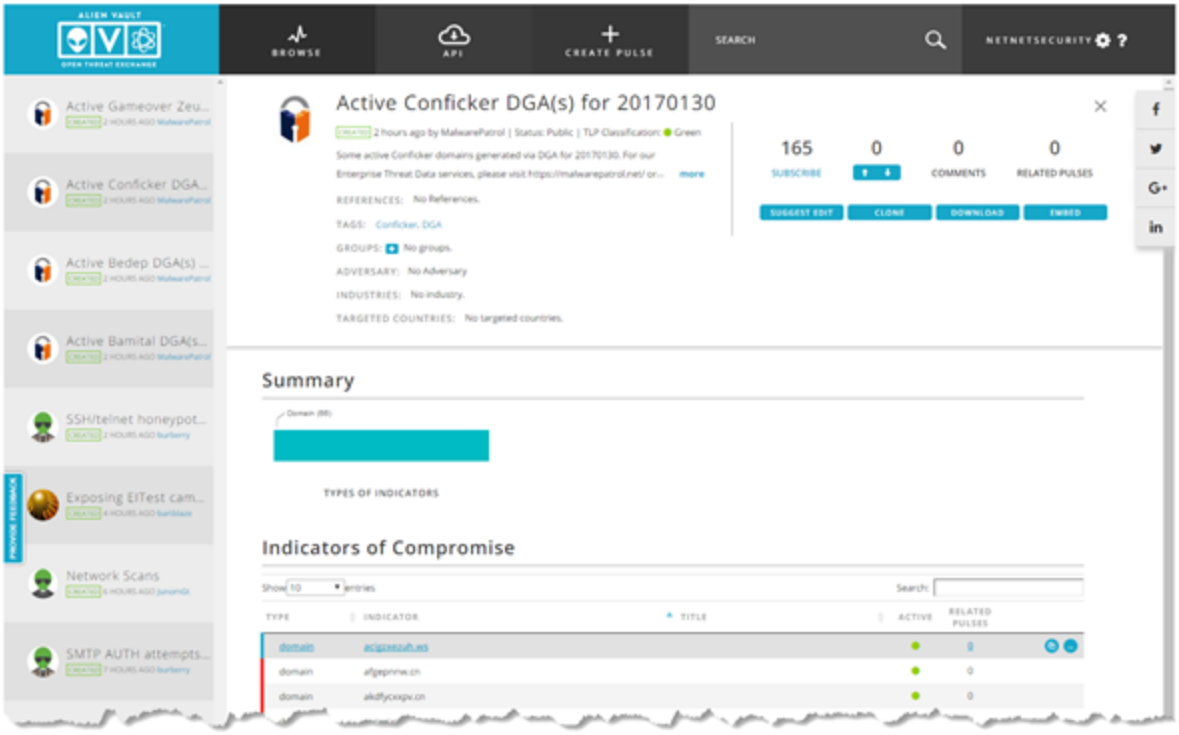
1. Launch the OTX user interface from https://otx.alienvault.com and log in.

2. From the OTX Activity feed, perform either of the following operations to locate a pulse:

- Scroll through the pulse activity feed to find a pulse you want to subscribe to.
- Perform a search for a pulse from the **Browse** page.



You can also click on a pulse and subscribe from either the pulse summary or detail views.



The **Subscribe** link toggles to **Unsubscribe**.

To unsubscribe to a pulse, you can simple click the **Unsubscribe** link for the subscribed pulse.

Note: When you unsubscribe from a pulse, you still receive information about the threat in your OTX pulse activity feed, but no raw data is pulled into your security tools for correlation and generation of alarms. You might consider unsubscribing to a pulse if it is creating too much noise and generating too many false positive alarms in USM Appliance or whatever security monitoring tools your organization is using.

Subscribing to or Following OTX Contributors

You may also subscribe to or follow public OTX contributors, in addition to subscribing to individual pulses. The difference between subscribing to and following a contributor is that:

- Subscribing to an OTX member or contributor directs OTX to send all of the contributor's pulses or IOCs to the tools used to monitor security in your environment. In the case of USM Appliance or LevelBlue OSSIM, this update of OTX data occurs automatically every 15 minutes.

- Pulse and IOC contributions from an OTX member or contributor you subscribe to automatically appear in your OTX pulse activity feed, and you also receive emails every time they update one of their pulses or when they create a new pulse.
- Following an OTX member or contributor directs OTX to show a followed member's pulses within your activity feed, but not to send raw data from their contributions to the security tools deployed in your environment (using the OTX DirectConnect API). Following an OTX contributor is the right approach if you only want to view a member's pulse contributions in the OTX user interface, not automatically sending them to your security monitoring and management environment.
- 

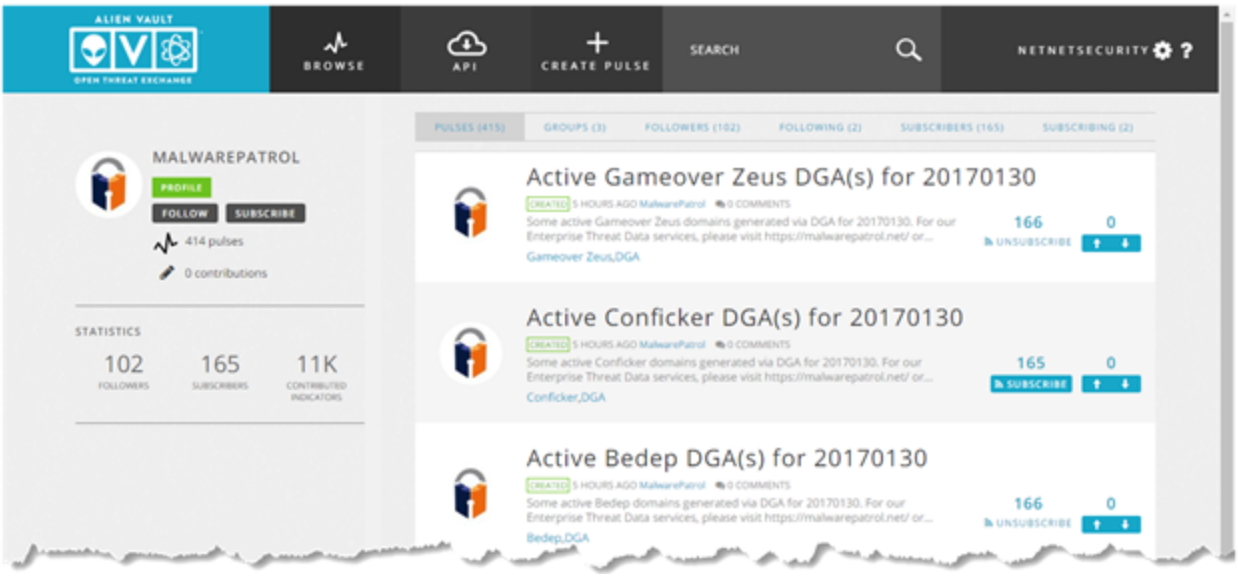
  Note: After subscribing to a pulse, you can also always unsubscribe from the pulse, if it is creating too much noise and generating too many false positive alarms in USM Appliance or whatever security monitoring tools your organization is using. When you unsubscribe from a pulse, you still receive information about the threat in your pulse activity feed, but no raw data is pulled into your security tools for correlation and generation of alarms.

To subscribe to or follow an OTX Contributor

1. Click the username of the OTX contributor to whom you want to subscribe. You can do that from one of several different locations:

- Pulse summary or detail display on the Home or Browse pages.
- The avatar from the **Top 5 Contributors** or **Recommended People to Follow** on the OTX Home page.
- The Users display on the Browse page.

After choosing a user from one of these displays, the OTX user interface displays the selected user's profile in the left-side panel.



In the main display area on the right, the OTX user interface provides a series of tab selections to view related information about the selected user: Pulses the user has already contributed, Groups the user belongs to, members that are following the user, who the user is following, members who are subscribers, and those the user has subscribed to.

2. In the left-side pane, click the **Subscribe** or **Follow** button to, respectively, subscribe to or follow the selected user.

In addition to subscribing to or following an OTX member, you can click the **Profile** button to view more information about a specific member. In addition, the OTX user interface displays statistics about the member's contributions to date, and their respective followers and subscribers.

Contributing to OTX

As an OTX community member, you can contribute to OTX in several different ways:

- You can comment on pulses contributed by other OTX members.
- When you have installed LevelBlue USM Appliance™, you can opt in to let USM Appliance share with OTX any IP Reputation event data generated from within your own system environment. OTX can then use that information to reevaluate IP Reputation severity levels that can then affect the issuing of USM Appliance correlation directives.

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

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

When you have installed USM Appliance and you also choose to contribute to OTX, USM Appliance data shared with OTX may only include the following:

- External IP addresses that try to or succeed in communicating with your system.
- Any Plugin IDs.
- Any event types (Security Identifiers, or SIDS).
- Counts from intrusion detection system (IDS) signatures.
- Any alarms generated based on observed traffic.
- IOC activity data within your environment for analysis against pulses.

Note: You can choose to stop sharing data with OTX at any time by going to the USM Appliance configuration page (**Configuration** > **Open Threat Exchange**).

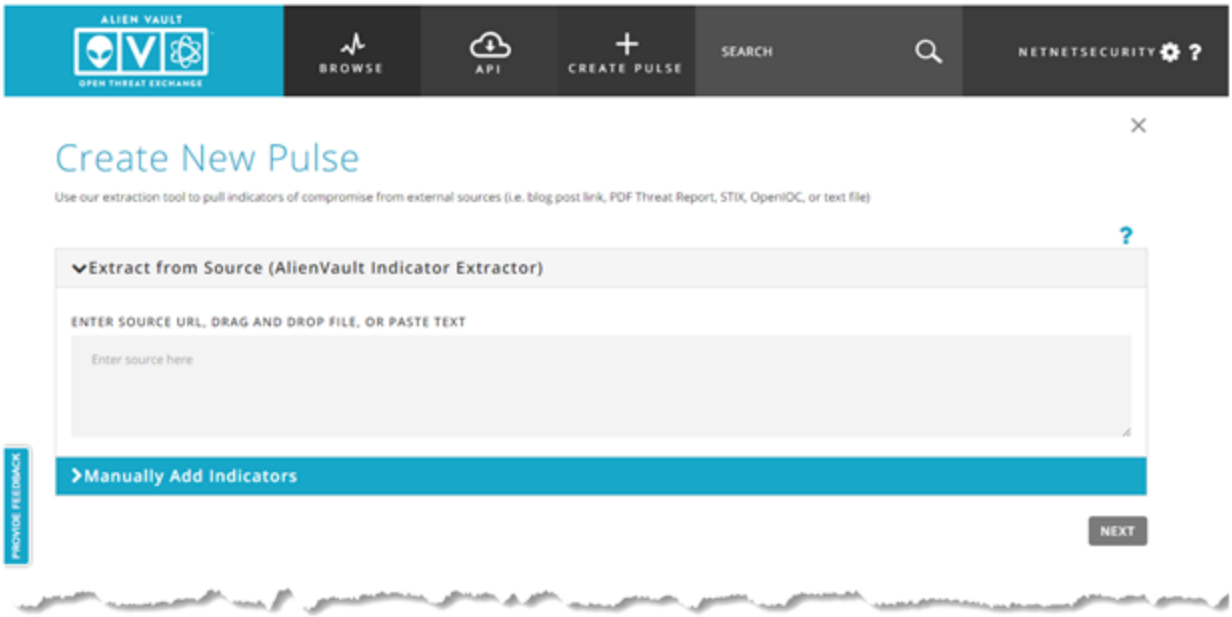
Creating and Updating Pulses

When you choose to create and contribute pulses to OTX, you can use a number of different methods to do so:

- Use 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.
- Manually add indicators of compromise to create a pulse.
- Copy and paste indicators into the detail of a new pulse.
- Clone an existing pulse possessing the characteristics of a pulse you want to create, and then edit the cloned pulse to create a new pulse.
- Open an existing pulse you've created and add indicators, either manually or using the LevelBlue Indicator Extractor.

Creating a Pulse Using the Indicator Extractor

1. From the OTX main menu, select **Create Pulse**.

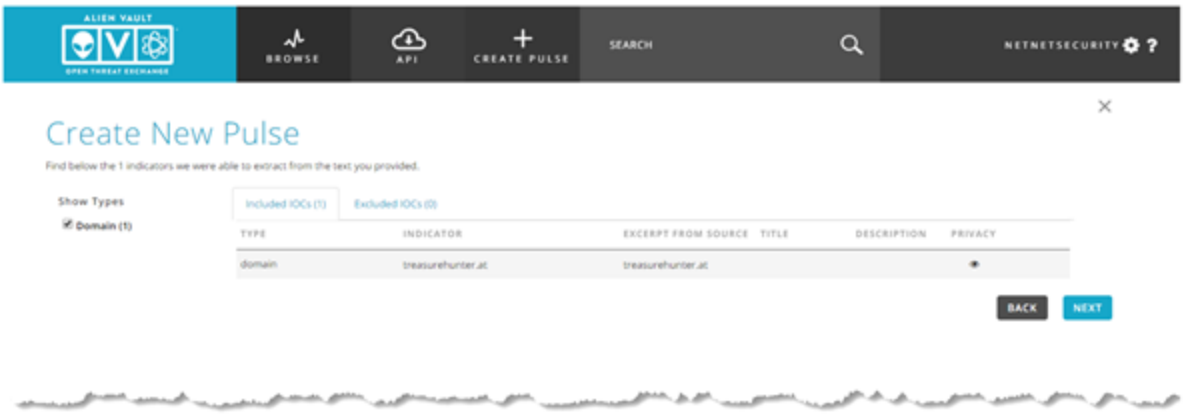


2. In the **Extract from Source** (LevelBlue Indicator Extractor) section of the **Create New Pulse** page, do one of the following, depending on the type of indicator you want to define for the new pulse:

- Type the URL of a website or blog.
- Drag and drop a text file (for example, a PDF, text, plain text log, STIX, or OpenIOC file).
- Paste the text describing an indicator.

3. Click **Next**.

OTX processes the request and displays the new pulse page with the newly Included indicators.



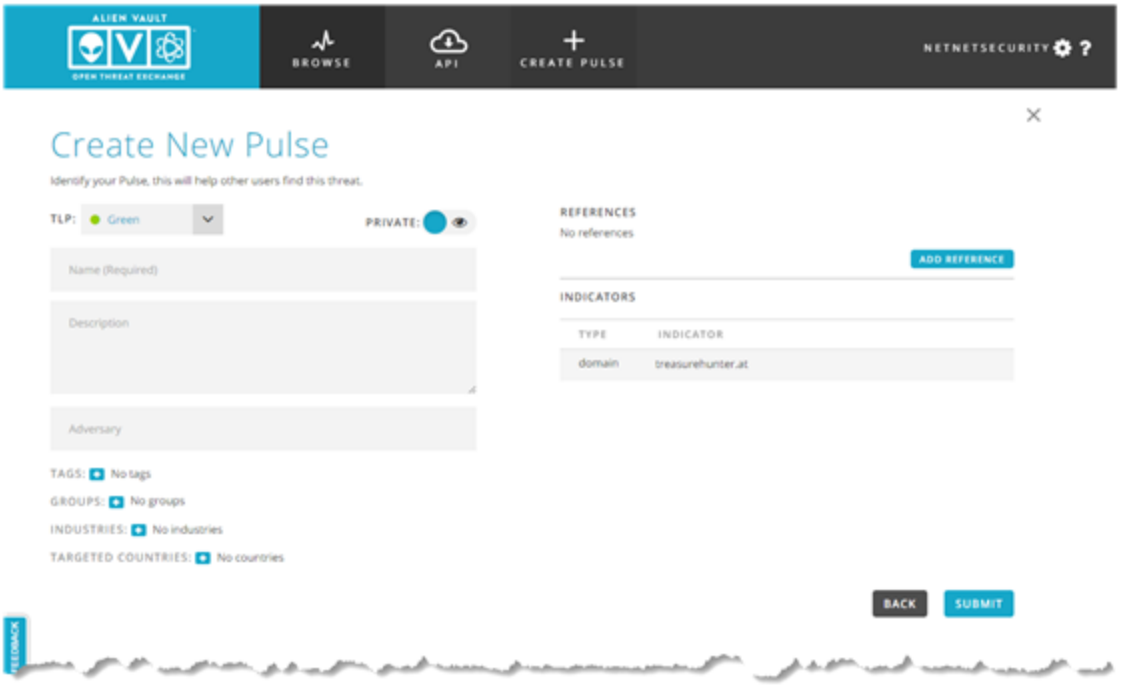
4. If OTX found any excluded IOCs, review the list of Excluded IOCs tab.

This tab 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.

5. If you see something suspicious on the list, transfer it to the list of Included IOCs.

6. Click **Next**.

OTX displays a final Create New Pulse page to include other details describing the new pulse you want contribute. The specific indicator you added on the previous page, and its type (for example, domain), appear on the right side of the page, in a table.



7. Identify the pulse and complete the pulse description with the following information:

- TLP — Indicate the Traffic Light Protocol (TLP) for the threat by expanding the TLP list. 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.
- Name — Give the pulse a concise name that uniquely characterizes the threat. This could consist of where the threat was found or what type of malware it represents, for example, “New PoSeidon spotted”.
- 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.

- Private — Indicate whether or not you want to share the pulse with others or make it private. (Private means that you do not want to share the pulse with others, because you need to conduct more research.)
- Tags — If your IOC is a URL, OTX creates relevant tags based on its 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.
- Groups — Add groups to associate with pulse.
- Industries — Specify primary industries targeted by threat.
- Targeted Countries — Specify countries that have been targeted by threat.

8. After reviewing all your entries for the new pulse, click **Submit**.

OTX returns you to the main pulse activity feed. Here you will see the pulse you just created, along with its associated tags. If you need to make changes to an existing pulse, for example, to add new indicators, you can simply open the existing pulse and add new indicators manually or using the LevelBlue Indicator extractor.

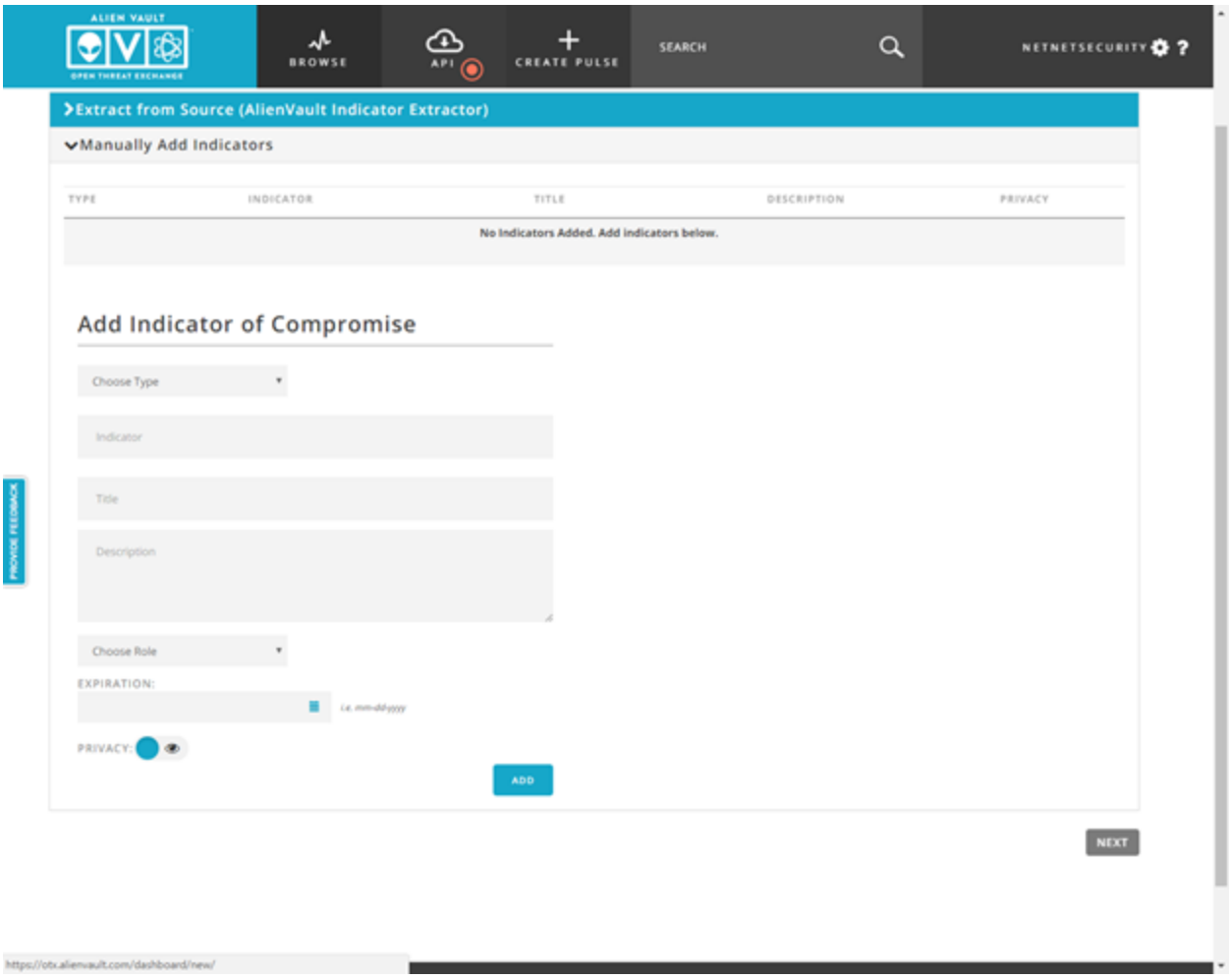
Creating a Pulse by Manually Adding Indicators

You can also create a pulse by adding indicators of compromise (IOCs) manually, as opposed to using the LevelBlue Indicator Extractor.

To create a pulse by manually adding indicators

1. Access the Create New Pulse page by selecting Create Pulse from the OTX user interface main menu.

2. Click the arrow to the left of the Manually Add Indicators section. A new data entry section appears.



3. From the Choose Type list, select the applicable IOC type.

4. Paste the indicator you want to include for the new pulse into the Indicator field.

5. Specify entries for the remaining fields you want to populate for the new pulse.

6. Click **Add**.

7. OTX again displays a final Create New Pulse page, allowing you to name and include other details describing the new pulse you want to submit.

8. After completing the remaining description entries for the new pulse, click **Submit**.

OTX returns you to the main pulse activity feed. Here you will see the pulse you just created, along with its associated tags. If you need to make changes to an existing pulse, for example, to add new indicators, you can open the existing pulse and simply add new indicators manually or using the LevelBlue Indicator extractor.

OTX Data with External Security Monitoring Systems

You can easily leverage OTX threat intelligence within your own security monitoring and management systems and tools, including USM Appliance or LevelBlue OSSIM, by taking advantage of the LevelBlue OTX DirectConnect API and DirectConnect SDK. You can connect to the OTX API using DirectConnect Agents available for a number of specific products and third party tools. If you have an USM Appliance/LevelBlue OSSIM installation, you can get the benefits of the DirectConnect API immediately simply by entering your OTX API key from the USM Appliance OTX Configuration web page.

Topics covered in this section include

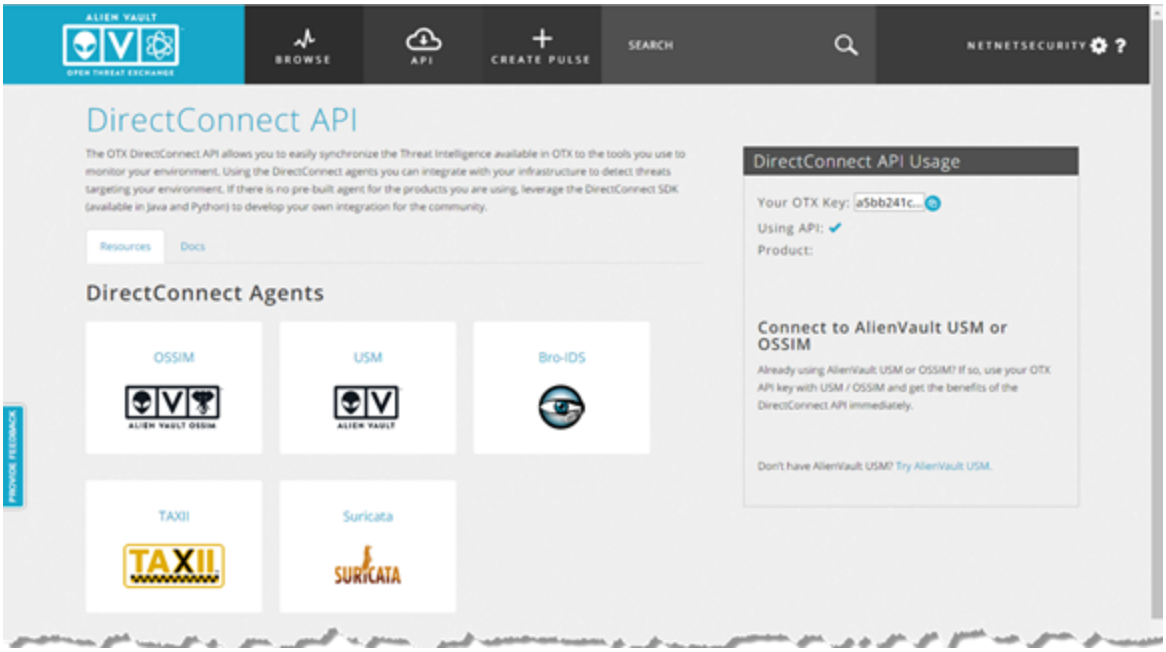
Connecting to the OTX API Using DirectConnect Agents

If you have an USM Appliance/LevelBlue OSSIM installation, you can get the benefits of the DirectConnect API immediately simply by entering your OTX API key on the Open Threat Exchange Configuration page in the USM Appliance web UI. In addition to DirectConnect support for USM Appliance and LevelBlue OSSIM, LevelBlue currently also provides DirectConnect Agents for the following platforms:

- Bro-IDS
- TAXII
- Suricata

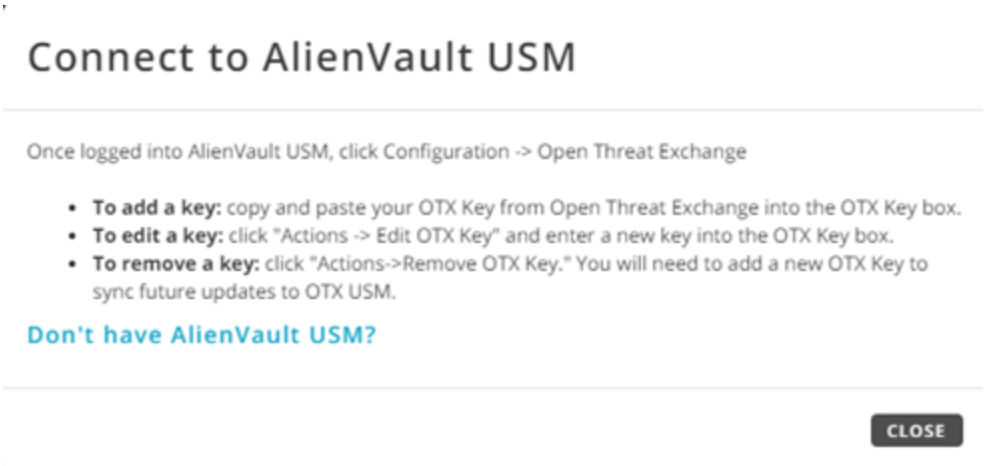
To connect to the OTX API using a DirectConnect Agent

1. From the OTX UI Home page, select the **API** menu option.



2. Click the box corresponding to the DirectConnect agent you want to use.

   If you clicked the label for USM Appliance, the following popup appears:



If you clicked the label for LevelBlue OSSIM, a similar popup appears specific to LevelBlue OSSIM. For the third-party products, you are directed to the GitHub page for your connector selection.

3. Copy your OTX key, located in the upper right corner of the DirectConnect API page, and follow the instructions provided to register your OTX key with your USM Appliance installation.

Accessing the OTX DirectConnect SDK

If a DirectConnect agent or connector that works with your particular product, tool, or environment is not available, you can make connections to the OTX API or develop a connector of your own, using the OTX DirectConnect SDK, available from the LevelBlue Labs™ GitHub library.

The DirectConnect SDK provides support for development of DirectConnect agents or connectors for the following programming environments:

- Java
- Python
- Golang

You can also always access the DirectConnect API using a command-line FTP/HTTP data transfer tool such as curl to access OTX threat intelligence information. For example:

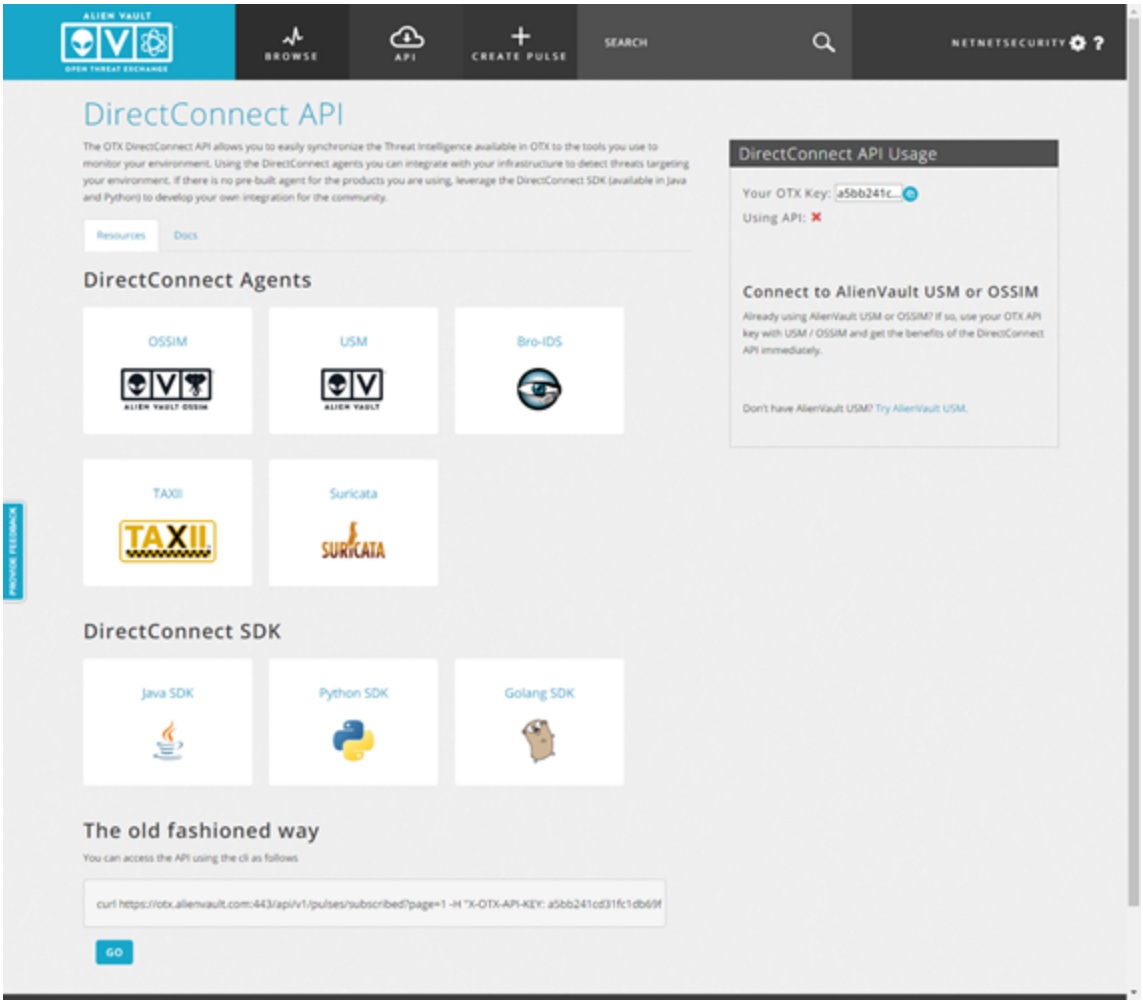
```
curl https://otx.alienvault.com:443/api/v1/pulses/subscribed?page=1 -H
"X-OTX-API-KEY
a5bb241cd31fc1db69fcf0fd61116160606lb9445e3758fd3e71d50e6477e12a"
```

You can access the DirectConnect SDK from two different locations:

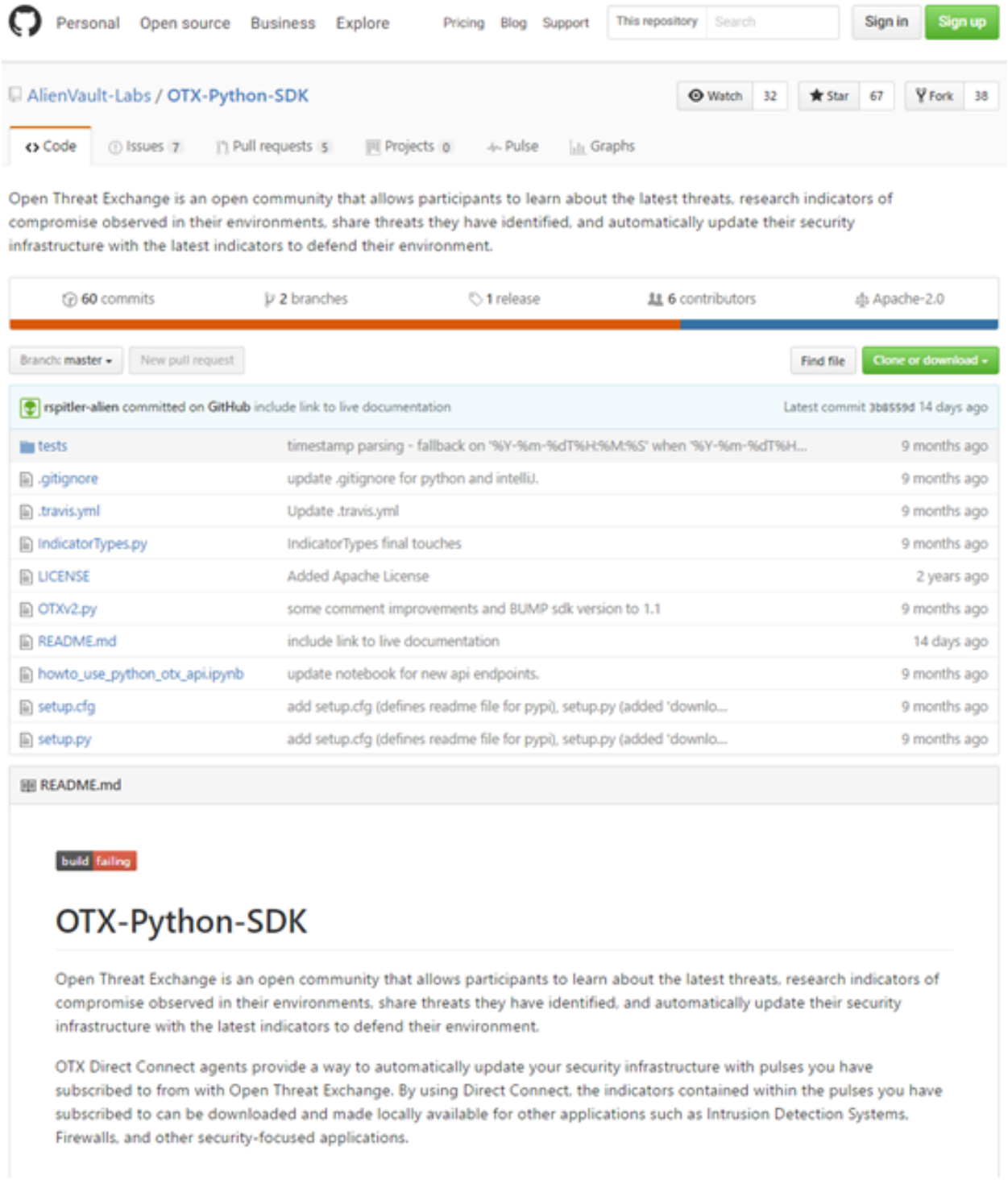
- The DirectConnect API page, accessed when you select the **API** menu option from the OTX Home page.
- The OTX Settings page, accessed when you click on the Settings ( ) icon from the OTX Home page.

To access the SDK from the DirectConnect API page

1. On the DirectConnect API page, scroll down and click one of the three labels: **Java SDK**, **Python SDK**, or **Golang SDK**.



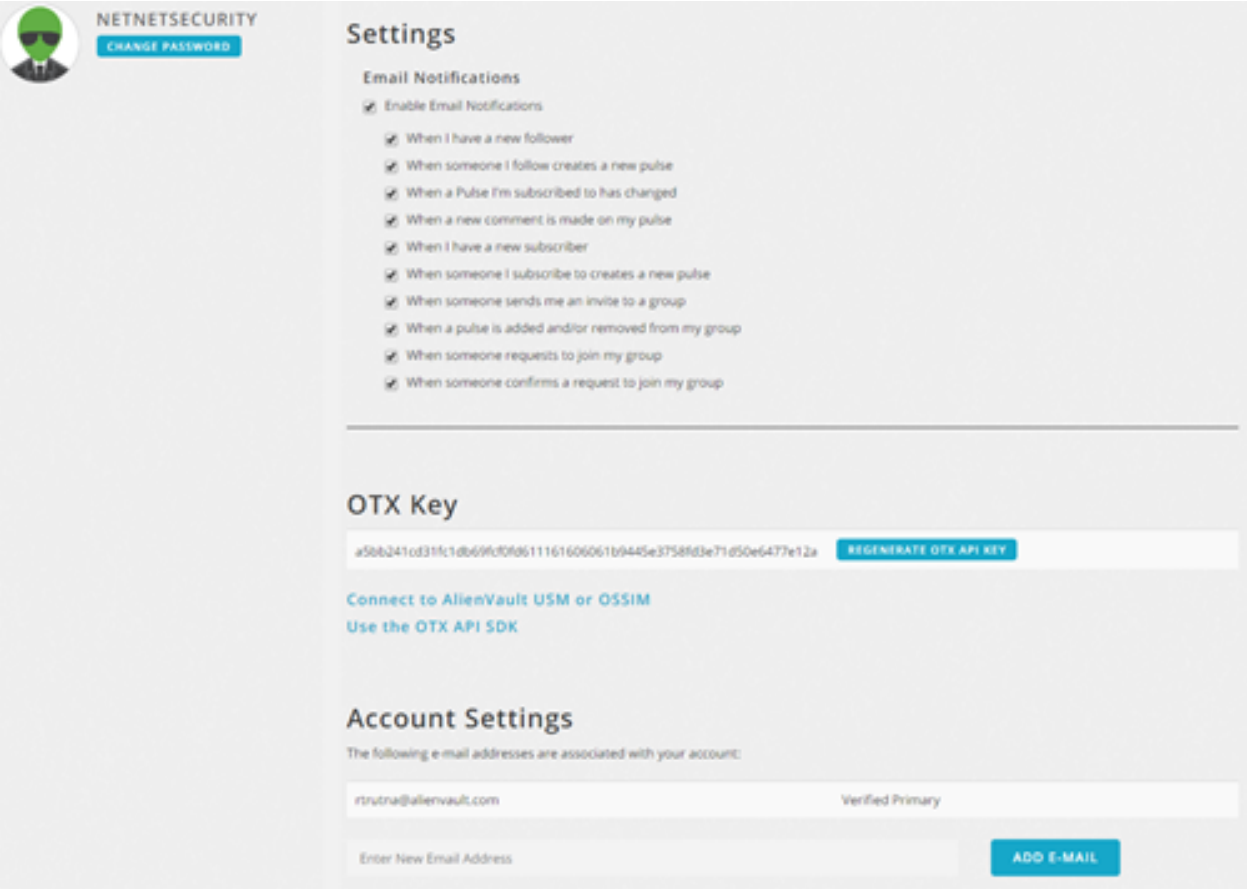
2. The OTX user interface directs you to the LevelBlue Labs SDK documentation page on GitHub for the specific language option you selected, for example, the OTX-Python-SDK resource page.



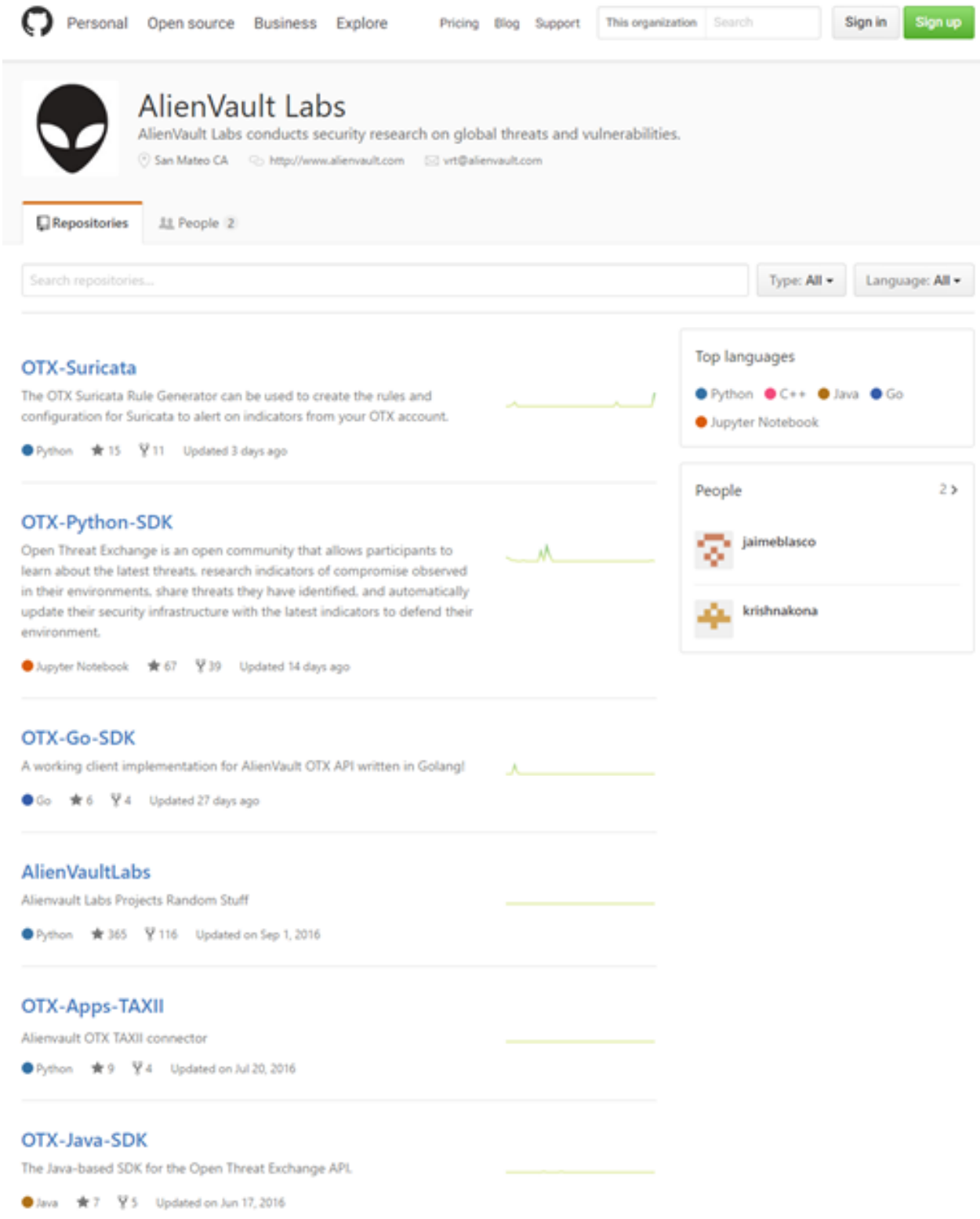
To access the Direct API SDK from the Settings Page

1. From the OTX user interface Home page, click on the **Settings** ( ) icon and choose the **Settings** menu option.

2. In the OTX key section of the page, click the **Use the OTX API SDK** link.



3. The OTX user interface directs you to the LevelBlue Labs SDK documentation page on GitHub which provides various support reference links for each of the different languages that are supported for the API.


Personal
Open source
Business
Explore
Pricing
Blog
Support
This organization
Search
Sign in
Sign up
AlienVault Labs
AlienVault Labs conducts security research on global threats and vulnerabilities.
San Mateo CA
http://www.alienvault.com
vrt@alienvault.com
Repositories
People 2
Search repositories...
Type: All
Language: All
OTX-Suricata
The OTX Suricata Rule Generator can be used to create the rules and configuration for Suricata to alert on indicators from your OTX account.
Python 15 11 Updated 3 days ago
OTX-Python-SDK
Open Threat Exchange is an open community that allows participants to learn about the latest threats, research indicators of compromise observed in their environments, share threats they have identified, and automatically update their security infrastructure with the latest indicators to defend their environment.
Jupyter Notebook 67 39 Updated 14 days ago
OTX-Go-SDK
A working client implementation for AlienVault OTX API written in Golang!
Go 6 4 Updated 27 days ago
AlienVaultLabs
Alienvault Labs Projects Random Stuff
Python 365 116 Updated on Sep 1, 2016
OTX-Apps-TAXII
Alienvault OTX TAXII connector
Python 9 4 Updated on Jul 20, 2016
OTX-Java-SDK
The Java-based SDK for the Open Threat Exchange API.
Java 7 5 Updated on Jun 17, 2016
Top languages
Python C++ Java Go
Jupyter Notebook
People 2 >
jaimeblasco
krishnakona

4. Choose whatever hyperlink options you want to view, to help you install and use the OTX SDK, for whatever language you want to use.