AlienVault

Using USM™ and OSSIM™ 5.1 with Open Threat Exchange (OTX)™

Using USM and OSSIM 5.1 with Open Threat Exchange (OTX)

Table 1. Revision Table

Revision No.	Date	Revision Description
2	Sept. 08, 2015	• Enhanced descriptions in topics from pages 4 through 16. • 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 that the Getting Started Wizard only comes with AlienVault All-in-One appliance. See Connecting OTX to USM. • Enhanced the description of how users contribute to OTX in About Contributing Threat Data to OTX. • Corrected example in the URL definition of **Table 2**. • Corrected Open Source Exchange to Open Threat Exchange in the note under **Who Has Access to IP Reputation?** • Corrected the description of how USM generates OTX-related alarms from IOC events. See **Analyzing OTX Alarms in USM**. • Corrected information about dates seen in the Trend Graph, accessible from the Security Events (SIEM) page. Corrected information about where to turn the graph on. The On/Off toggle is only present in the Events view. See **Trend Graph**. • Updated **Figure 10** based on USM/OSSIM 5.1.1 change regarding representation of Asset Value in Event Details view. • Enhanced field descriptions for the Alarms list and Alarm Details. See **Table 9** and **Table 11**. • Substituted references to `https://www.alienvault.com/documentation` with `https://www.alienvault.com/documentation/usm`. • Corrected erroneous trademark for IP Reputation. IP Reputation is not trademarked at this time; OTX IP Reputation Monitor™ is.

Contents

Audience for This Guide 4
About How Product Names Are Used in This Guide 4
What Is Open Threat Exchange (OTX)™? 4
About OTX Pulses and Indicators of Compromise 4
About OTX IP Reputation 6
Why Connect USM to the New OTX? 7
About Contributing Threat Data to OTX 8
Voluntary and Anonymous Data Contribution 8
Information Collected by AlienVault 9
Connecting OTX to USM 9
About the Signup Process for Existing Subscribers 9
Connecting Through the Open Threat Exchange Configuration Page 10
Connecting Through the Getting Started Wizard 13
Managing Pulse Subscriptions 14
Subscribing to a Pulse 14
Unsubscribing from a Pulse 15
Managing OTX Events and Alarms in USM 16
Analyzing OTX Security Events in USM 16
Analyzing OTX Alarms in USM 29
Reviewing Your OTX Account and Pulse Activity 37
Reviewing Account Information 37
Reviewing OTX Pulse Subscriptions in USM 39
Getting Information About the Top OTX Pulses 40
Reviewing OTX Dashboard Information in USM 42
Open Threat Exchange Statistics 42
Events from Most Active OTX Pulses 42
Events from All OTX Pulses 43
IP Reputation Dashboard 43

Audience for This Guide

This guide is intended for users of Unified Security Management (USM)™ 5.1 and OSSIM™ 5.1, who want to the additional threat data provided by linking their products with AlienVault Open Threat Exchange (OTX)™.

For a more comprehensive understanding of OTX, refer to the *AlienVault Open Threat Exchange (OTX) User Guide* on the AlienVault Documentation Center (`https://www.alienvault.com/documentation/usm`).

About How Product Names Are Used in This Guide

References to the product name USM™ in this guide are intended to encompass OSSIM™ functionality unless otherwise noted.

When the OSSIM implementation of OTX differs from USM, the guide explicitly states this, as it does, for example, regarding access to IP Reputation data.

What Is Open Threat Exchange (OTX)™?

Open Threat Exchange (OTX)™ is the world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data.

OTX provides open access for all, allowing you to collaborate with a worldwide community of threat researchers and security professionals. This access enables collaborative research by allowing everyone in the OTX community to actively share threat data, trends, and techniques. In addition to accelerating the distribution of the latest threat data, OTX automates the process of updating your security infrastructure. OTX enables everyone in the OTX community to actively collaborate, strengthening their own defenses.

Information is derived from both public and private entities, as well as other resources.

The OTX platform consists of two chief components:

- **Pulses—**Collections of indicators of compromise (IOCs), reported by the OTX community, which other community members review and on which they provide comments. Pulses provide you with a summary of the threat, a view into the software targeted, and the related IOCs, reported by the OTX community worldwide. (For details, see **About OTX Pulses and Indicators of Compromise**.)
- **IP Reputation—**Provides notification of communication between known malicious hosts and your assets.

Both of these components benefit USM and OSSIM in very material ways, described under **Why Connect USM to the New OTX?**

About OTX Pulses and Indicators of Compromise

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.

An 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 contains at least one, but more often multiple 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.
URL	Uniform resource locations (URLs) specify the location of a resource associated with suspected malicious activity. This is often in the form of a protocol prefix, for example, URI: filez.jackson.net.
URI	A uniform resource identifier (URI) consists of a sequence of characters describing the location of a 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 a network exhibiting malicious behavior.
mutex	Name of a mutex resource describing the execution architecture of a file, which may be malicious.
CVE (Common Vulnerabilities and Exposures)	Describes a software vulnerability that can be exploited to engage in malicious activity.

About OTX IP Reputation

OTX IP Reputation identifies IP addresses and domains worldwide that are submitted by the OTX community. IP Reputation 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 can affect your system.

IP Reputation Data Sources

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

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

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

Who Has Access to IP Reputation?

All USM users receive the benefit of IP Reputation data whether or not they sign up for an OTX account. However, OSSIM users must explicitly subscribe to IP Reputation to have access to its data unless they subscribe to OTX. In this case, they receive the full benefits of OTX, including IP Reputation.

When you open an OTX account, you may elect to share IP Reputation data with other OTX users. Any data you contribute are anonymous and secure. **Figure 1** illustrates the data that IP Reputation shares with OTX.

Note: You can configure USM to stop sharing IP Reputation data with OTX at any time on the Open Threat Exchange Configuration page.

DESTINATION ALL:

HOST	EVENT	COUNT
216.151.164.	snort: "ET TROJAN Possible Graftor EXE Download Common Header Order"	4
216.151.164.	directive_event: AV Malware, malware infection detected on SRC_IP	1
216.151.164.	directive_event: AV Malware, trojan connecting to a low reputation CnC server on SRC_IP	2
5.149.248.1	snort: "ETPRO TROJAN Backdoor.Win32.Simda.abpn Checkin"	1
176.9.63.2	snort: "ET POLICY Python-urllib/ Suspicious User Agent"	17
255.255.255.2	directive_event: AV Policy violation, Dropbox file sharing service usage on SRC_IP	1
79.142.66.2	snort: "ET TROJAN Simda.C Checkin"	12
159.224.244.2	snort: "ETPRO TROJAN Trojan-Spy.Win32.Zbot.relx Checkin"	10

SOURCE ALL:

HOST	EVENT	COUNT
216.151.164.	snort: "ET CURRENT_EVENTS Malicious Redirect 8x8 script tag"	1
216.151.164.	directive_event: AV Client side attack, external host delivered known exploit kit component and executable, successful exploitation to DST_IP	1
216.151.164.	directive_event: AV Misc, suspicious executable download from a bad IP reputation web site on DST_IP	2
216.151.164.	snort: "ET POLICY PE EXE or DLL Windows file download"	6
50.197.161.1	snort: "GPL WEB_SERVER .htpasswd access"	2
50.197.161.1	snort: "ET WEB_SPECIFIC_APPS PHP phpMyAgenda rootagenda Remote File Include Attempt"	2
50.197.161.1	snort: "GPL WEB_SERVER service.cnf access"	1
50.197.161.1	snort: "ETPRO WEB_SERVER Oracle Web Server Expect Header Cross-Site Scripting"	1
50.197.161.1	snort: "ET SCAN Sqlmap SQL Injection Scan"	2

Figure 1. Sample of data shared by IP Reputation with OTX.

IP Reputation Ranking Criteria

IP Reputation uses ranking criteria based on IP Reliability and IP Priority that OTX updates on an ongoing basis to calculate changing assessments to risk level. This helps prevent false positives.

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.

For details about the IP Reputation view on the OTX Dashboard in USM, see **IP Reputation Dashboard**.

Why Connect USM to the New OTX?

When you sign up for OTX and connect it to your USM/OSSIM instance, it configures USM to receive raw pulse data.

USM then correlates that data, alerting you to related OTX pulse and IP Reputation-related security events and alarms when it detects IOCs interacting with assets in your environment. Such interactions might consist of malicious IPs communicating with systems, malware detected in your network, or outbound communication with command-and-control (C&C) servers.

Connecting OTX to USM/OSSIM helps you to better manage risks and effectively take action on threats in the following ways:

- USM receives threat updates every 15 minutes in the form of raw data for all pulses to which you subscribe, either directly or through subscriptions to other OTX users. You likewise receive updates on your subscribed pulses by email.
- Review a pulse activity feed, containing detailed analytics about related threat vectors reported by OTX.
- From the USM Dashboard Overview, see which pulses in your environment are most active, as soon as you log into USM.
- Receive immediate notification in the form of an event or an alarm when a malicious IP address communicates with any of your system assets, or when USM identifies any other IOCs active in your network. For details, see **Analyzing OTX Security Events in USM** and **Analyzing OTX Alarms in USM**.

Important Information for Current AlienVault Community (OTX) Account Holders

If you previously signed up for an AlienVault Community account, you must still complete the OTX signup process to access the enhanced OTX platform.

For details about the signup process, see **Connecting OTX to USM**.

About Contributing Threat Data to OTX

OTX community members contribute to OTX in the following ways:

- When they create pulses to share threat data they gathered and want to share with others.
- When they comment on pulses.
- When USM users connected to OTX explicitly allow OTX to extract any IP Reputation event data from their system environment. OTX can then use that information to re-evaluate IP Reputation severity levels that affect USM correlation directives.

  To understand the nature of what OTX gathers, see **Voluntary and Anonymous Data Contribution** and **Information Collected by AlienVault**.

Voluntary and Anonymous Data Contribution

All data contributed to OTX whether individually or through USM are completely voluntary and anonymous.

No data submitted to OTX through USM can be used to identify any of the following:

- Any individual.

- Data coming from any individual system.
- Data coming from the internal IP traffic of any individual system.

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.
- Telemetry of indicators of compromise associated with any OTX pulse detected in the subscriber environment.

Note: You may choose to stop sharing data with OTX at any time by visiting the Open Threat Exchange Configuration page in USM (Configuration > Open Threat Exchange).

Connecting OTX to USM

All USM or OSSIM users—whether or not they have subscribed to OTX in past, for example, to contribute or receive IP Reputation and other data—should sign up for or upgrade to the new OTX platform. (For details, see **Why Connect USM to the New OTX?**)

You can sign up for and connect an OTX account to USM from one of the following USM locations:

- **Open Threat Exchange Configuration** page, if you are an existing USM user.
- **AlienVault Getting Started Wizard,** if you are configuring a new USM All-in-One appliance.

About the Signup Process for Existing Subscribers

When you upgrade to USM or OSSIM 5.1 and log in for the first time, you receive the message:

```
OTX upgrade available. Please re-authenticate your OTX account to take advantage of the new features!
```

The same message appears within the **Top OTX Activity in Your Environment** pod of the Dashboard Overview.

Connecting Through the Open Threat Exchange Configuration Page

The following procedures describe how to connect USM to OTX for the first time, and how to upgrade to the new OTX platform from an AlienVault Community account.

Important: If your organization deploys federated environments, you must use the same OTX key in all connected USM AIO and USM Server appliances. Otherwise, the OTX data will be inconsistent amongst the federated levels.

Signup for USM Users Who Have Never Had an OTX Account

This procedure describes how to connect USM to OTX for USM users who have never subscribed previously.

To connect USM to the new OTX platform

1. From the USM Primary Navigation bar, select Configuration > **Open Threat Exchange.**
2. On the **Open Threat Exchange Configuration** page, click **sign up** (Figure 2).

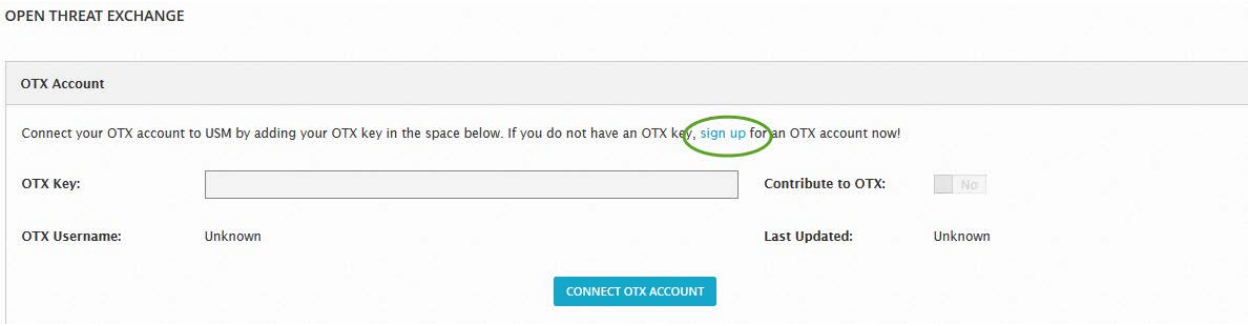

Figure 2. OTX sign up link on the USM-OSSIM Open Threat Exchange Configuration page.

3. Fill out the form that appears with the following information:
   a. **Username—**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—**Type the email address to which you want OTX to send you pulses, and which records your account.
   c. **Password—**Type a password.
   d. **Password (again)—**Retype the password to confirm.
4. Click **Sign Up.**

As part of the signup process, an information page appears, reporting that a verification email 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 within it.

   This takes you to a confirmation page that prompts you to confirm the email address and the username you provided during signup.

6. Click **Confirm.**

   This takes you to the OTX Activity feed.

7. Click on your username next to the gear icon, located in the upper-righthand corner of the Activity feed.
8. On the **Settings** page, copy the OTX key displayed.
9. Paste the OTX key you just copied into the empty **OTX Key** field of the USM **Open Threat Exchange Configuration** page.
10. Click **Connect OTX Account.**

    USM confirms that your OTX account is now linked.

11. (Optional) If you *do not* want to contribute IP Reputation data to OTX, click the gray square next to **Contribute to OTX** to toggle the setting to **No**.

    The default setting is Yes.

Signup for Legacy OTX Account Holders Who Forgot Their OTX Email

The following procedure describes how to upgrade your legacy AlienVault Community account to the new OTX platform, should you not remember the email you subscribed with previously.

Because OTX keeps track of existing users by the email they used at signup time, if you forget it, you must open a new OTX account.

You receive a new OTX key and the old key no longer works.

You must then delete your legacy OTX key and paste the new key into the **OTX Key** field on the USM OTX Configuration page before you can connect the accounts.

To connect USM to the new OTX platform

1. From the USM Primary Navigation bar, select Configuration > **Open Threat Exchange.**
2. On the Open Threat Configuration page of USM, click **Actions** and select **Remove OTX Key.**
3. When USM prompts you to confirm the deletion, click **Yes.**
4. Click **sign up.**
5. Fill out the registration form with the following information:
   a. **Username—**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—**Type the email address to which you want OTX to send you pulses, and which records your account.

c. **Password—**Type a password.

d. **Password (again)—**Retype the password to confirm.

6. Click **Sign Up.**

   As part of the signup process, an information page appears, reporting that a verification email was sent to the email address you provided.

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

7. After you receive the email, click the link within it.

   This takes you to a confirmation page that prompts you to confirm the email address and the username you provided during signup.

8. Click **Confirm.**

9. On the OTX Activity feed, click on your username next to the gear icon, located in the upper-righthand corner of any OTX page.

10. On the **Settings** page, copy the OTX key displayed.

11. Paste the OTX key you just copied into the empty **OTX Key** field of the USM **Open Threat Exchange Configuration** page.

12. Click **Connect OTX Account.**

    USM confirms that your OTX account is now linked.

Signup for Existing OTX Account Holders Who Remember Their OTX Email

When upgrading from a previous AlienVault Community account to the new OTX platform, you must use the same email address that you did to open your AlienVault Community account.

To connect USM to the new OTX platform

1. Log into USM.
2. Open a browser and go to **https://otx.alienvault.com**.
3. Click **Sign Up.**
4. Fill out the registration form with the following information:

   a. **Username—**Type the same username you used to open the legacy OTX account.

   b. **Email Address—**Type the same email address you used to open the legacy OTX account.

   c. **Password—**Type your existing OTX password.

   d. **Password (again)—**Retype the password to confirm.

5. Click **Sign Up.**

   As part of the signup process, an information page appears, reporting that a verification email 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, click the link within it.

   This takes you to a confirmation page that prompts you to confirm the email address and the username you provided during signup.

7. Click **Confirm.**

   This completes the OTX signup process; USM is now receiving data from the new OTX platform.

Connecting Through the Getting Started Wizard

This task describes how to connect OTX and USM from the USM Getting Started Wizard.

The Getting Started Wizard displays five configuration tasks that you can complete using the wizard to configure your USM deployment. Setting up an OTX account and connecting it to USM appears as the final task (Figure 3).

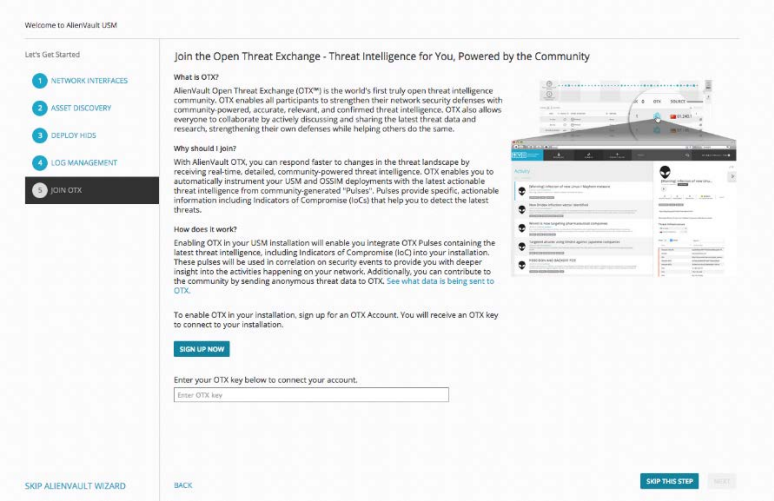

Figure 3. Connecting OTX and USM through the Getting Started Wizard.

To connect OTX to USM

1. From the **Join OTX** page of the Getting Started Wizard, click **Signup Now.**
2. Fill out the registration form with the following information:

   - 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.

- An email address—If you previously opened an AlienVault Community account, make sure to use the same email you did when you opened it.
- A password, which, after initial entry, you must retype to confirm.

3. Click **Sign Up.**

   As part of the signup process, 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.

4. After you receive the email, click the link and, on the confirmation page for logged-in USM users, click **Login.**

   A USM key page appears. It displays your OTX key and states that the username you used to register for OTX is logged in.

5. Copy the OTX key and paste it into the **Enter OTX Key** field shown in Figure 3.
6. Click **Next.**
7. On the **Thank You for Joining the Open Threat Exchange** page, click **Finish.**

Managing Pulse Subscriptions

When you connect OTX to USM, you automatically subscribe to every pulse generated by AlienVault OTX Labs, receiving new updates every 15 minutes through an OTX Activity feed and by email.

You can also subscribe explicitly to a pulse created by another OTX community member whose research you respect. This ensures that USM receives the same raw data on every pulse that user creates or updates in OTX.

When you connect USM to OTX, you receive events and alarms when a threat vector (indicator of compromise) from a pulse you subscribe to interacts with one or more of your system assets. (For information about OTX security events and alarms in USM, see **Analyzing OTX Security Events in USM** or **Analyzing OTX Alarms in USM**.)

For information about subscribing to an OTX community member and their pulses, see the *Open Threat Exchange (OTX) User Guide.*

Subscribing to a Pulse

Subscribing to pulses instruments USM to correlate raw data it receives from OTX directly related to those pulse. This occurs when an indicator associated with any of those pulses interacts with your system assets.

As described under **Managing Pulse Subscriptions**, when you connect your accounts, you automatically subscribe to all pulses from AlienVault.

To subscribe, on the other hand, to a pulse created by an OTX community member, follow this procedure.

To subscribe to a pulse

4. Launch 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 4).

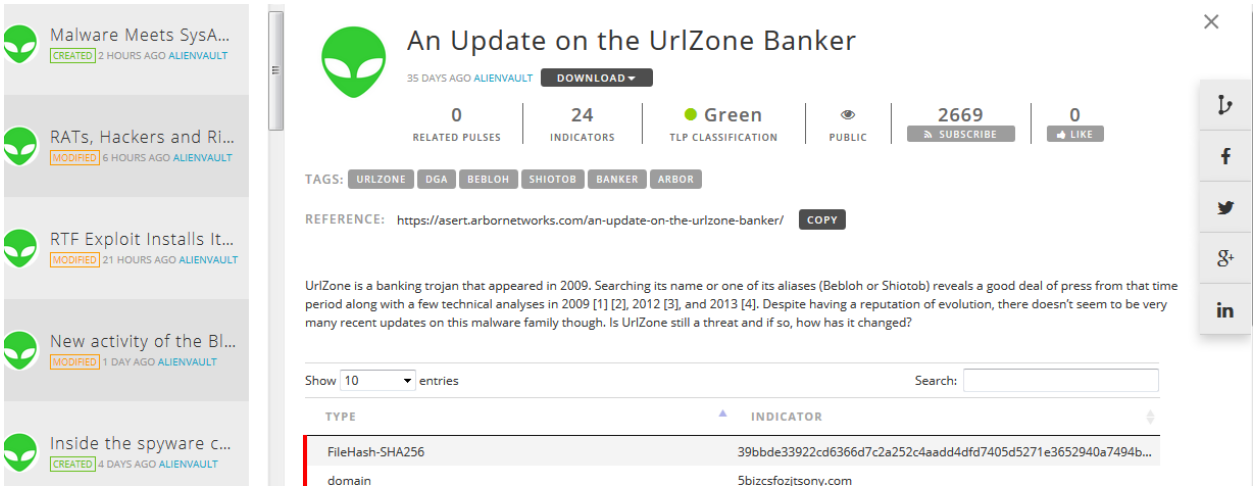

Figure 4. Subscribing to a pulse in OTX.

7. Click **Subscribe,** located under the pulse name.
8. Log into USM to view the pulse.

   The pulse now appears in the **OTX Subscriptions** section of the **Open Threat Exchange Configuration** page.

Note: You may need to refresh the page to see the newly added pulse.

Unsubscribing from a Pulse

When you unsubscribe from a pulse, you still receive information about the threat in your Activity feed, but USM no longer pulls any raw data for that pulse into USM for correlation purposes. This means that you are no longer instrumented against it.

To unsubscribe from a pulse

1. Within OTX, 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.

2. Click the pulse.
3. On the **Pulse Details** page, click **Unsubscribe.**

Managing OTX Events and Alarms in USM

The primary location from which USM users gain detailed and actionable data about a pulse is through the USM **Security Events** and **Alarms** reporting pages.

- Security Events (SIEM) reporting page (Analysis > **Security Events [SIEM]).** See **Analyzing OTX Security Events in USM**.
- Alarms reporting page (Analysis > **Alarms**). See **Analyzing OTX Alarms in USM**.

Other locations in USM provide you with overviews of pulse information, allowing you to scan pulse activity and IP Reputation data at a high level:

- **Top OTX Activity in Your Environment** pod (Dashboards > **Overview**)—Provides a snapshot of those pulses most actively interacting with your assets. See **Getting Information About the Top OTX Pulses**.
- **Open Threat Exchange Configuration** (Configurations > **Open Threat Exchange**)—Acts as an activity feed for all of the pulses you subscribe to in OTX. See **Reviewing Your OTX Account and Pulse Activity.**

Analyzing OTX Security Events in USM

You can view information related to OTX events in USM through two views under **Analysis > Security Events (SIEM)**:

- **SIEM view—**See **About the SIEM View**.
- **Real-Time view—**See **About the Real-Time View.**

The main difference between the two views is that the default **Security Events (SIEM)** view offers you the ability to filter OTX events using dates or date ranges.

About the SIEM View

The SIEM view displays any events generated by intruders to your system, based either on OTX pulses you subscribe to or on malicious IPs contacting your assets and seen by OTX IP Reputation.

The SIEM view consists of the following sections:

- **Event Filters—**Filtering criteria that allow you to fine-tune your OTX event search using date ranges, and whether the events you want to see are IP Reputation- or OTX pulse-related.

> **Note:** When starting a new query within the Advanced Search box, for best query results, clear the filters from previous searches.

- **Trend Graph**—Shows event activity levels by date in a graphical format.
- **Events List**—After you select the IP Reputation or OTX Pulse filters, displays all of the results that correspond to your OTX search criteria.

Event Filters

USM provides a rich set of filters for searching on events in your environment. This topic describes only those filters used to select and view OTX events.

Within the **Event Filters** section (Figure 5), you can create an OTX-specific search of events based on any or all of the filters described in Table 3.

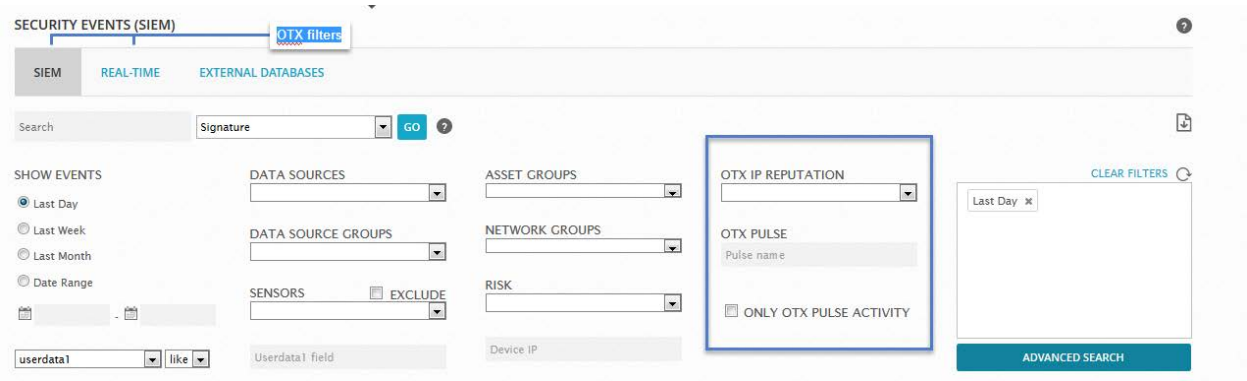

Figure 5. OTX-related filters in the SIEM view of the Security Events page.

Table 3. OTX event filters.

Filter Name	Description
OTX IP Reputation	Clicking the list icon expands the list to show a set of IP Reputation filters. These let you see *all* events with IP Reputation data or, alternatively, only events with IP Reputation data of a specified severity level, or type of malicious activity. IP Reputation ranks severity based on the number of reports existing about an IP address, as well as the nature of the threat the IP poses. For more information, see IP Reputation Ranking Criteria.
OTX Pulse	Double-clicking this field expands a list of pulse names, from which you then select a pulse to review as an event. If you know the pulse name, you can type it within the field. This quickly displays the pulse from the list.
Only OTX Pulse Activity	Shows all events within your environment resulting solely from OTX pulse indicators. **Note:** You cannot filter on events with IP Reputation data and OTX pulses simultaneously.

Filter Name	Description
Show Events	Filters for OTX events, based on a specific day, week, month, or range of time.

Note: When starting a new query within the **Advanced Search** box, for best query results, clear the filters from previous searches.

Trend Graph

The Trend Graph provides a graphical representation of spikes in event activity, including OTX events, within your environment currently.

The Trend Graph does not appear by default. You must turn it on.

To view or to close the Trend Graph

- Under the **Events** tab, click **Off** (next to **Show Trend Graph**) to toggle the graph to **On** (Figure 6).

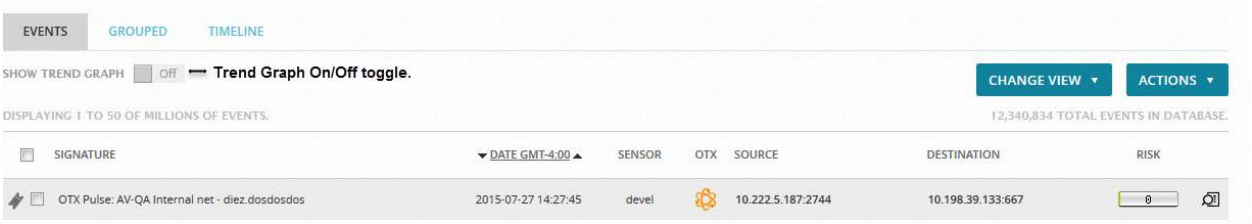

Figure 6. Trend Graph On/Off toggle.

The higher the Trend Graph spike, the more events are or were occurring, depending on the filtered time period. The lower the spike, the fewer events (Figure 7).

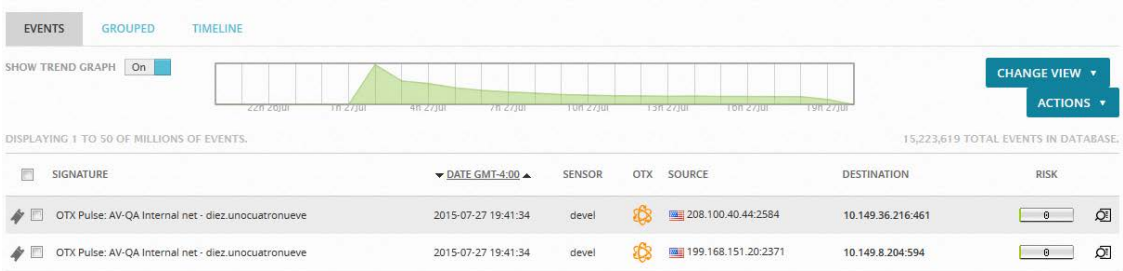

Figure 7. Trend Graph of OTX pulses on the Security Events page.

The Grouped view and Timeline tabs are unrelated to the Trend Graph and simply represent different ways of looking at the data in the Events list.

Events List—SIEM View

OTX events are immediately identifiable within the OTX column of the SIEM Events list by their special icon (Figure 8 and Figure 9).

SIEM Events List—IP Reputation View

Figure 8 shows the SIEM Events list for events containing IP Reputation data, specifically.

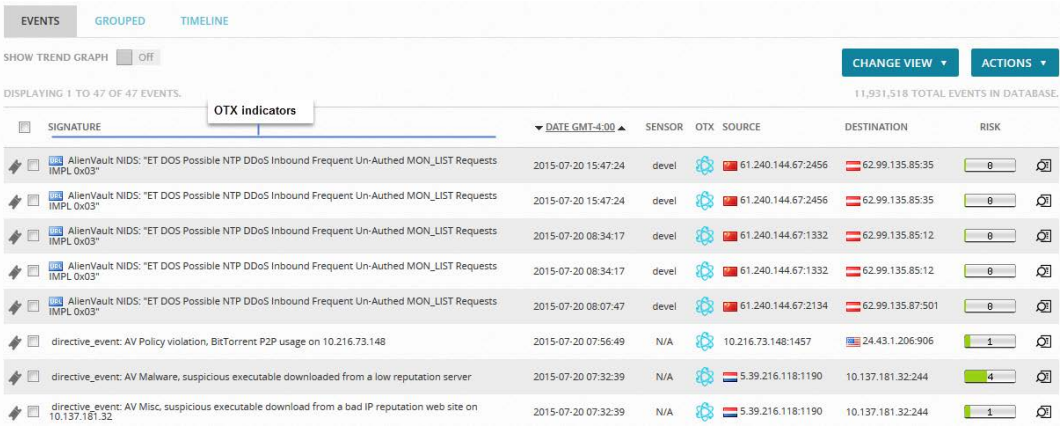

Figure 8. SIEM Events list—IP Reputation view.

SIEM Events List—OTX Pulse View

Figure 9 shows the SIEM Events list for OTX Pulse events, specifically.

Figure 9. Sample SIEM Events list—Pulse view.

Table 4 describes categories of information for both events with IP Reputation data and OTX pulse events in the Events list.

Table 4. SIEM Events list columns.

Column Name	Description
Signature	• If IP Reputation—IP Reputation indicator types associated with event. • If OTX pulses—Name of the pulse whose indicators are associated with the event.
Date	GMT date and time registered by USM for the event.
Sensor	Name of USM Sensor detecting the event, if available.

Column Name	Description
OTX	• **Orange—**Alarm was generated by one of the following: o A pulse o Both IP Reputation and OTX pulse indicators. In this case, the pulse name displays. • **Blue—**Alarm contains IP Reputation data about one more of the IP address involved.
Source	Hostname or IP address of the host, with national flag if country is known, that initiates the event.
Destination	Hostname or IP address of the host, with national flag if country is known, that receives the event.
Risk	Risk level, based on asset value × event priority × event reliability ÷ 25. For more information about risk assessment, see the *Asset Management Guide* (`https://www.alienvault.com/documentation/usm`).
More Information Icon	Clicking the magnifying glass takes you to the Event Details. (See **Getting More Event Details**.) **Note:** You can go to **Event Details** by clicking anywhere within the event, with the exception of the OTX icon.

Getting More Event Details

Event Details identifies the IP source and IP destination of a selected event with its associated asset target. It also displays the number of indicators involved, when the event relates to an OTX pulse, and the IP Reputation-calculated reliability and risk level data **(**Figure 10 and Table 6).

With the exception of OTX icon color, the Event Details for both IP Reputation and OTX pulses contains the same categories of information (Table 5).

If no data appear within a category of information (N/A), it means that USM has no related data in the event log or the asset inventory.

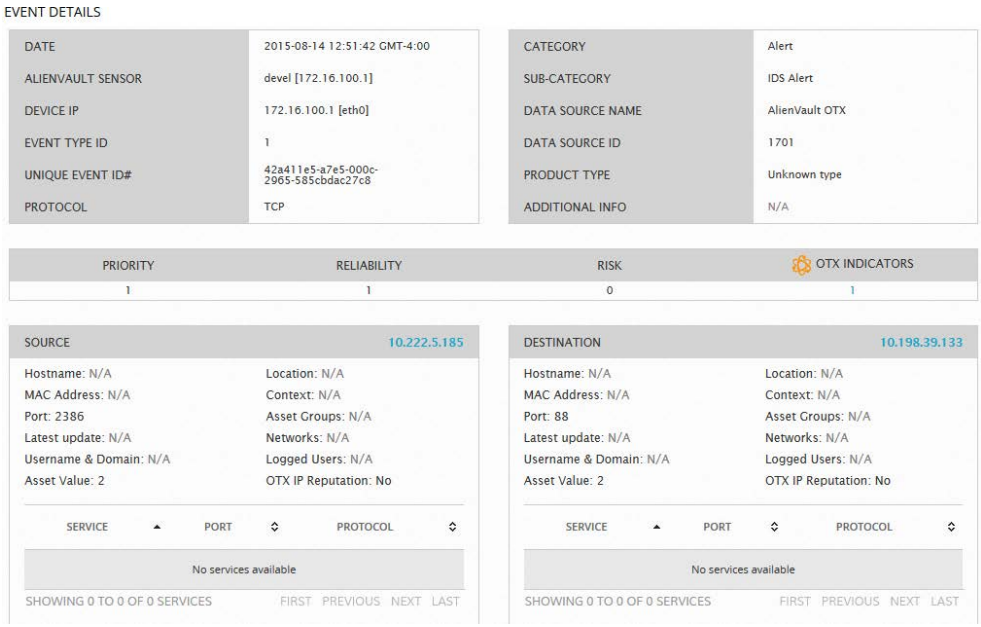

Figure 10. Sample Event Details, showing one indicator associated with an OTX pulse event.

Figure 11. Bottom half of Event Details, showing Raw Log data for an event.

Table 5. Event Details

Field	Description
Date	Date and time of the event.
AlienVault Sensor	Sensor that processed the event.
Device IP	IP address of the USM Sensor that processed the event.
Event Type ID	ID assigned by USM to identify the event type.

Field	Description
Unique Event Type ID#	Unique ID number assigned to the event by USM.
Protocol	Protocol used for the source/destination of the event, for example, TCP IP.
Category	Event taxonomy for the event, for example, authentication or exploit.
Sub-Category	Subcategory of the event taxonomy type listed under Category. For example, this would be Denial of Service, if the category were Exploit.
Data Source Name	Name of the external application or device that produced the event. **IP Reputation events—**Name of the external application or device on record with IP Reputation. **OTX pulse events—**All events from OTX pulses show *AlienVault OTX* as the producer of the event.
Data Source ID	ID associated with the external application or device that produced the event. **IP Reputation events—**Data source ID specific to the external application or device that produced the event. **OTX pulse events—**Data source ID for all OTX pulse events is 1701.
Product Type	AlienVault Labs event taxonomy for product type. **Note:** Events with IP Reputation-related data have product types; at this time, OTX pulses do not.
Additional Info	If the event were generated by a suspicious URL, for example, this field would state URL. When present, these URLs provide additional background information and references about the components associated with the event.
Priority	Priority ranking, based on value of the event type. Each event type has a priority value, used in risk calculation.
Reliability	Reliability ranking, based on the reliability value of the event type. Each event type has a reliability value, which is used in risk calculation.
Risk	Risk level is calculated based on asset value × event priority × event reliability ÷ 25. For more information about risk assessment, see the *Asset Management Guide* (`https://www.alienvault.com/documentation/usm`).
OTX Indicators	Number of indicators associated with an IP Reputation or OTX pulse event.

Field	Description
Source/Destination	IP addresses and hostname for the source and destination, respectively, of the event. If the host is an asset, you can right-click it to go to the **Asset Details** page for information. Right-clicking the IP address displays a menu from which you can select information about the IP, such as all events originating from that host or all events for which the IP is the destination.
• Hostname	Hostname of the event source/destination. If the source or destination hostname for an event is within your asset inventory, this field contains a value. You can click it to go to the **Asset Details** page for more information.
• MAC Address	Media Access Control (MAC) of the host for the event, if known.
• Port	External or internal asset source/destination port for the event.
• Latest Update	The last time USM updated the asset properties.
• Username & Domain	Username and domain associated with the asset that generated the event.
• Asset Value	Asset value of the asset source/destination if within your asset inventory.
• OTX IP Reputation	(Yes/No) Whether or not IP Reputation identifies the IP address as suspicious.
• Location	If the host country of origin is known, displays the national flag of the event source or destination.
• Context	If the asset belongs to a user-defined group of entities, USM displays the contexts.
• Asset Groups	When the host for the event source/destination is an asset belonging to one or more of your asset groups, this field lists the asset group name or names. You can click the field to go to the **Asset Details** page for more information.
• Networks	When the host for the event source/destination is an asset belonging to one or more of your networks, this field lists the networks. You can click the field to go to the **Network Group Details** page for more information.
• Logged Users	A list of any users who have been active on the asset, as detected by the asset scan, for example, with the username and user privilege (such as admin).

Field	Description
Service	List of services or applications detected on the source/destination port.
Port	Port used by the service or application.
Protocol	Protocol used by the service or application.
When event data derives from a log or the asset inventory, the fields below appear after Service, Port, and Protocol and above the Raw Log data (Figure 12). Otherwise, these fields do not display.	
Filename	Name of file associated with the event.
Username	The username associated with the event.
Password	The password associated with the event.
Userdata 1-9	User-created log fields.
Payload	Payload of the event.
Rule Detection	AlienVault NIDS rule used to detect the event.
Raw Log	Raw log details of the event.

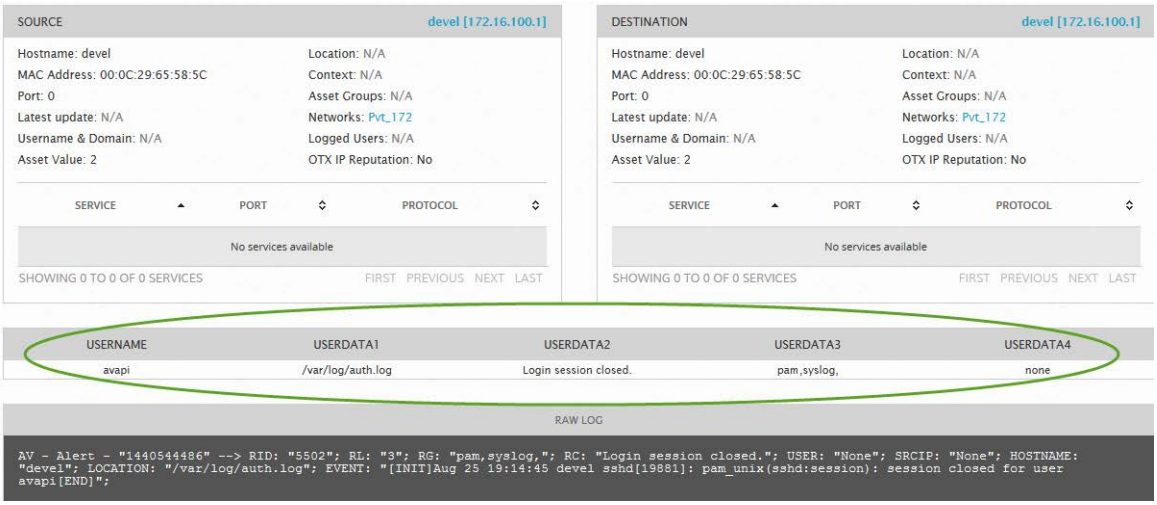

Figure 12. Event Details for an event derived from a log.

Viewing More OTX Indicator Details

OTX Details provides a bird's eye view of indicators associated with an IP Reputation or an OTX pulse event.

To get more OTX details about an indicator

- In **Event Details**, click the number in *blue* under OTX Indicators (shown in **Figure 10**).

Or

- In the **SIEM Events** list, click the orange or blue OTX icon.

In either case, the OTX Details popup for either an IP Reputation or an OTX pulse indicator appears.

OTX Details—IP Reputation

OTX Details—*IP Reputation* displays the indicator information shown in Figure 13 and described in Table 6. It also provides a link for you to go to OTX to research this indicator.

Figure 13. Sample OTX Details for an IP Reputation indicator.

Table 6. OTX Details—IP Reputation fields.

Field Name	Description
Type	Tells you whether the indicator is the source or the destination of the event.
Indicator	IP address or hostname of the event source.
Activity	Type of malicious activity identified by IP Reputation, for example, a scanning host.
Reliability	IP Reputation reliability ranking. (See **IP Reliability**.)
Priority	IP Reputation priority ranking. (See **IP Priority**.)
More Information magnifying glass icon	Clicking the **More Information** magnifying glass takes you to OTX to learn more about the indicator.

OTX Details—OTX Pulse

OTX Details—*OTX Pulse* displays the indicator information shown in **Figure 14** and described in Table 7 associated with a pulse. It also provides a link for you to go to OTX to research this indicator.

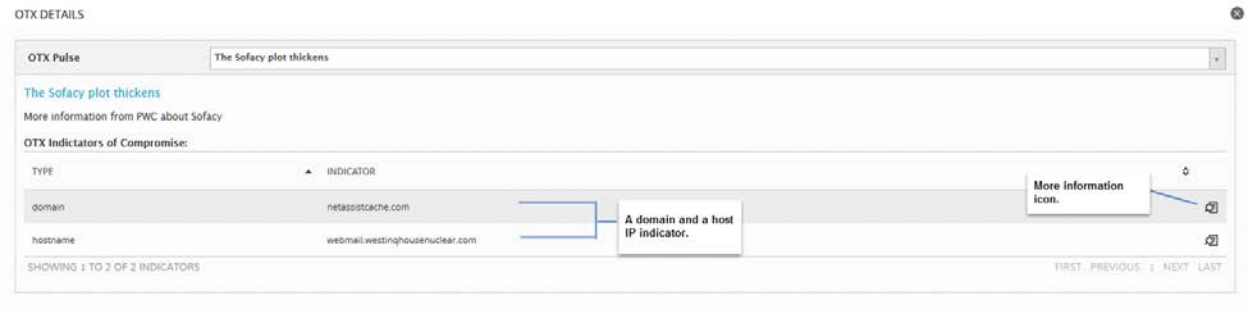

Figure 14. Sample OTX Details for a pulse.

Table 7. OTX Details—OTX Pulse fields.

Field Name	Description
OTX Pulse Name	Name of the pulse associated with the indicator.
Type	Type of indicator, for example, IPv4 or CVE
Indicator	Signature of the specific indicator, for example, if an IPv4, its IP address; if for a CVE, its CVE ID.
More Information magnifying glass icon	Clicking the **More Information** magnifying glass takes you to OTX to learn more about the indicator.

About the Real-Time View

The Real-Time view of the Security Events (SIEM) page offers you an up-to-the-minute snapshot of all events occurring within your system.

This view may or may not contain any OTX data, depending on what events are currently transpiring in your system.

Events List—Real-Time View

Real-Time view shows you the events occurring in your system right now.

OTX events only appear in the Real-Time view if an OTX event *currently* is in progress.

This view consists of both an events list and a number of filters, displayed under the Events list, which you can apply to make your search more focused.

Events List

Similar to the Events list in SIEM view, the Events list in Real-Time view displays many of the same categories of information, but with some differences, as well as unique information (**Table 8**).

Table 8. Events List—Real-Time View information categories.

Column Name	Description
Date	Local date and time of event detection; no GMT displayed.
Event Name	Event name, as described in the SIEM view Events list.
Risk	Risk level, as described for the SIEM view Events list.
Generator	Data source that generated the event, for example, a directive alert. ID associated with the external application or device that produced the event.
Sensor	USM Sensor that processed the event.
OTX	• **Orange—**Event was generated by one of the following: o A pulse o Both IP Reputation and OTX pulse indicators. • **Blue—**Event contains IP Reputation data about one more of the IP address involved.
Source IP	Hostname or IP address of the source host, with national flag if country is known.
Dest IP	Hostname or IP address of the destination host, with national flag, if country is known.

Filters

Filters correspond to the hosts displayed.

To expand a filter list

- Left-click or start typing inside of the field to display its options (Figure 15).

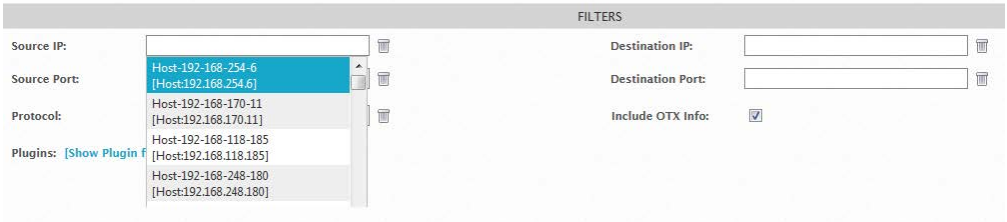

Figure 15. Expanded Real-Time view filter list.

If you already know the individual filter

- Type the filter identifier into the field.

  The display jumps to that entry in the list.

- If USM *finds* real-time events for the filter you select, they display in the Events list.
- If USM *does not find* real-time events for that filter, the Events list appears empty.

Analyzing OTX Alarms in USM

USM generates an OTX alarm whenever it detects an event it associates with an individual OTX pulse. Alarm correlation begins then and proceeds for a period of 24 hours.

During this time, USM adds any new events related to that pulse to the same alarm. The more events generated by a single pulse within that timeframe, the higher the alarm severity.

If new events related to the pulse occur after that 24-hour correlation period, they generate a second alarm and a new correlation period begins.

In the case of events with data on record with IP Reputation, USM correlates alarms, using its standard directive taxonomy.

About the List View

Only the List View of the Alarms page contains OTX data at this time. The List View consists of the following sections:

- **Search and Filter—**Alarm filtering criteria that allows you to quickly find data on an alarm you receive through OTX.
- **Alarm Graph—**Graphical display of the number of alarms generated relative to other dates.
- **Alarms List—**Lists all of the alarms matching any filtering criteria you selected.

Search and Filter

You can filter on a specific pulse or on all OTX pulses that generated alarms (**Figure 16**).

- **OTX Pulse—**Search for an alarm generated by a specific OTX pulse, if you know its name.
- **Only OTX Pulse Activity—**Selects only alarms generated by OTX pulses.

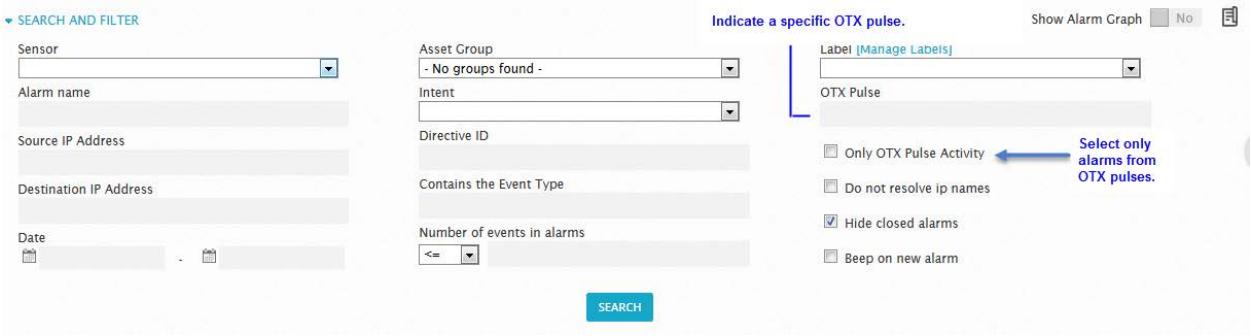

Figure 16. OTX alarm filters.

At this time, the Alarms page does not offer an IP Reputation-related filter. However, you can review any IP Reputation-related alarms, along with pulse-related alarms, within the Alarms list.

Alarm Graph

Alarms in the graph appear categorized by *intent,* which is based on the Cyber Kill Chain model of an attack, familiar to many security analysts.[1]

Blue bubbles of varying size indicate the relative number of alarms generated among your assets on each day within a 31-day period (**Figure 17**).

When you click on one of the bubbles in the graph, it filters the Alarms list for those events.

Figure 17. Number of alarms generated by day.

To show or hide the Alarms graph

- In the **Show Alarm Graph** box, located in the top-right corner of the page, click **Yes** or **No** to toggle the setting.

> **Note:** The setting you select remains active even after you restart your computer until you change it back.

Alarms List

OTX alarms are immediately identifiable within the OTX column of the Alarms list and are color-coded to indicate their OTX source—blue for IP Reputation and orange for OTX pulse-related alarms.

Depending on whether an alarm was generated by events with IP Reputation data or OTX pulse events, the information in the Alarms list varies slightly. For descriptions of OTX data in the Alarms list, see Table 9.

[1]A cyber kill chain is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it. Each stage demonstrates a specific goal along the attacker's path.

Alarms List—OTX Pulse View

Figure 18 shows what the list looks like when an indicator of compromise from an OTX pulse generated an alarm.

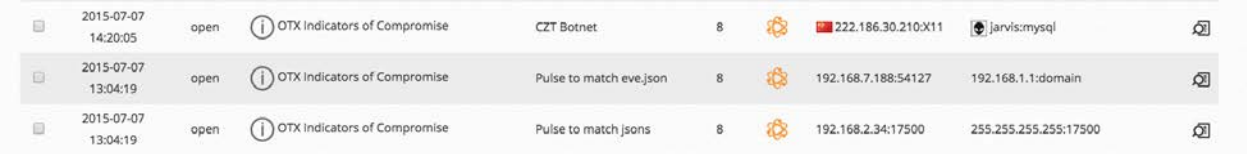

Figure 18. OTX Pulse-related alarms in the Alarms list.

Alarms List—IP Reputation View

Figure 19 shows what the list looks like if the source or destination IP addresses in one of the events responsible for an alarm were identified by IP Reputation as suspicious.

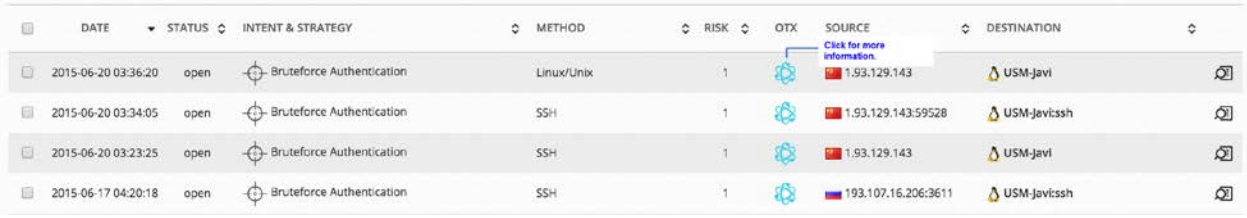

Figure 19. OTX IP Reputation-related alarms in the Alarms list.

Table 9. OTX-related Alarms list information.

Column Name	Description
Date	Date and time USM completed alarm correlation.
Status	Whether or not the alarm is open and still correlating, or closed.
Intent & Strategy	Describes the attack pattern of indicators intruding on your system. Intent and strategy are based on the taxonomy, or classification, of a USM directive. For example, a directive of AV Malware might have an “intent” of *system compromise,* with a strategy of *suspicious behavior.* When alarms come from OTX pulses, the Intent is always *Environmental Awareness* and the Strategy is *OTX Indicators of Compromise*. **Note:** Due to the size of the field label, only the strategy is visible from the Alarms list. However, when you click the row, thereby expanding the Alarms tray (Figure 19), the strategy becomes visible. The taxonomy for alarms with IP reputation data is based on the directive that generated the alarm.

Column Name	Description
	For more information, see the *Correlation Reference Guide* and *Customizing Correlation Directives and Cross-Correlation Rules* on the AlienVault Documentation Center (`https://www.alienvault.com/documentation/usm`).
Method	If known, the method of attack or infiltration associated with the indicator that generated the alarm. For OTX pulses, the method is the pulse name.
Risk	Risk level, based on asset value × event priority × event reliability ÷ 25. For more information about risk assessment, see the *Asset Management Guide* (`https://www.alienvault.com/documentation/usm`).

OTX	OTX icon present when events causing the alarm contained IP Reputation-related data or were from IOCs related to an OTX pulse.
	• **Orange—**Alarm was generated by one of the following:
	  o A pulse
	  o Both IP Reputation and OTX pulse indicators. In this case, the pulse name displays.
	• **Blue—**Alarm contains IP Reputation data about one more of the IP address involved.
	• **N/A—**If no OTX data available.

Source	Hostname or IP address of the source, with national flag if country is known, for an event creating the alarm.
Destination	Hostname or IP address of the destination, with national flag if country is known, that received the events generating the alarm.

Viewing More Alarm Details

Alarm Details provides you with more detail on the indicator of compromise that led to the alarm.

To view Alarm Details

1. In the Alarms list, click anywhere within the row for the alarm, with the exception of the OTX icon.

   This launches the **Alarms** tray initially (Figure 20).

   The Alarms tray provides a statistical overview of an event indicator of compromise that led to an alarm. Table 10 describes the Alarms tray data fields.

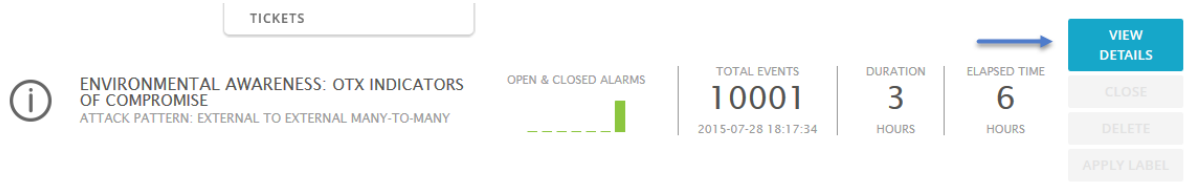

Figure 20. Alarms tray, with View Details button.

2. To access the **Alarm Details** page, click **View Details.**

Table 10. Alarms tray field descriptions.

Field Name	Description
Environmental Awareness: OTX Indicators of Compromise	See definition in **Table 10**.
Open & Closed Alarms	When you hover over the column heading, you see the date the alarms finished correlation; the number of open, correlating alarms; and the number of closed alarms. When green, the alarm is open and still correlating.
Total Events	Number of events associated with an alarm.
Duration	Duration between the first event and the most recent event represented in this alarm.
Elapsed Time	Time since the first alarm was generated.

When you access Alarm Details (**Figure 21**), you receive more in-depth information about an alarm (Table 11).

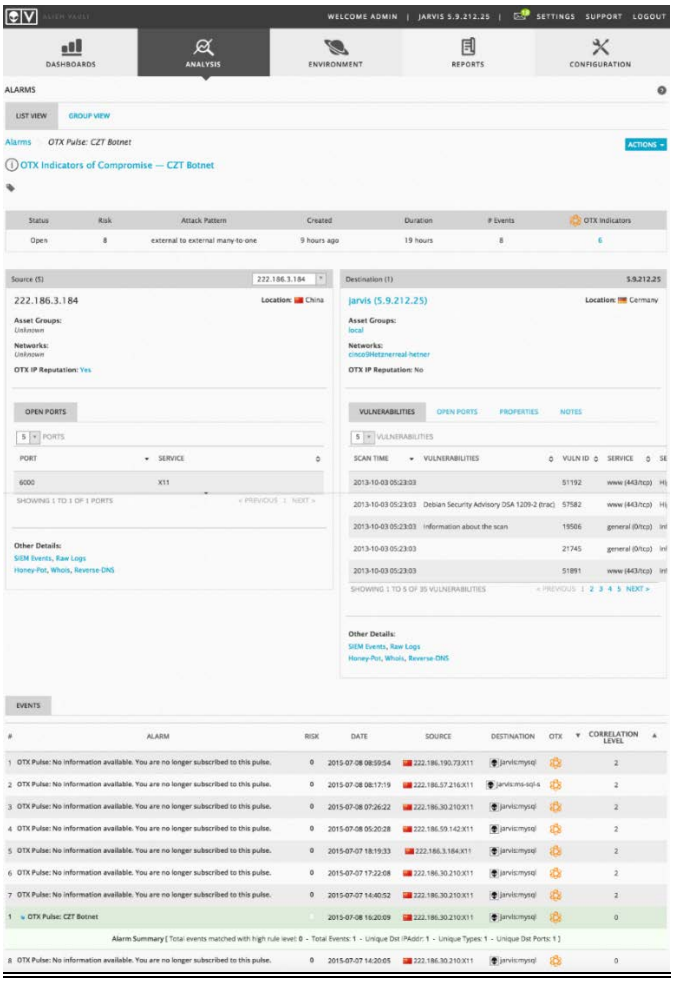

Figure 21. Sample Alarm Details associated with a pulse.

Table 11. Alarm Details information.

Column/Field Name	Description
Status	Whether or not the alarm is open or was closed.
Risk	Risk level, based on asset value × event priority × event reliability ÷ 25. For more information about risk assessment, see the *Asset Management Guide* (`https://www.alienvault.com/documentation/usm`).
Attack Pattern	Analyzed method of infiltration or attack. Shows how the attack took place, for example, external to internal, one to many, external to external, or many to many.
Created	Date alarm was correlated

Column/Field Name	Description
Duration	Duration between the first event and the most recent event creating the alarm.
# Events	Number of events associated with the alarm.
OTX Indicators	Number of OTX pulse indicators, shown in blue, generating the alarm.
Source/Destination	Hostname or IP address of the host. The number in parentheses next to the label stands for the number of IPs or hosts involved with the events associated with this alarm (*5* in Figure 20).
• Location	If the country of origin is known, displays the national flag of the event responsible for the alarm.
• Asset Groups	When the source/destination belongs to your asset inventory, displays any asset groups to which that asset belongs. • When the source/destination is an *external host,* Assets Groups displays *Unknown.* • When the source/destination is a host *within one of your asset groups,* these sections contain a value. You can click it to go to the **Asset Details** page for more information.
• Networks	When the source/destination belongs to your asset inventory, displays any networks to which that asset belongs. • When the source/destination originates from a host in an external network, Networks displays *Unknown.* • When the source/destination of the alarm events comes from one of your networks, the field contains a value. You can click it to the **Network Group Details** page for more information.
• OTX IP Reputation	(Yes/No) If “Yes,” the IP or hostname is known to IP Reputation and it may be malicious. It is, at minimum, suspicious. **Note:** When you click **Yes,** a popup displays, providing more information about the IP address. A hypertext link to the details about that IOC in OTX also appears, allowing you to better assess the threat.
Open Ports	Any open ports discovered by USM. • If the source/destination is an asset in your inventory, displays all open ports detected. • If the source/destination is an external host, displays any open ports detected, based on USM communication with that host.
• Ports	You can select the number of ports you want to display in increments of 5, 10, and 20.

Column/Field Name	Description
• Port	Associated port number.
• Service	Name of the service using the port, if applicable.
Vulnerabilities, Properties, Notes	These tabs appear only if the source/destination is an asset belonging to your asset inventory.
• Vulnerabilities	Includes the service/port and severity of the vulnerability.
• Properties	Lists all asset properties defined in the Asset Details.
• Notes	User-entered comments about the asset and/or alarm.
Other Details	Clicking **SIEM Events** and **Raw Logs** takes you to those respective pages, where are filtered by the source/destination IP address. These pages provide information about other events or logs that reference the IP address related to the alarm. Other links go to external security resources, such as Honey-Pot, Whois, or Reverse-DNS, where you may find out more about the particular IP. For information on these, see the *Open Threat Exchange (OTX) User Guide* or visit their respective websites.
Events	Lists the events that generated the alarm. **Note:** In general, whether events generate an alarm depends solely on the directive taxonomy in USM. However, IOC events from OTX pulses automatically generate an alarm.
• Alarm, Risk, Date, Source, Destination, OTX	For definitions, see above.
• Correlation Level	Correlation level assigned, based on a rules hierarchy USM employs, with each rule assigned a priority and a reliability value. For details, see the *AlienVault Correlation Reference Guide* (`https://www.alienvault.com/documentation/usm`).

Viewing OTX Details

OTX Details provides a bird's eye view of the indicators associated with a pulse or an IP associated with an event in your environment. You can also use it to quickly link to OTX to find out all of the information known about the indicators and about this and any other pulses associated with them.

To see OTX details

1. From the **Alarms** list, click the OTX icon itself in the row of the alarm you want to research.

An OTX Details popup appears that gives you a high-level overview of the involved pulse and its indicators, as well as any pulse data (Figure 22) or IP Reputation data (Figure 23).

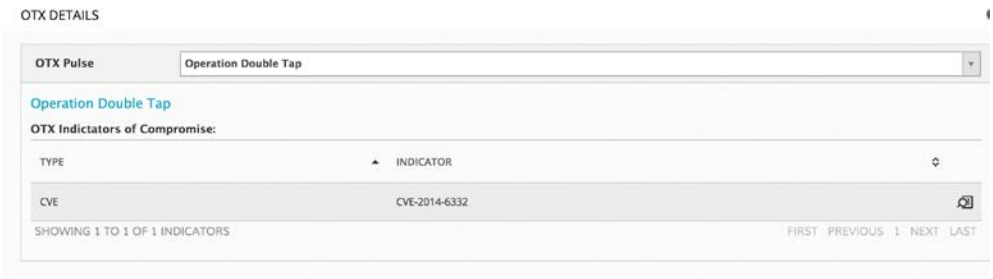

Figure 22. OTX Details—OTX Pulse.

OTX Details—OTX Pulse references the name of the pulse, as well as the type of indicator.

OTX Details—OTX IP Reputation does not generate an alarm, unlike pulses. This popup provides data from IP Reputation on any source or destination IP or hostname referenced in the alarm.

It also displays the type of activity that hostname or IP address is engaged in; and includes the IP Reputation reliability and priority ranking.

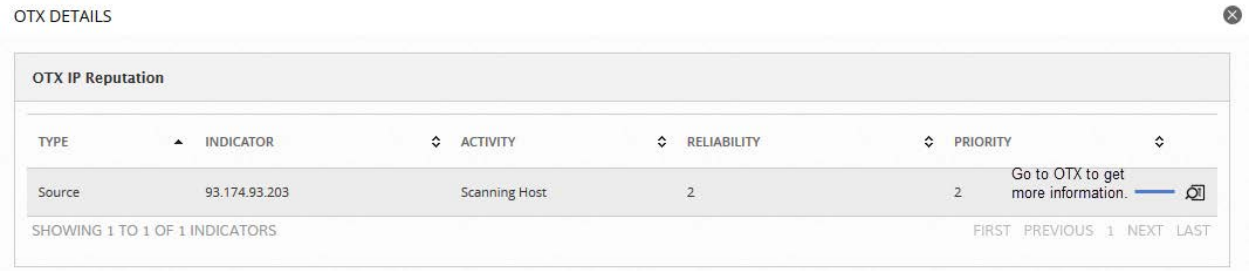

Figure 23. OTX Details—OTX IP Reputation.

2. To get more information about either a pulse or an IP Reputation indicator in OTX, click the **More Information** magnifying glass on the far-right of its row.

Reviewing Your OTX Account and Pulse Activity

You can review your OTX account information and also an activity feed of all of the pulses you subscribe to in OTX in concise format from the OTX Configuration page (Configuration > **Open Threat Exchange)**.

Reviewing Account Information

The Account Information section of the OTX Configuration page summarizes your USM-OTX account status (Figure 24).

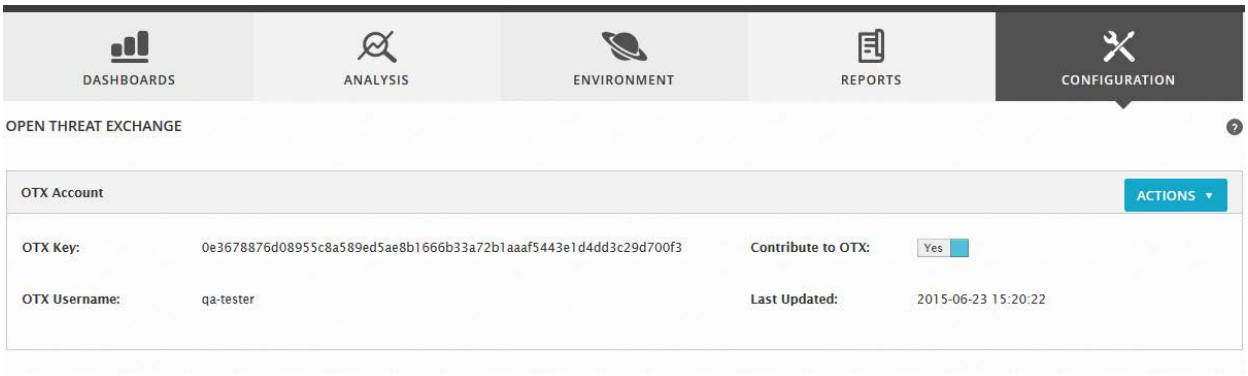

Figure 24. Reviewing OTX account information on the Open Threat Exchange Configuration page in USM.

Table 12 lists fields and their definitions on the OTX Account section of Open Threat Exchange Configuration.

Table 12. OTX account Information section--OTX Configuration page.

Field Name	Description	Actions You Can Take
OTX Key	Your OTX key.	
Contribute to OTX	Lets you indicate whether or not you want to anonymously contribute data to IP Reputation.	Default is Yes. **To change the status** • Click **Yes** to toggle it to **No.**
OTX Username	Your OTX username, for example: `dbrown@mycompany.com.`	N/A
Last Updated	The last time OTX subscription information was updated.	N/A
Actions	List of actions you can take regarding your account:	N/A
	• Edit OTX key	Makes the OTX Key field editable, so that you can register a new OTX key in USM. **To update** • Click **Connect OTX Account**.
	• Remove OTX Key	Disconnects USM from OTX. If you select **Remove OTX Key**, USM prompts you: `Are you sure you want to disconnect your OTX account?`

Field Name	Description	Actions You Can Take
		No/Yes When you click **Yes,** USM removes your account data and the list of subscribed pulses.
	• View Account Details	Launches the OTX login page if you are not already logged in. If already logged into OTX, it takes you to your **OTX Profile** page.

Reviewing OTX Pulse Subscriptions in USM

The **Pulse Subscriptions** section of the Open Threat Exchange Configuration page displays all of the pulses you subscribe to in OTX in concise form (Figure 25).

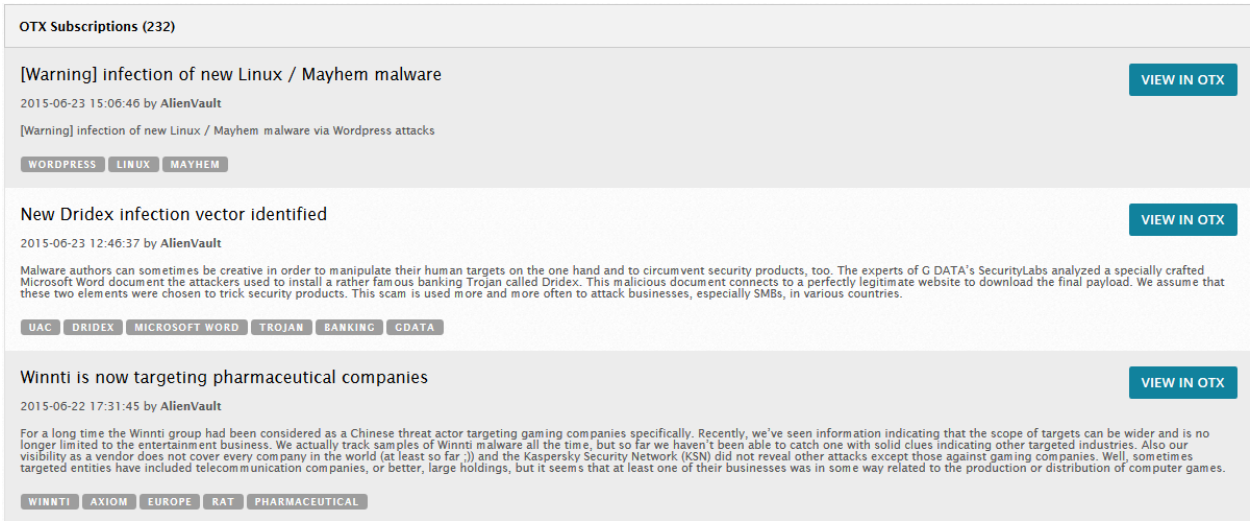

Figure 25. Pulse activity in the Open Threat Exchange Configuration page.

Pulse subscription information viewed in USM includes the details shown in Table 13.

Table 13. Pulse subscription information.

Field	Description
OTX Subscriptions (*number*)	Number of pulses to which you subscribe.
Name of pulse	Example: Dyre Botnet Using Malicious Microsoft Word Macros
Pulse creation or update date and time.	Format: yyyy-mm-dd and hh:mm:ss
Pulse submitter	Username of the individual who contributed the pulse.

Field	Description
Description of the pulse.	Concisely describes the pulse in terms of its IOCs, how discovered, who is responsible, and other material information.
Tags	OTX sometimes creates these tags based on its analysis of IOCs for the pulse. For information about IOCs, see **About OTX Pulses and Indicators of Compromise**. Examples: FIREYE, BLACKCOFFEE, POS, FTP **Note:** You can click on tags to find out about other pulses with the same threat vectors.

To get more detail about a pulse on the Open Threat Exchange Configuration page

- Click **View in OTX.**

  This takes you to the Pulse Detail page in the OTX platform, where you can browse details about pulse and associated IOCs.

Or

- Click on the pulse itself.

  This expands the pulse information to display a list of all associated IOCs.

For details about pulses and their IOCs, see the *Open Threat Exchange* (*OTX) User Guide* on the AlienVault Documentation Center (`https://www.alienvault.com/documentation/usm`).

Getting Information About the Top OTX Pulses

As soon as you log into USM, you see a snapshot of the most active OTX pulses within your system environment, in other words, those pulses whose indicators are presently interacting with your assets the most.

These pulses appear in graph format within the **Top OTX Activity in Your Environment** pod of the **Dashboard Overview** (Figure 26) under Dashboards > **Overview.**

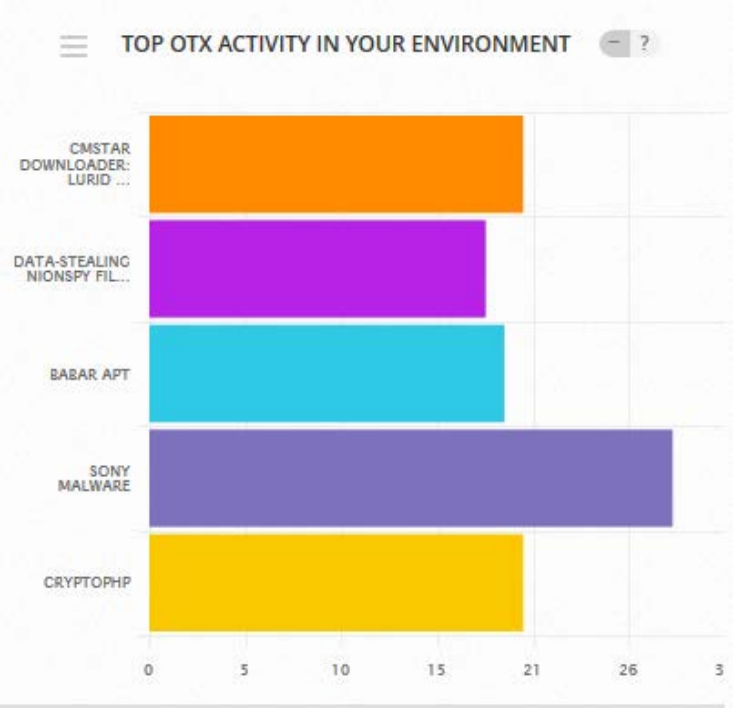

Figure 26. Most active pulses in your environment in bar graph format from USM Dashboard Overview.

Details from the Top OTX Activity in Your Environment pod consist of the following:

- Name of each of the most active OTX pulses in your environment.
- Relative activity level compared to the other top OTX pulses, expressed by number of events at the bottom of the graph.

To get more information about any of these pulses

1. Hover over the one of the pulse bars to see how many indicators USM detected for this pulse.
2. Click the bar of any pulse within the graph (**Figure 26**) to go to the **Security Events (SIEM)** page, where you can review recent events in your environment associated with this pulse.

To understand the SIEM Events page as it relates to OTX, see **Analyzing OTX Security Events in USM**.

Reviewing OTX Dashboard Information in USM

You can get more details about your pulse subscriptions and related alarms and events through the Open Threat Exchange Dashboard in USM (Dashboards > **Open Threat Exchange**).

Open Threat Exchange Statistics

The top-most section of the OTX Dashboard page offers a statistical overview of data related to your pulse subscriptions (Table 14)

Table 14.Top-level OTX dashboard statistics.

Column Name	Description
Pulses Subscribed	Total number of pulses to which you subscribe.
Indicators	Total number of indicators of compromise active in your environment that are associated with those pulses.
Last Updated	Last time USM received OTX data on your subscribed pulses.
Number of Alarms	Total number of alarms generated, based on your OTX pulse subscriptions.
Number of Events	Total number of events generated, based on your OTX pulse subscriptions.

- When you click **Pulses Subscribed, Indicators,** or **Last Updated,** it takes you to the **OTX Configuration** page in USM.
- When you click **Number of Alarms,** it takes you to the **USM Alarms** page. The Alarms page displays all of the OTX pulse-related alarms generated.
- When you click on **Number of Events,** it takes you to the USM **Security Events (SIEM)** page. This displays all of the OTX pulse-related events generated.

Events from Most Active OTX Pulses

This graph provides yet another view of the events generated in your environment from the most active pulses over the last seven days.

The blue “bubbles” indicate the number of events that occurred on a specific date, relative to others—the larger the bubble, the more events generated by a specific pulse.

To get more event detail for a specific date

- Hover over the bubble to see the date and the number of pulse-related events then.
- Click one of the bubbles to see more detail about the events for that day in the **Security Events (SIEM)** page. Details include the date range and the OTX pulse name.

For details about **Security Events (SIEM)**, see **Analyzing OTX Security Events in USM**.

Events from All OTX Pulses

This graph provides a seven-day overview of all events related to your OTX pulse subscription.

To see event details

- Click on any point directly above a date in the event curve.

  This takes you to **Security Events (SIEM)** page, where you can see details about those specific events.

  For details about this page, see **Analyzing OTX Security Events in USM**.

IP Reputation Dashboard

The bottom third of the Open Threat Exchange dashboard provides information from IP Reputation.

Note: Detailed IP Reputation-related events and alarms information appears on the Security Events and Alarms pages, respectively.

About the IP Reputation Map

The IP Reputation map has two views—**SIEM Events** and **Reputation Data**.

SIEM Events view (**Figure 27**) shows you the IPs that have *actually* interacted with your USM assets.

Reputation Data view provides a visual summary of all of the IP addresses in the IP Reputation database—whether or not they have interacted with your assets.

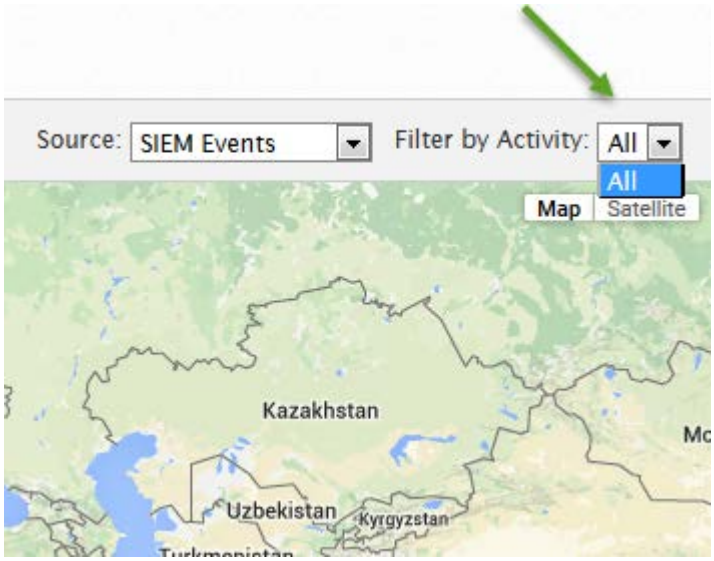

Figure 27. Filtering by All activity in IP Reputation map.

About the SIEM Events View

By default, the icons on the map show any IP addresses worldwide that have interacted with your USM assets as **SIEM events**.

- Inverted red teardrops on the map signify malicious hosts.
- Blue, concentric circles indicate the number of IPs that interacted with your assets, regardless of the threat level.

To get details on an IP interacting with your assets

- Click one of the red teardrop icons within the map.

  This launches an instance of the OTX website and displays the OTX **Indicator Details** page for that specific IOC.

  For details about the OTX Indicator Details page, see the *Open Threat Exchange (OTX) User Guide,* available on the AlienVault Documentation Center (`https://www.alienvault.com/documentation/usm`).
- Click one of the blue icons within the map to zoom into a location where multiple IOCs, represented by red teardrops, are active.

SIEM events relate to all activity types (malware domains, scanning hosts, malicious hosts, and malware IPs).

To get events for a particular IP activity type

- Expand the **Filter by Activity** list by clicking it. Default is All.

To expand the view of IP addresses that interacted with your assets

- Click the minus sign (-) on the expansion bar at left.

  This expands the view, so you can see IP addresses worldwide.

To contract the view of IP addresses that interacted with your assets

- Click the plus sign (+) on the expansion bar at left.

  This reduces the focus to show you more local event sources.

About the Reputation Data View

The Reputation Data map displays color-coded concentric circles on the points of malicious IP origin. These also display numbers that correspond to the number of active IPs and colors that represent the type of malicious activity, as illustrated in a key under **Malicious IPs by Activity,** below the map.

A colored pie chart accompanying the key shows you the relative numbers of any particular malicious IP activity worldwide, including totals. These activities consist of the following:

- Scanning Hosts
- Malicious Hosts
- Spamming
- C&C (command-and-control server)

- Malware Domain
- Malware distributions
- Malware IP

General Statistics

Reports how many IPs reside in the IP Reputation database and the date the database was last updated.

Top 10 Countries

Displays the flags of the top 10 countries from which malicious IP activity originates, with the countries with most malicious IPs appearing at the top.

The list also includes the number of unique IP addresses included in the data for each country.