ALIEN VAULT

The Value of Crowd-Sourced Threat Intelligence

Shared Intelligence for Collaborative Defense

For years, the systems and networks that run our businesses have been secured by the efforts of IT and security practitioners acting on their own. We continue to deploy the latest countermeasures, always trying to keep up with adversaries. Criminal attackers, on the other hand, have shared information quite successfully to facilitate their exploits. Couple this with the 'attacker's advantage" of choosing where, when and how to launch attacks, and it is no surprise that collaborative hackers appear to be winning against even the largest companies, despite their generous spending on security tools.

Collaboration between reputable companies on the latest exploit methods has been patchy at best. Fear of exposure or liability has kept most organizations silent about the efforts they have taken to secure their systems, or any incidents they may have experienced. Occasionally, information is shared at a conference or in an article, but typically at a very high level. There are some invitation-only information sharing and analysis networks, such as FS-ISAC, Infragard and ISAC, but they are useful only to the 'security elite", not the millions of other IT practitioners on the front lines trying to secure their organizations. As a result, there is little opportunity for security practitioners to share what they have learned in any detail.

The secrecy that has blanketed the security industry has not worked out well. Time and again attackers are able to use the same exact methods to breach different organizations, largely because we are not learning from each other and from our collective failures fast enough. Our inability to share information about how we are being attacked, and who is launching those attacks, leaves us at a disadvantage.

The US government has not met with much success in providing non-government organizations access to threat data that it has collected. Ideally, the government could provide a wealth of information about known malicious actors and the methods they use. This data could provide an edge for those trying to defend their systems. Knowing that a particular actor is known to be malicious allows for far more valuable judgments to be made when suspicious behavior is observed. This type of collaboration would deprive attackers of their critical advantage of anonymity. The NSA is unlikely to provide a government-sponsored program in the foreseeable future – even if it did, trust in such a program would be difficult, given recent publicity around its controversial practices.

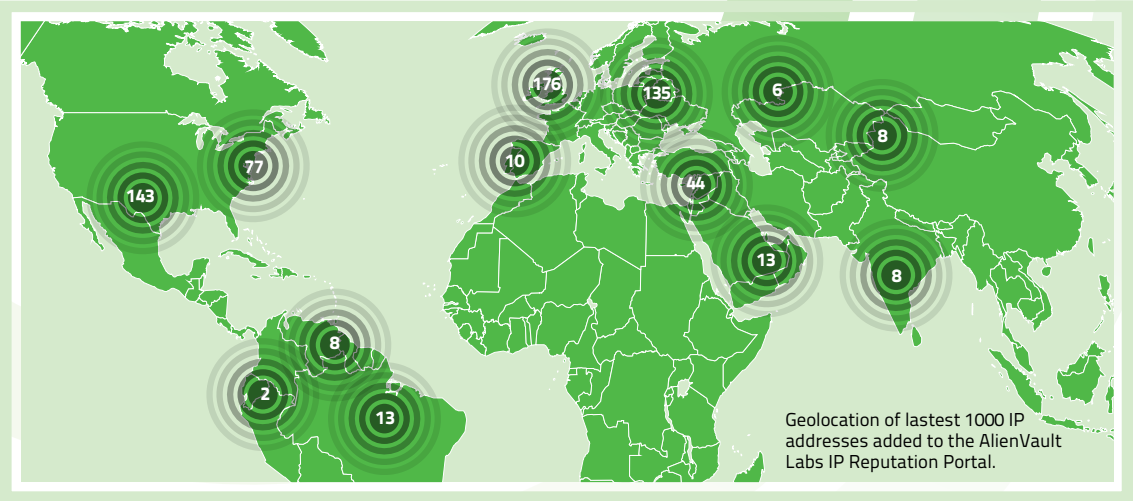
Without an effective way for organizations of all types and sizes to share threat data, attackers can refine their methods on one organization before moving on to target similar organizations. They use the isolation of organizations to their advantage, knowing that the fingerprints left on the infrastructure of one will not be used to identify the attack on another. Ultimately, this isolation has led to the mass commercialization of exploits within criminal communities. Knowing that a successful exploit in one organization will not substantially reduce the chance of success in another, means that there is a high commercial value for an exploit that can be targeted at a large number of organizations. Sharing threat intelligence is the first step to changing the dynamics of this situation.

Crowd-Sourced Threat Intelligence: AlienVault Open Threat Exchange™ (OTX)

With the government's ineffectiveness in providing a collaborative defense infrastructure, private sector initiatives are the best alternative. As an industry, we need a threat-sharing solution that is open and available to everyone for the mutual benefit of all who contribute. With this goal in mind, AlienVault created the Open Threat Exchange™ (OTX). OTX is an open information sharing and analysis network that provides real-time, actionable threat information submitted by over 8,000 contributors in more than 140 countries. Threat intelligence from OTX is built into the Open Source Security Information Management (OSSIM) project as well as commercial products such as AlienVault Unified Security Management™ (USM). OTX allows for anonymous sharing of threat intelligence for mutual benefit.

OTX Stats at a Glance:

- 200,000-350,000 validated malicious IPs at any point
- 8,000 collection points
- 140 Countries



Users can opt-in to share anonymous threat data with the OTX community. When users choose to contribute, information related to attacks observed on their systems is sent to OTX. This data is then validated by the AlienVault Labs research team and distributed to all other participants in the OTX network, but without any details that would identify the specific contributor. So, an attack on any system in the network can now be used as an indicator for subsequent attacks on any other participant in the network. By participating in OTX, **defenders can learn from each other and quickly adapt to new threats**. With collaborative threat intelligence, an attack on one organization greatly reduces the chance of success in subsequent organizations.

OTX IP Details Summary:

An example of the IP Reputation data available via OTX

The Importance of Data Diversity in Threat Intelligence

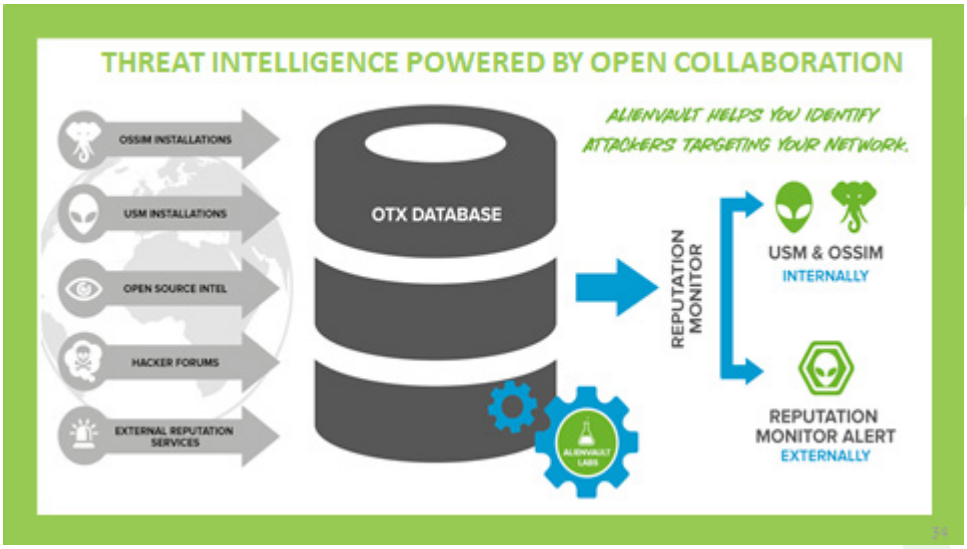
Users can contribute threat data to the AlienVault Open Threat Exchange via OSSIM, the most widely used SIEM offering in the world, as well as commercial products such as AlienVault USM. A SIEM, by design, gathers data from a very diverse set of devices. Any device that produces information about its own operation can be incorporated into a SIEM. The SIEM then analyzes this data to identify probing attempts, attacks, and breaches.

Gathering threat data from a SIEM means that the data gathered is not limited to the types of attacks that a single type of security control can detect. For example, if one were to build a threat intelligence system gathering data from firewalls only, attacks that can be detected at the network level would feed the system. Using a SIEM as the platform for gathering the threat intelligence allows information from any type of attack to feed into the system.

In addition to the diversity of the devices that the OTX threat intelligence is gathered from, the diversity of the organizations contributing also plays a major role. A diverse set of contributors means that the attackers cannot use geography, size of company, or industry as a means for isolation. If threat intelligence is gathered only from attacks targeting US based companies, or only from attacks targeting financial service companies, the system can easily be gamed. Attackers could simply use a different country or industry to refine their attack before moving on. OTX collects threat data from over 8,000 collection points in over 140 countries, so users can benefit from contributions made by organizations of all different sizes, from all over the world, and in all different types of industries.

Users of AlienVault OSSIM and USM can voluntarily contribute IP reputation information from a broad range of devices in their environment (firewalls, proxies, web servers, anti-virus systems, and intrusion detection/prevention systems). This raw data is automatically cleansed, aggregated, validated, and published via OTX.

How OTX Works



What's next for OTX and the Security Community?

Failing to collaborate on the changing threat landscape will allow attackers to retain the advantages they have been leveraging for years: fear and isolation. Simply having a forum for an open dialog on threat intelligence isn't enough; the mechanism for sharing threat intelligence needs to be automated and it needs to be real-time. Trying to secure a system without the benefit of learning from others will mean that our adversaries will always be able to isolate us to their advantage.

The Open Threat Exchange provides a substantial step toward collaboration in the security community. OTX is an open program allowing any contributor to benefit from the lessons of the community. Such an open program allows for better threat intelligence due to its diverse community of contributors and the diverse set of devices that can be used to detect attacks. The Open Threat Exchange is an asset of the community that contributes to it. It is time to embrace collaboration, and work together to secure the future of reputable organizations such as yours.

Join OTX

Join OTX now to benefit from the world's largest collaborative threat intelligence system, connect with peers, get free tools and learn about the latest threats and defensive tactics. You can contribute to OTX by using OSSIM, the world's most widely used SIEM product, or the commercially available AlienVault Unified Security Management (USM). Both products include SIEM, plus fully integrated capabilities for asset discovery, vulnerability assessment, threat detection (IDS) and behavioral monitoring.

You can also take advantage of these free tools powered by OTX:

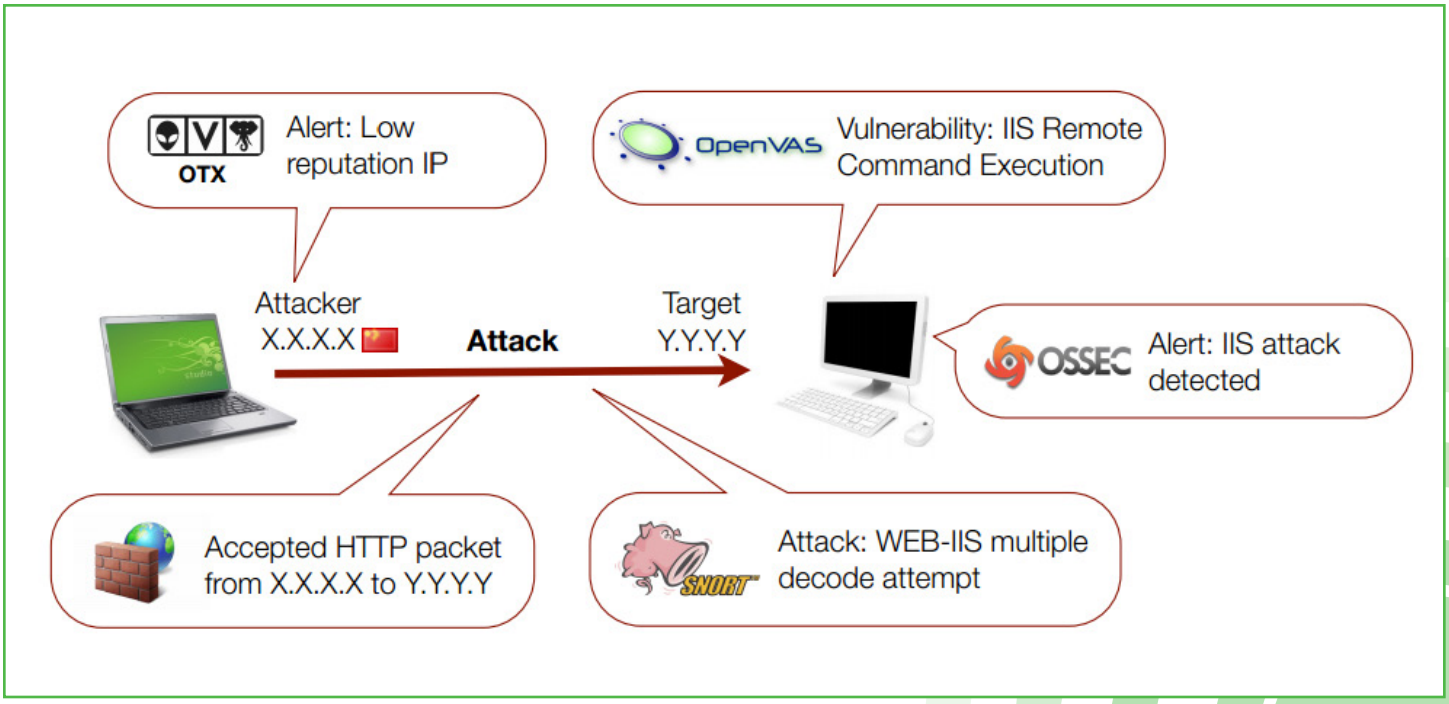
- OTX Reputation Monitor Alert℠ is a free service to monitor the reputation of your own external IP assets. Once subscribed, you will be alerted anytime one of your IP addresses of domains is listed in a hacker forum, a blacklist or matches one of the known malicious IPs in OTX. OTX Reputation Monitor also monitors DNS registration and SSL certificates to make sure there aren't any changes you don't know about.
- The OTX Dashboard is an interactive tool that shows you the top malicious IPs and domains world-wide and provides the ability to investigate any IP address to see if malicious activity has been reported. You can also download a detailed report covering details on the type of attacks observed, methods deployed, associated domains, and more.

Take Threat Detection Further with USM

Fueled by the collective power of Open Threat Exchange, AlienVault Unified Security Management (USM) gives you a better understanding of your environment and active threats. USM helps you identify, alert and respond to your assets' interactions with malicious IPs. By correlating malicious IPs from OTX with activities on network components such as firewalls, proxies, web servers, anti-virus systems, and intrusion detection systems, USM helps you prioritize risk and focus your resources better,

For example: you are investigating a potential security incident after you see an alarm from AlienVault's built-in IDS. You check if the asset under attack has had any communications with known external malicious IPs, from the USM console (powered by OTX). You also get visibility to details about the asset under attack, including OS, software running and known vulnerabilities on the system, all from the same console. The following illustrates how the open source tools of USM work together in the case of a security incident.

With USM and OTX, you'll finally have the visibility you need to secure your network, with all the security tools you need at your fingertips.



Learn more about AlienVault USM:

- Download a free 30-day trial
- Try the Interactive Test Drive
- Join us for a Live Demo

About AlienVault

AlienVault provides organizations of all types and sizes with unprecedented visibility across the entire security 'stack' with the AlienVault Unified Security Management™ (USM™) platform. Based on OSSIM—the de facto standard open source SIEM created by AlienVault—the USM platform has five essential security capabilities built-in: asset discovery, vulnerability assessment, threat detection, behavioral monitoring and security intelligence. The AlienVault Open Threat Exchange™, a system for sharing threat intelligence among OSSIM users and AlienVault customers, ensures USM always stays ahead of threats. AlienVault is a privately held company headquartered in Silicon Valley and backed by Kleiner Perkins Caufield & Byers, Sigma, Trident Capital and Adara Venture Partners. For more information visit www.AlienVault.com or follow us on Twitter.

ALIEN VAULT

www.alienvault.com