AlienVault® Open Threat Exchange™

The world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data.

Threat sharing in the security industry remains mainly ad-hoc and informal, filled with blind spots, frustration, and pitfalls. Our vision is for companies and government agencies to gather and share relevant, timely, and accurate information about new or ongoing cyberattacks and threats as quickly as possible. Armed with this information, organizations of all sizes can avoid major breaches or minimize the damage from an attack. AlienVault's Open Threat Exchange (OTX) delivers the first truly open threat intelligence community that makes this vision a reality.

AlienVault OTX provides open access to a global community of threat researchers and security professionals. It delivers community-generated threat data, enables collaborative research, and automates the process of updating your security infrastructure with threat data from any source. OTX enables anyone in the security community to actively discuss, research, and share the latest threat data, trends, and techniques, strengthening your defenses while helping others do the same.

Pulses

Pulses are the format for the OTX community to share information about threats. Pulses provide you with a summary of the threat, a view into the software targeted, and the related indicators of compromise (IOC) that can be used to detect the threat.

IOCs include IP addresses, domain names, file hashes (MD5, SHA1, SHA256, PEHASH, etc), CVE numbers and more! Pulses and their included IOCs help answer questions like:

- Is my environment exposed to this threat?
- Is this relevant to my organization?
- Who is behind this, and what are their motives?
- What are they targeting in my environment?

Open Access

Security research tends to be an insular process and rarely do individuals or groups share threat data with one another. This is due to lack of trust, internal policies, or simply the inability to get the information out to the masses. OTX helps to solve this problem with the ability to subscribe or follow the most trusted pulses in the community.

- Subscribe to pulses and use the DirectConnect feature to automatically instrument your security products to detect the latest IOCs.
- Follow OTX contributors and get valuable insight into their recently researched threats.

Openly Research & Collaborate on Emerging Threats

The traditional threat sharing model is a one-way communication between researchers/vendors and subscribers. There is no way for subscribers to interact with peers or threat researchers on emerging threats, as each recipient is isolated from each other. That's why we built OTX — to change the way we all create, collaborate, and consume threat data.

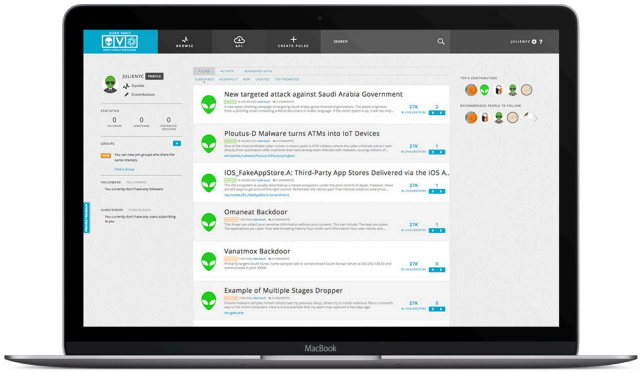
Integrate with the AlienVault USM Platform & Export IOCs to Any Security Product

Most threat data sharing products or services are expensive and/or overly complex. Users often find themselves buying multiple services since the traditional, isolated, approach to threat data limits their ability to export threat data from one tool to another. OTX provides several methods for your security tools to ingest pulse data, allowing you to react quickly and more efficiently to any threats.

Direct Integration with the AlienVault USM Platform
Automatically instrument your built-in IDS capability within the AlienVault USM platform deployments, as well as third party security tools, with the latest actionable threat data from community-generated pulses.

OTX DirectConnect API
Export IOCs automatically into your existing security tools, eliminating the need to manually add IP addresses, MD5 hashes of malware files, domain names, etc. in the following formats: OpenIoC, STIX, and CSV.

Export to Third Party Security Tools
Import IOCs from pulses into third party security tools.



CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM