AlienVault
Open Threat Exchange

Well known attack methods continue to successfully breach defenses. The adversary is doing something that company security teams are not doing—actively collaborating.

The industry's inability to share information about attack vectors gives the adversary another advantage. AlienVault's Open Threat Exchange™ (AV-OTX™) enables anonymous sharing of threat intelligence across a broad range of devices, in more than 50 countries, is free for all who choose to share, and is validated by AlienVault Labs. It makes sense that security teams should work together as they must be correct every time, while adversaries only need to be correct once. AV-OTX is an element of AlienVault's Unified Security Management (USM) platform's Security Intelligence (SIEM) module.

Open Threat Exchange is a framework for a unique and powerful collaborative defense capability adding IP Reputation-based defenses to the Unified Security Management (USM) platform. USM enables you to more easily and efficiently configure, manage, and operate the 5 essential security capabilities that no company should be without. Unifying the essential security capabilities within a single platform simplifies management and reduces complexity, allowing you to spend more time securing the network and less time learning, deploying, and configuring tools.

- **FRAMEWORK FOR SHARED INTELLIGENCE THAT ENABLES A COLLABORATIVE DEFENSE, IMPROVING SECURITY**
- **PARTICIPATION FROM MORE THAN 50 COUNTRIES, PROVIDING COMPREHENSIVE IP REPUTATION COVERAGE**
- **COLLABORATIVE DEFENSE IS FREE FOR EVERYONE**
- **ALIENVAULT LABS RENOWNED SECURITY EXPERTS ENSURE ACCURACY**

Diverse Community

AlienVault's Open Threat Exchange (AV-OTX) enables anonymous sharing of threat intelligence. It is built into OSSIM (Open Source SIEM) and AlienVault products, sharing and receiving threat updates from installations across more than 50 countries. IP Reputation information from a broad range of devices (firewalls, proxies, web servers, anti-virus systems, and intrusion detection/prevention systems) is automatically cleansed, aggregated, validated, and published. Collaborative security intelligence is spread among many industries and countries, composed of organizations of all sizes, limiting the attacker's ability to isolate targets by industry or organization size. It is the most diverse and comprehensive IP Reputation threat feed possible.

Free for Everyone

To participate, download the latest OSSIM update, and simply click to opt-into AV-OTX. The system will automatically begin contributing validated data and will automatically begin receiving and using threat intelligence from the community. Rest assured that no information related to the layout of your network or configuration of any controls or machines in your network will be shared. All data is stored anonymously.

OPEN THREAT EXCHANGE

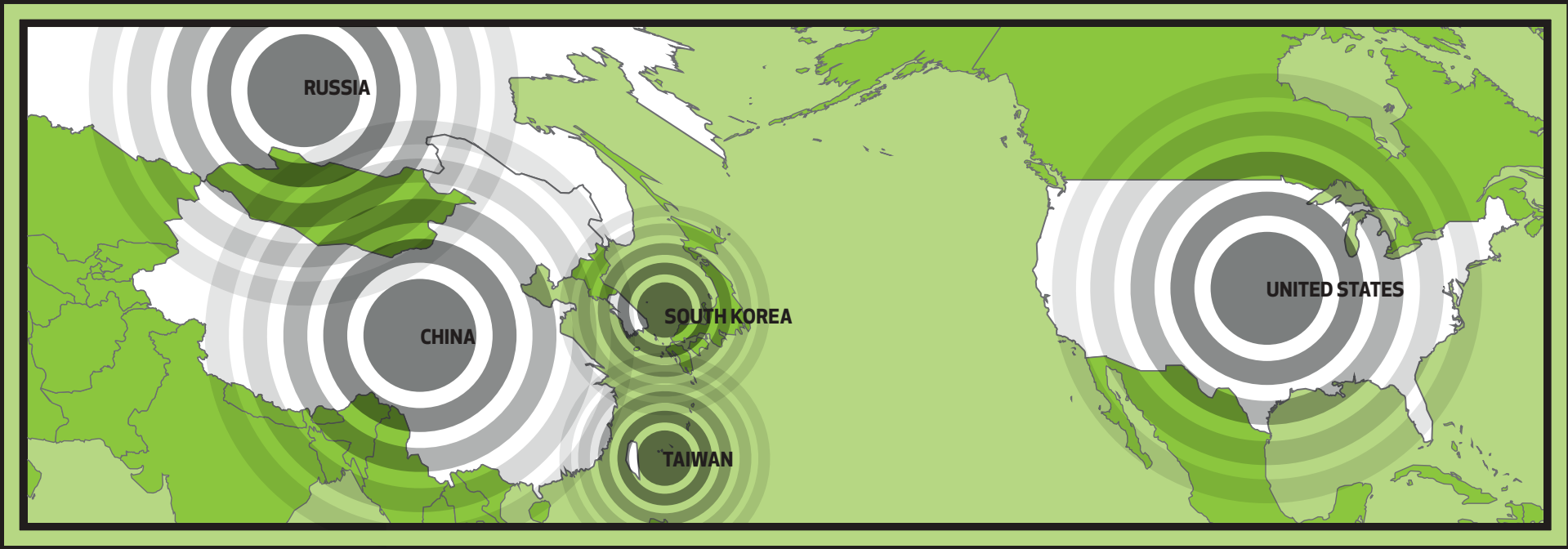
Validated by AlienVault Labs

Validated results are distributed to all AV-OTX participants and published in the IP Reputation Portal. The reputation information is used to detect further probing attempts from the same malicious actors in other installations. A validated, collaborative defense model offers AlienVault users an improved level of security over standalone alternatives.

Open Threat Exchange in Action

At another participating AV-OTX installation, a port scan is detected by the firewall. The source address of the scan is correlated with the destination address of an SSH session from an internal host. From the security investigation it is determined to be a security breach. The incident is automatically reported to the AlienVault Labs OTX so other OTX-enabled AlienVault installations are protected from connection attempts to the identified address.

The threat landscape is constantly changing. New exploits are invented every day. There are countless hackers working tirelessly to find a way into your infrastructure. Adversaries are actively collaborating on methods to breach the network and disrupt operations. AlienVault's collaborative defense model offers an improved level of security over today's standalone security solutions operating in isolation.



AlienVault
WWW.ALIENVAULT.COM