AlienVault Threat Intelligence Subscription

Delivering the Information You Need Now

The threat landscape is constantly changing with the almost daily discovery of new vulnerabilities, new attack techniques, and new strains of malware. You don't have the time or the resources to research these emerging threats or determine if your environment is at risk, or already compromised. Instead, busy IT security teams turn to the AlienVault Labs Threat Intelligence subscription to stay up to date on the latest information about malicious actors, their tools, infrastructure and methods.

The Threat Intelligence subscription delivered by the AlienVault Labs team enables organizations of all sizes to focus on responding to the threats reported by the AlienVault Unified Security Management (USM™) platform, rather than having to research them. By alerting you to the most significant threats targeting your network, the USM platform maximizes the effectiveness of any IT team by allowing you to respond quickly and efficiently.

Keeping Your USM Platform Protected Against the Latest Threats

The USM platform delivers five essential security capabilities that no company should be without: Asset Discovery, Vulnerability Management, Intrusion Detection, Behavioral Monitoring, and SIEM (Security Information and Event Management). The AlienVault Labs team uses several manual and automated techniques to help develop threat intelligence such as: honeypots, in-house malware analysis, and big data analytics.

By unifying these essential security capabilities within a single platform and delivering continuously updated threat intelligence, the USM platform provides you with answers to the following critical questions:

- Am I vulnerable to this threat?
- Can my systems detect this threat?
- Am I being targeted?

By automating the threat detection process, USM enables you to spend more time responding to threats on your network and less time learning, deploying, and configuring tools. AlienVault USM gives you everything you need to manage threats and achieve regulatory compliance.

Threat Validation

To eliminate the need for our customers to conduct their own research, the AlienVault Labs threat research team spends countless hours mapping out the different types of attacks, the latest threats, suspicious behavior, vulnerabilities and exploits they uncover across the entire threat landscape.

Because we own both the data sources as well as the management platform, our threat experts have a comprehensive understanding of the interactions between the different data types being correlated and analyzed as well as the latest attack techniques. We embed this expertise in the built-in security controls and seamlessly integrated threat intelligence we deliver, to allow you to detect the latest threats as well as instruct you on how to mitigate the threats quickly and effectively, regardless of your network environment.

The AlienVault Labs team regularly delivers threat intelligence as a coordinated set of updates to the USM platform, which accelerates and simplifies threat detection and remediation:

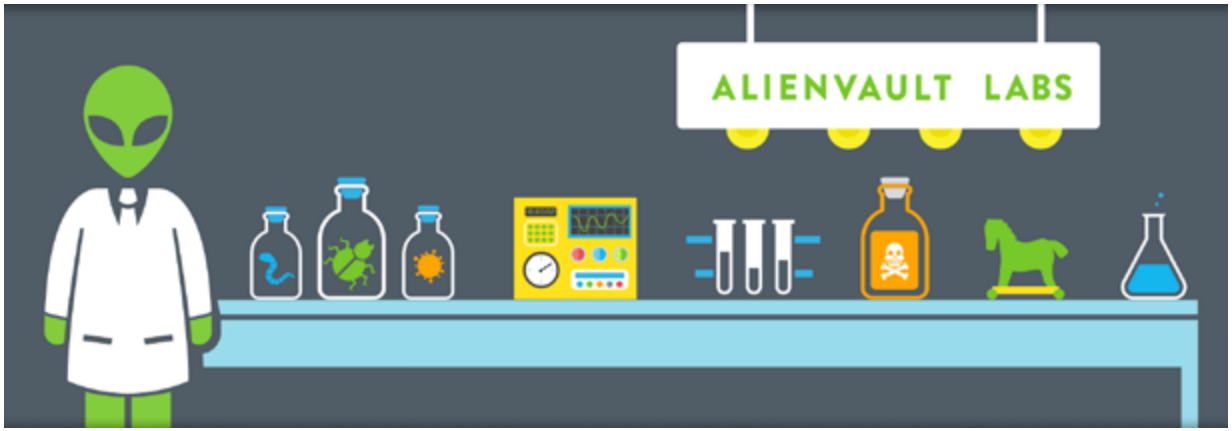
- **Correlation directives** – USM ships with over 2,500 pre-defined rules that translate raw events into specific, actionable threat information by linking disparate events from across your network
- **Network IDS signatures** – detect the latest malicious traffic on your network
- **Host IDS signatures** – identify the latest threats targeting your critical systems
- **Asset discovery signatures** – detect the latest operating systems, applications, and device information
- **Vulnerability assessment signatures** – uncover the latest vulnerabilities on your systems
- **Reporting modules** – receive new views of critical data about your environment to management and satisfy auditor requests
- **Dynamic incident response templates** – customized guidance on how to respond to each alert
- **Newly supported data source plugins** – expand your monitoring footprint by integrating data from legacy security devices and applications

Continuous Threat Research

AlienVault Labs constantly monitors, analyses, reverse engineers, and reports on sophisticated threats including zero-day attacks, advanced malware, botnets, phishing campaigns and more. Through this team of dedicated and renowned security experts, AlienVault contributes code, documentation, analysis and research results in various forms to the security community, to educate it and to make the world a more secure place for all of us.

The threat research provided by AlienVault Labs includes the latest information on the following areas:

- Vulnerabilities and Exploits
- Bruteforce Attacks
- Denial of Service Attacks
- Malware Detection
- Network-level Attacks
- SCADA Attacks
- System Probing and Scanning
- Malicious Activity



The AlienVault Threat Intelligence Subscription incorporates the latest threat research from the AlienVault Labs team. To learn more about the updates provided by the Threat Intelligence Subscription, go to the AlienVault Labs update section of the AlienVault Forums. To learn more about the other security research the team publishes, go to the AlienVault Labs blog.

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM