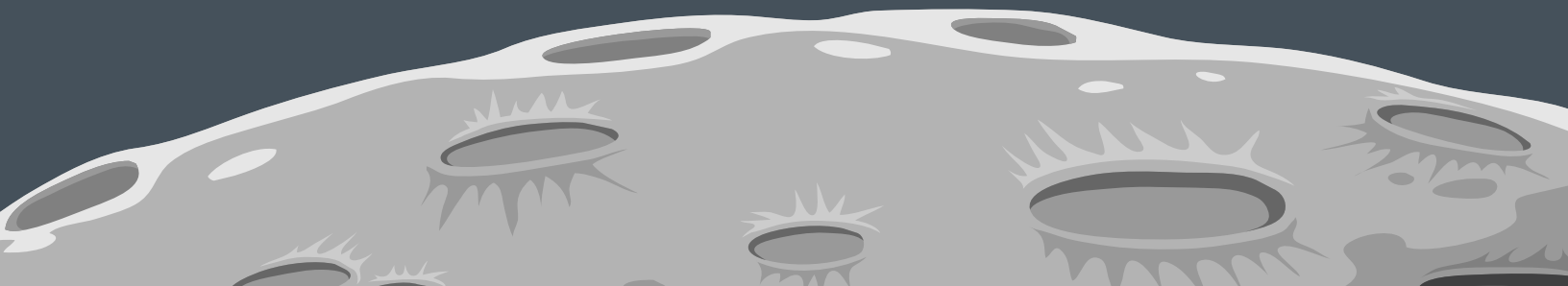
ALIEN VAULT

ALIENVAULT TECHNICAL WHITE PAPER

# Unified Security Management

VS.

# SIEM



The purpose of this white paper is to provide an overview of the changing security landscape, and more importantly to provide insight into the rapidly changing SIEM category, and the reasons that have led to those changes. To offer a complete picture of the changes to SIEM technology, it is valuable for some customers to understand the context of the SIEM market and how (and why) AlienVault differentiates itself from this traditional approach.

**ABOUT ALIENVAULT**

**Founded:**
2007

**Global Headquarters:**
San Mateo, CA

**EMEA/APAC Headquarters:**
Cork, Ireland

**Ownership:**
Privately held

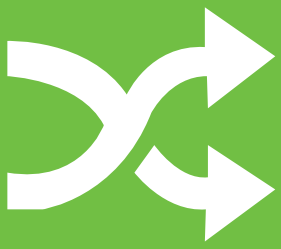
## The History of "SEM, SIM or SIEM?"

To best describe the market today, it's helpful to first revisit how the market has evolved. Initially Security Event Management (SEM) tools were designed for threat management against a noisy external threat environment that consisted primarily of worms. The orientation of SEM tools was primarily network and system events combined with real-time analysis to support incident response. There were also Security Information Management (SIM) vendors that provided long-term storage of log files, historical analysis and trending against a large database of data to support forensic activities. So we had real-time analysis to support incident response and long-term storage and historical analysis to support trend reporting and forensics.

Security Information and Event Management (SIEM) emerged as companies found themselves spending a lot of money on intrusion detection/prevention systems (IDS/IPS). These systems were helpful in detecting external attacks, but because of their reliance on signature-based detection, they generated a large number of false positives. First-generation SIEM technology was designed to reduce this signal-to-noise ratio and helped to capture the most critical external threats. Using rule-based correlation, SIEM helped IT teams detect real attacks by focusing on a subset of firewall and IDS/IPS events that were in violation of policy. Although expensive and time-intensive to maintain and tweak, SIEM investments continued as they solved a big headache of sorting through excessive false positives and effectively protecting companies from external threats.

While SIEM was a step in the right direction towards improved management, the world got more complicated when new regulations such as the Sarbanes-Oxley Act (SOX) and the Payment Card Industry Data Security Standard (PCI DSS) required much stricter internal IT controls and assessment. Virtualization became more prevalent as well, and new security point solutions were introduced as the explosion of personal devices entered the enterprise.

Log management tools were designed to collect, report, and archive a large volume and breadth of log data, whereas SIEM solutions were designed to correlate a subset of log data.



To satisfy these new requirements, organizations were required to collect, analyze, report on and archive all logs to monitor activities inside their IT infrastructures. The intent was not only to detect external threats, but also to provide periodic reports of user activities and create forensics reports surrounding a given incident. Though SIEM technologies collected logs, they processed only a subset of data related to security breaches. They weren't designed to handle the sheer volume of log data generated from all IT components, such as applications, switches, routers, databases, firewalls, operating systems, IDS/IPS and Web proxies.

Created to monitor user activities rather than external threats, Log Management (LEM) products entered the market as a technology with an architecture to handle much larger volumes of data and with the ability to scale to meet the demands of the largest enterprises. Although companies implemented log management and SIEM solutions to satisfy different business requirements, they also discovered that the two technologies work well together. Log management tools were designed to collect, report, and archive a large volume and breadth of log data, whereas SIEM solutions were designed to correlate a subset of log data to point out the most critical security events, and that hasn't changed. Splunk, for example, is a log management solution with a very small security use case. SIEM solutions continue to focus on aggregating 'external' data sources.

Unfortunately, both LEM and SIEM lack the security intelligence needed to detect threats and effectively combat today's attacks. To make matters worse, in tough economic times or tight budgets influencing decisions, we can expect to see IT trying to stretch its legacy logging technologies to solve even more problems (as demonstrated by the convergence of SEM and SIM, which created SIEM). Now we've caught you up, let's talk about "What's Changed?" and "Why?"

## "What's Wrong with SIEM?"

Fast-forward a decade—today we have many IT security teams that have made a significant investment in both money and resources (people) to support traditional SIEM products, only for the SIEM to show little-to-no material value on delivering on the promise of security visibility. The reasons for these shortfalls are numerous.

It's important to note that the risk that organizations feel is real, just as the threats are very real. The reality is that the "actual" threat is usually much greater than the "perceived" threat inside of most organizations.

The dirty little secret in the SIEM industry is that most SIEM solutions have a shelf life of approximately 18-24 months before organizations give up and begin to look for another SIEM solution. Most organizations cannot support these deployments and many SIEM technologies fail not due to technology failures but because organizations simply don't have the time, money, resources or process to support the technology. It's the inability of organizations to Implement and Tune the technology and not the SIEM solution itself that threatens the long-term value of traditional SIEM. In other words, the entire category of SIEM is flawed in its approach, especially in the mid-market where resources are often hard to come by. Let's examine the specific areas that lead to these failures:

### Poor Correlation

It is difficult to strike the right balance between correlation rules that catch all possible attacks and correlation rules that produce too many false-positive alerts. Tuning often requires a professional services engagement and on-going expenses, and industry analysts report speaking with customers for whom, "...a year of tuning was required". This lack of balance will continue to plague the SIEM vendors as the complexity of managing all of the changes in a typical network, including moves, adds, and edits to the data sources (such as servers, devices, and applications) is not something they can solve.

Organizations rely on the data collection, normalization and retention capabilities of the SIEM for the purpose of correlation. Without very strong (i.e. custom) correlation, detecting and responding to threats is impossible. And, if an organization wants to ensure the fidelity of their correlation logic, it must verify its custom correlation every time there is a change on the network. For example, it's not uncommon to see a routine update to a data source (for example, due to an OS/firmware update) dramatically impact the fidelity of the correlation rules/alarms/logic. This happens when updates are performed to network devices, servers (physical and virtual), antimalware, applications, and so forth. Organizations are very dynamic, and the network infrastructure is always evolving.

### Ease of Use

As stated before, SIEM solutions have been around for almost a decade. These same solutions were built to serve the largest of enterprises where resources and "dedicated" headcount are more the norm. Understanding "whom" these solutions were designed to serve, the vast majority of SIEM solutions are very difficult to use. Sadly, security pros have resigned themselves to accept this as just another part of the job. But that doesn't have to the case.

### Trending and analytics

If the tuning/correlation doesn't get you the failure, then consumable analytics will. SIEMs often have a selection of canned reports but new report creation is not flexible to adjust to rapidly changing conditions in today's environments. Canned reports can be useful, and may look great initially, but relying on a canned report to understand the end-to-end implications of a security event from the edge router to the application simply doesn't work. In a world where threats are increasingly dynamic, reporting must also be dynamic.

### The "Rules-based" approach

When a correlated security event is presented to the security analyst, it's reasonable to expect the analyst to limit his or her investigation to the data sources reported by the alert. A "Rules-based" approach supports only a go-forward view of security data—if you get a correlation rule wrong, you can't adjust the model and re-analyze the data, because events that didn't match the old rule have already been discarded. Not the desired outcome, and certainly not for what these traditional SIEM solutions cost.

### Cost

SIEM is expensive. It's expensive because large enterprise organizations continue to pay hefty prices for these solutions. SIEM has, in most cases, been cost-prohibitive for the mid-market customer who is looking to secure their organization. Costs associated

with a traditional SIEM deployment include:

- Initial Licensing Costs
- Implementation/Optimization Costs
- Ongoing Management Costs
- Renewal Costs
- Integration of data sources from disparate security technologies
- Training of personnel/incoming personnel

The hidden costs are what usually result in the demise of the traditional SIEM deployment—the very real and painful costs associated to deploying, integrating, using, managing, training, tuning, cursing, and potentially expanding the deployment.

These are the areas that have led to such dissatisfaction with the traditional SIEM approach. These are very real and evident in almost every organization that has had experience with SIEM. AlienVault only had to listen to its customers to know that something had to change. This was the primary driver in introducing the Unified Security Management (USM) platform.

"By using AlienVault's Unified Security Management platform, with its correlation engine and threat intelligence, we were able to save on both of these fronts while still delivering effective security."

*Kim Halavasoki, Chief Security Officer, Crosskey Banking*

## "What Options Does My Organization Have Besides SIEM?"

Despite the Billions (with a "B") being spent every year on security, these things hold true:

- More and more organizations are finding themselves in the crosshairs of various bad actors for a variety of reasons, most often to steal customer data or IP, or smear a reputation.
- The "security arms race" cannot continue indefinitely as the economics of securing your organization is stacked so heavily in favor of those launching the attacks that incremental security investments are seen as impractical.
- In spite of SIEM technology being on the market for several years, it continues to disappoint users.

Fortunately, there is an alternative to traditional SIEM, one that overcomes the challenges that continue to limit the effectiveness of SIEM technology: Poor Correlation, Ease of Use, Trending and Analytics, Rules-Based Approach, and High cost—Unified Security Management, or USM.

Unlike any other security solution on the market, AlienVault's USM platform has dramatically reduced the cost and complexity related to buying and deploying all of the essential security controls required for comprehensive security visibility.

Gartner recognizes that there is only one vendor in the SIEM category that is seen as a "Visionary." AlienVault is fundamentally changing the way threat detection and incident response is done, taking into consideration the last decade of lessons and building a solution that will finally address the lack of security visibility organizations have today.


*Source: Gartner (August 2016)*

## The Alternative: Unified Security Management

IT organizations of all shapes and sizes have embraced USM to reduce the cost, improve security visibility and accelerate threat detection and remediation. They need access to security solutions that offer significant time-to-value returns, while improving their overall security posture.

At AlienVault we're committed to unifying best-of-breed technology with shared global threat intelligence for truly open and collaborative security.

AlienVault's Unified Security Management™ (USM) platform gives organizations a solution that offers an effective alternative to the most sophisticated and expensive enterprise-level security products.

AlienVault has included five essential security capabilities managed by a single console, providing everything you need for complete security visibility and threat intelligence. These capabilities include Asset Discovery, Vulnerability Assessment, Threat Detection, Behavioral Analysis, and Security Intelligence. These integrated features are powered by up-to-the-minute threat intelligence from AlienVault Labs and our Open Threat Exchange™—the world's largest crowd-sourced collaborative threat repository.

AlienVault offers the only Unified Security Management solution to unify these five essential security capabilities. With essential security controls built-in, AlienVault USM

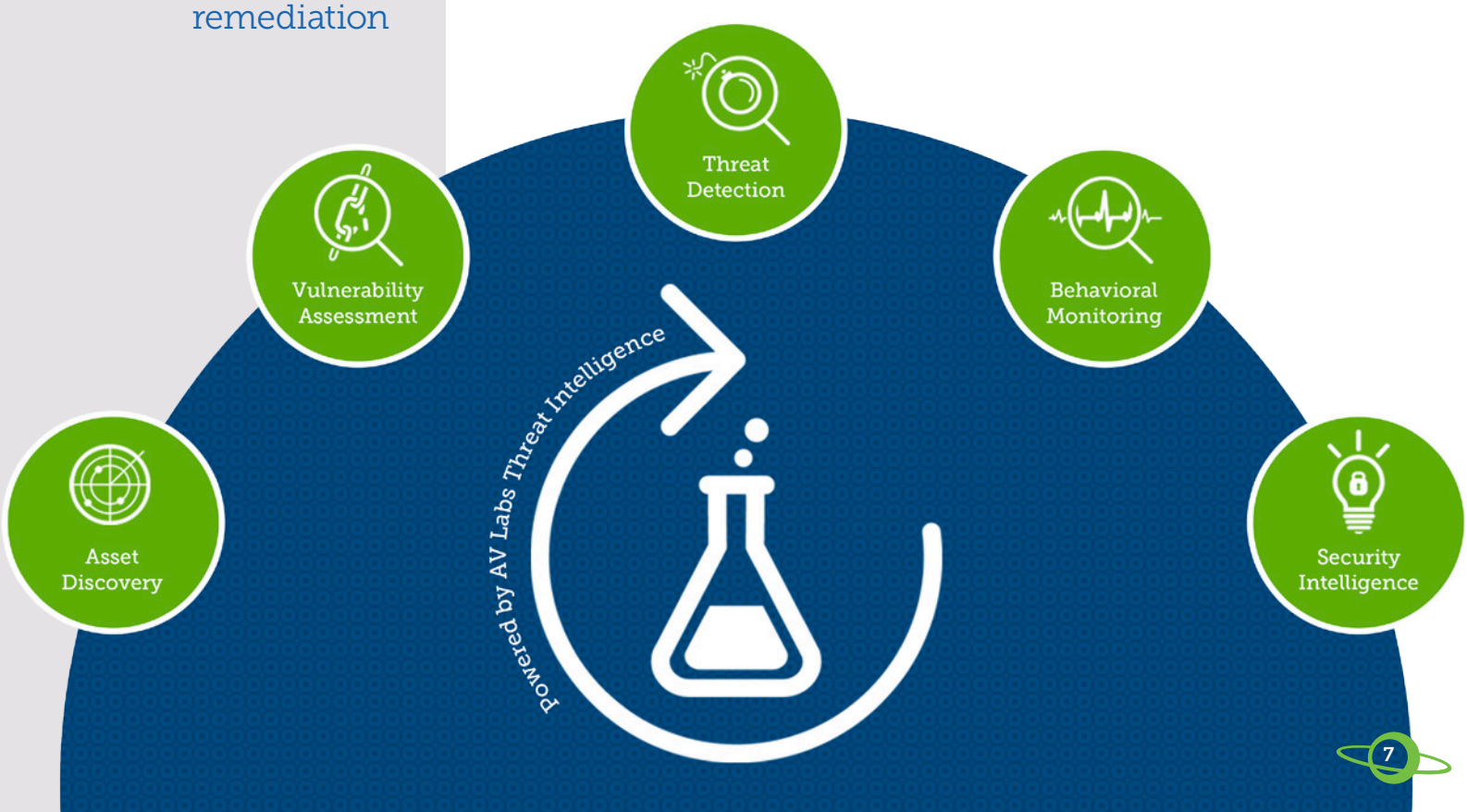
puts complete security visibility within fast and easy reach, which translates into rapid time to value. Whether large or small, all organizations need the complete visibility USM offers to:

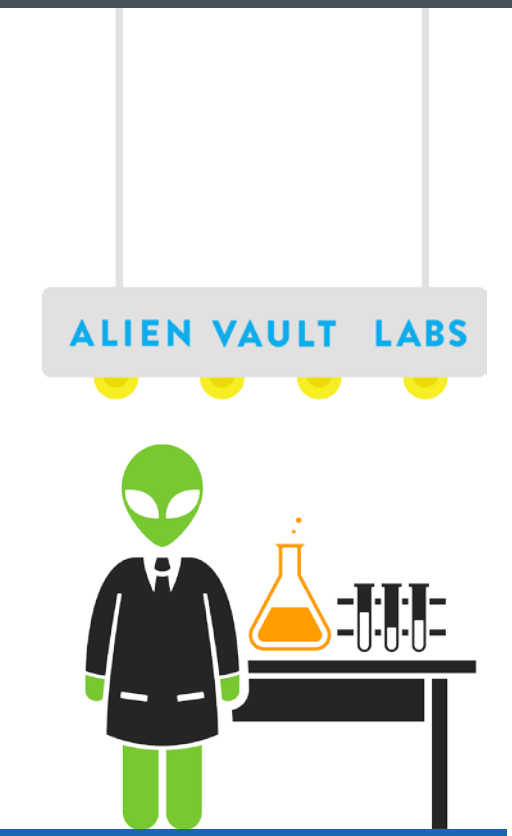
- Detect emerging threats across your environment
- Respond quickly to incidents and conduct thorough investigations
- Measure, manage, and report on compliance (PCI, HIPAA, ISO, and more)
- Optimize your existing security investments and reduce risk

USM also offers simplicity, streamlined installation and use, and the ability to update all the security functions concurrently. These concurrent updates allow AlienVault to do something no other solution on the market can do—AlienVault Labs threat research team can write, maintain and verify all the needed correlation delivering the highest levels of security visibility.

AlienVault believes to simplify security, you must simplify the solutions designed to deliver security visibility. AlienVault is fanatical about putting users first in everything we do. We strive every day to deliver powerful functionality that is easy to use with one of the fastest and longest lasting ROIs in the market.

USM delivers integrated security controls to simplify and accelerate threat detection and remediation






Think of AlienVault Labs as an extension to your IT team.

## AlienVault Labs Threat Intelligence and Open Threat Exchange

One of major challenges smaller IT organizations have is being able to conduct the research needed to keep up with the constant evolution of the threat landscape. Fortunately, you have AlienVault on your side.

Think of our Labs team as an extension to your IT team. AlienVault understands that threat experts are very difficult to find. It's an enormous financial commitment to have threat experts dedicated to researching the latest threats and how to detect them, as well as being constantly engaged in dialogue with other threat experts around the trends that are being observed in the market.

The AlienVault Labs Threat Intelligence team maximizes the efficiency of your security-monitoring program, by delivering the following directly to your AlienVault Unified Security Management (USM) installation. This team of security experts delivers updates to the product every 30 minutes that include 8 coordinated rule-sets that unify your entire technology stack:

- **Network-based and Host-based IDS signatures** — which detect the latest threats in your environment.
- **Asset discovery and inventory database updates** — identifies the latest operating systems, applications and device types
- **Vulnerability database updates** — dual database coverage to find the latest vulnerabilities on all your systems
- **Report modules and templates** — providing new ways to view data in your environment
- **Incident response templates / "how to" guidance** for each alarm in USM

### Event Correlation

Another area where AlienVault's integrated, security-focused design has an advantage over other tools is event correlation. AlienVault understands that most organizations don't have the time, resources or expertise in-house to monitor changes to the threat landscape as well as manage all the technologies they have deployed in their environment.

AlienVault delivers actionable security intelligence by automating the event correlation process:

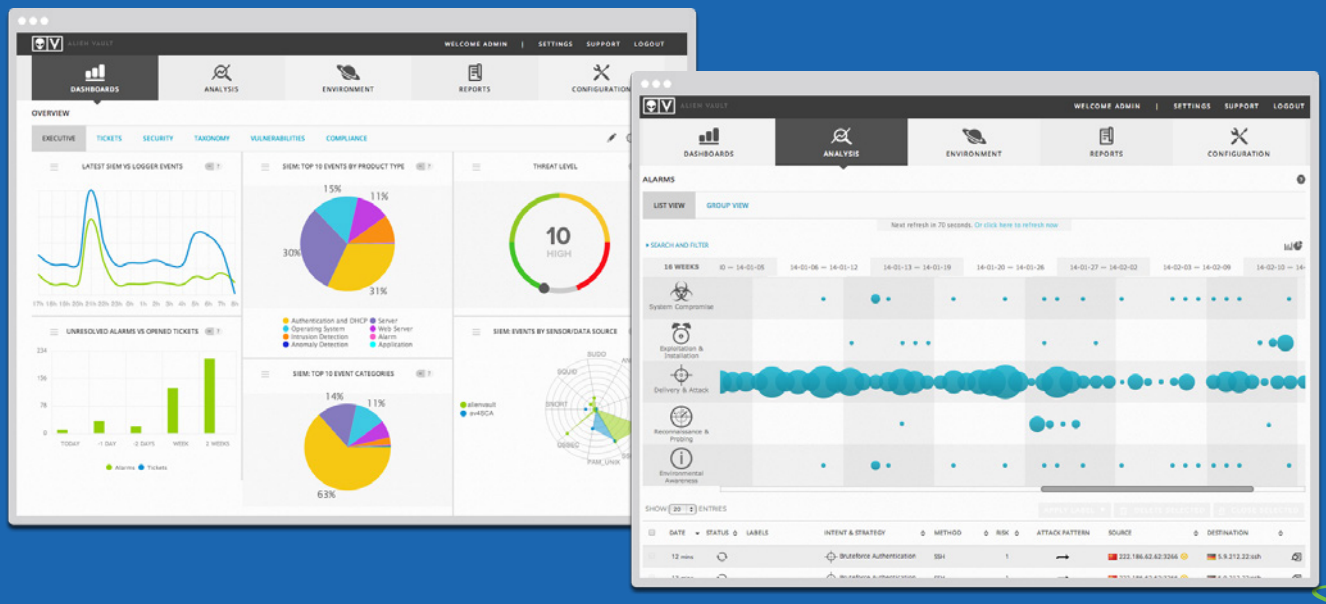
- **Data Collection** — Identify log data for automatic import and integration, from both the technologies included in the USM platform and third party tools via plug-ins
  - *Customers can utilize our extensive library of plug-ins or create their own for custom applications and legacy devices*
- **Normalization** — Parse, normalize, and integrate log data into built-in SIEM analysis engine
- **Cross Correlation** — Apply 1,700+ correlation rules to asset, vulnerability, network traffic, and threat data

- **Alarms & How to Respond** — Assess severity, with detailed context-specific remediation instructions
- **Emerging Threat Detection** — Automatic updates of new correlation rules and signatures for new threats, assets, vulnerabilities, and more

Traditional SIEM solutions would leave all this work up to you to perform. In other words, you would be responsible for the SIEMs ability to detect threats — you would need to write the correlation rules, do the research, integrate threat feeds, etc. If your team is putting out other fires or you fundamentally believe that you should be leveraging the investments made at monitoring your environment instead of managing your SIEM; USM is the right solution for you.

AlienVault understands that most organizations don't have the time, resources or expertise (in some cases) in house to develop, manage and monitor all of these areas of their environment. With this easily consumable threat intelligence fueling your USM platform, you'll be able to detect the latest threats and prioritize your response efforts. Specifically, you'll extend your security program with:

- **Real-time botnet detection** — identifies infection and misuse of corporate assets
- **Data exfiltration detection** — prevents leakage of sensitive and proprietary data
- **Command-and-control traffic (C&C) identification** — identifies compromised systems communicating with malicious actors
- **IP, URL, and domain reputation data** — prioritizes response efforts by identifying known bad actors and infected sites
- **APT (Advanced Persistent Threat) detection** — detects targeted attacks often missed by other defenses
- **Dynamic incident response and investigation guidance** — provides customized instructions on how to respond and investigate each alert



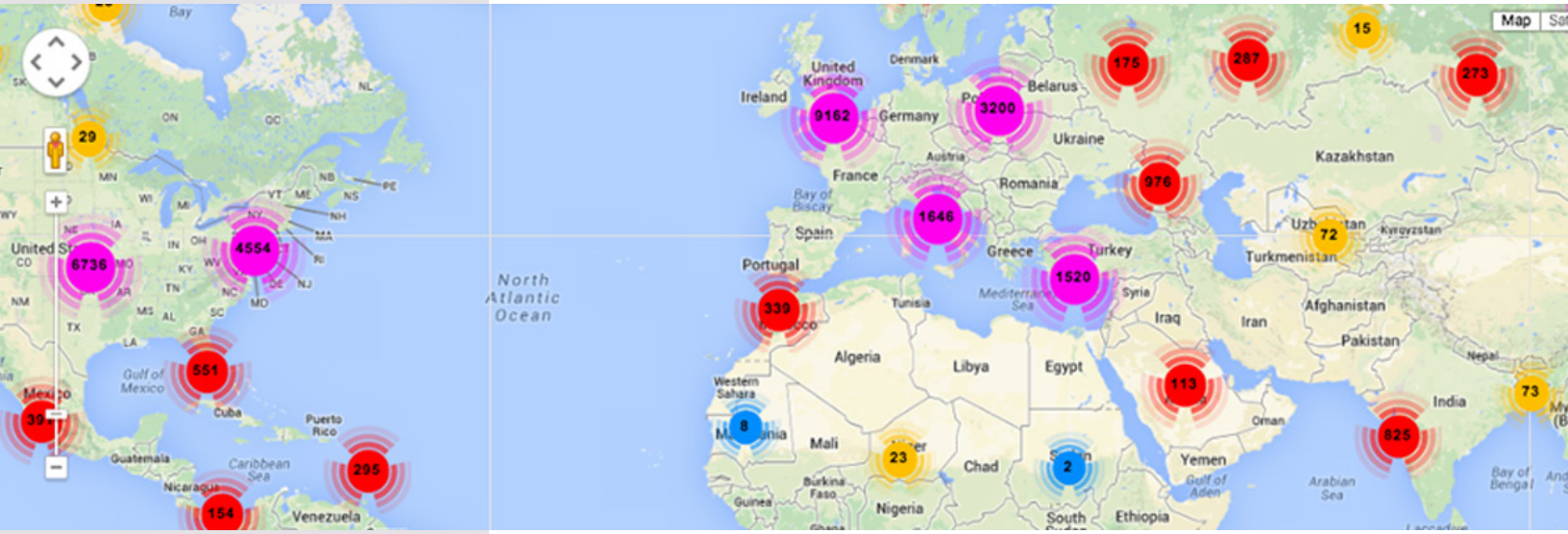
Threat data is automatically cleansed, aggregated, validated, curated and published by the AlienVault Labs threat research team

### Open Threat Exchange

Adding to the difficult is that 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 an advantage. Most threat intelligence networks are closed and limited to only certain industries, vendors, or government agencies. For the first time, AlienVault's OTX enables anonymous sharing of threat intelligence with anyone who joins.

OTX is an element of AlienVault's USM platform's security intelligence capability. OTX is a framework for a unique and powerful collaborative defense capability that the AlienVault Labs threat research team validates and curates. It incorporates a data from more than 140 countries and a broad range of devices (firewalls, proxies, web servers, anti-virus systems, and intrusion detection/prevention systems).

This data is automatically cleansed, aggregated, validated, curated and published by the Alienvault Labs threat research team. In addition to providing data for the regular updates of the USM platform, OTX enables collaborative security intelligence to spread among many industries and countries, composed of organizations of all sizes. This sharing limits the attacker's ability to isolate targets by industry or organization size, improving the security of anyone who participates.



## AlienVault Capabilities Matrix

| CAPABILITY | ALIENVAULT | SIEM |
|---|---|---|
| **Asset Discovery** — Discover and track hosts, services, and installed software present in the environment for improved correlation and context for incident response | ✓ | |
| **Vulnerability Assessment** — identify vulnerabilities in the monitored environment and track historical record for compliance purposes | ✓ | |
| **Threat Detection** — monitor the environment for threats, identifying known attack vectors, attack patterns, payload signatures and behavioral identification of exploits and malware. | ✓ | |
| **Behavioral Monitoring** — monitor the ongoing behavior of observed systems to provide context for forensic investigation and identification of potential security incidents | ✓ | |
| **Security Intelligence** — aggregate and analyze information from all the security controls and environment in order to correlate disparate behavior and provide a platform for forensic investigation. | ✓ | ✓ |
| **Threat Intelligence** — emerging threat analysis and research, which leverages more than 8,000 global collection points across more than 140 countries to analyze over 500,000 malware samples and over 100,000 malicious IP addresses daily within the world's largest crowd-sourced threat intelligence exchange—Open Threat Exchange (OTX) | ✓ | |

| TECHNOLOGY | ALIENVAULT | SIEM |
|---|---|---|
| **Passive Network Discovery** — identify hosts with passive network monitoring | ✓ | |
| **Active Network Scanning** — actively scan the network to identify and version running services without local access to the machine | ✓ | |
| **Host-based Software Inventory** — provide full binary-level inventory of software packages running on assets | ✓ | |
| **Continuous Vulnerability Monitoring** — using data from the asset discovery capabilities, correlate the latest known vulnerability feeds with the existing asset inventory information to identify vulnerable services without active scanning | ✓ | |
| **Active Network Scanning** — actively scan the network to identify vulnerable services. Both authenticated and unauthenticated scanning is available depending on the target. | ✓ | |
| **Network IDS** — perform deep-packet inspection of the network traffic in order to identify attacks, behaviors of compromised systems, policy violations, and more. | ✓ | |
| **Host IDS** — monitor the operating system level activity of a host to identify indicators of compromise, such as rootkits, malware, or abuse of system services | ✓ | |
| **File Integrity Monitoring** — monitor changes to critical files to identify potential security issues on critical hosts. | ✓ | |
| **Netflow Analysis** — identify network activity throughout your environment. Identifies protocol usage, and volume of traffic between hosts in monitored environments. | ✓ | |
| **Service Availability Monitoring** — identify service availability in the environment to detect disruptions in availability, which could indicate a successful attack or compromise. | ✓ | |
| **Log Management** — provides a consolidated interface for reporting and querying activity occurring in the monitored environments. Critical for most compliance use cases. | ✓ | ✓ |

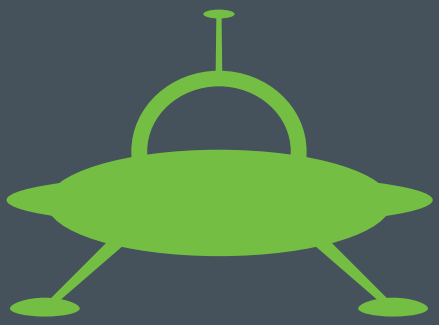
## Don't take our word for it — see what your peers and industry experts are saying:

GARTNER MAGIC QUADRANT

CUSTOMER STORIES

FREE TRIAL

WATCH A DEMO



## About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).