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.

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 large databases of data to support forensic activities. In other words, IT professionals could purchase a SEM tool for real-time analysis to support incident response, and a separate SIM tool for long-term storage and historical analysis to support trend reporting and forensics.

ABOUT ALIENVAULT

Founded: 2007

Global Headquarters: San Mateo, CA

EMEA/APAC Headquarters: Cork, Ireland

Ownership: Privately held

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 lot of false positives. First-generation SIEM technology was designed to reduce this signal-to-noise ratio and help 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. More recently, the rapid rise of public cloud computing introduced new security challenges for IT departments, in part because of architectural differences that make security tools built for on-premises environments sub-optimal for security visibility of public cloud environments.

To satisfy new compliance regulations, 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 environments (including public cloud, private cloud and virtualized on-premises infrastructure, and hybrid environments) and 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. However, whenever tough economic times or tight budgets influence security decisions, we can expect to see IT teams trying to stretch 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 invested significant time, money, and personnel to support traditional SIEM products, only for the SIEM to show little-to-no delivery on the promise of security visibility. The reasons for these shortfalls are numerous.

Though organizations may be reluctant to give up the resources they've sunk into SIEM products, there is a hidden cost to maintaining an under-performing product that can't keep up with today's threat landscape. Comparatively, a data breach resulting from an under-performing SIEM could cost an organization significantly much more than the cost of replacing the outdated system.

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." SIEM vendors will continue to struggle with this balancing act due to the complexity of managing all the changes in a typical network, including moves, additions, and edits to data sources.

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 the breadth of threats that can affect your organization's critical infrastructure is impossible. If an organization wants to ensure the fidelity of its correlation logic, it must verify its custom correlation every time there is a change in the environment. 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 devices, servers (physical and virtual), anti-malware, applications, and so forth. Organizations are very dynamic, and 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 large enterprises that typically have substantial resources and dedicated security personnel. Given the audiences these solutions were designed to serve, the majority of SIEM solutions are very difficult to use. Sadly, many security professionals have resigned themselves to this as just another part of the job.

Trending and Analytics

If correlation limitations don't cause your solution to fail, then consumable analytics will. SIEMs often have a selection of canned reports, but lack flexible data visualization tools that can capture the rapidly changing conditions in today's environments. While canned reports can be useful, they're not sufficient to help you understand the end-to-end implications of a security event from the edge router to the application. In a world where threats evolve daily, analysis and data visualization must also be dynamic.

The "Rules-based" Approach

When a correlated security event is presented to a security analyst, it's reasonable to expect the analyst to limit his or her investigation to the data sources reported by the alert. However, a "rules-based" approach supports only a go-forward view of security data. If you encounter a problem with the correlation rule that generated an alert, 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, particularly given the high cost of these traditional SIEM solutions.

Cost

SIEM is expensive. While 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 wants 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 lead organizations to abandon the traditional SIEM product—the very real and painful costs associated with deploying, integrating, using, managing, training, tuning, and potentially expanding the deployment.

Behind the Technology Curve

The traditional SIEM approach has not kept up with the pace of changes to the IT landscape, from the influx of new technologies on the market to the recent surge in public cloud computing. As organizational security needs continue to evolve, the traditional SIEM will fall even further behind the curve, leaving IT teams to wrestle with cumbersome, expensive tools that fail to accommodate their entire infrastructure in a centralized, easy-to-manage way. Organizations that want to avoid these headaches should look for a more complete security solution.

> "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") 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.
- In the "security arms race" between malicious actors and the organizations defending against their attacks, stacking single-point security solutions is not only an expensive approach, but also ineffective and impractical for most organizations.
- In spite of SIEM technology's tenure in the marketplace, 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: AlienVault Unified Security Management™, or USM™.

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

Gartner recognizes that there is only one vendor in the SIEM category that qualifies as a "Visionary." AlienVault is fundamentally changing the way threat detection and incident response are 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.

The Alternative: Unified Security Management

IT organizations of all shapes and sizes have embraced USM to reduce costs, improve security visibility, and accelerate threat detection and compliance management across their on-premises and cloud environments. They need security solutions that offer significant time-to-value returns, while improving their overall security posture.

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

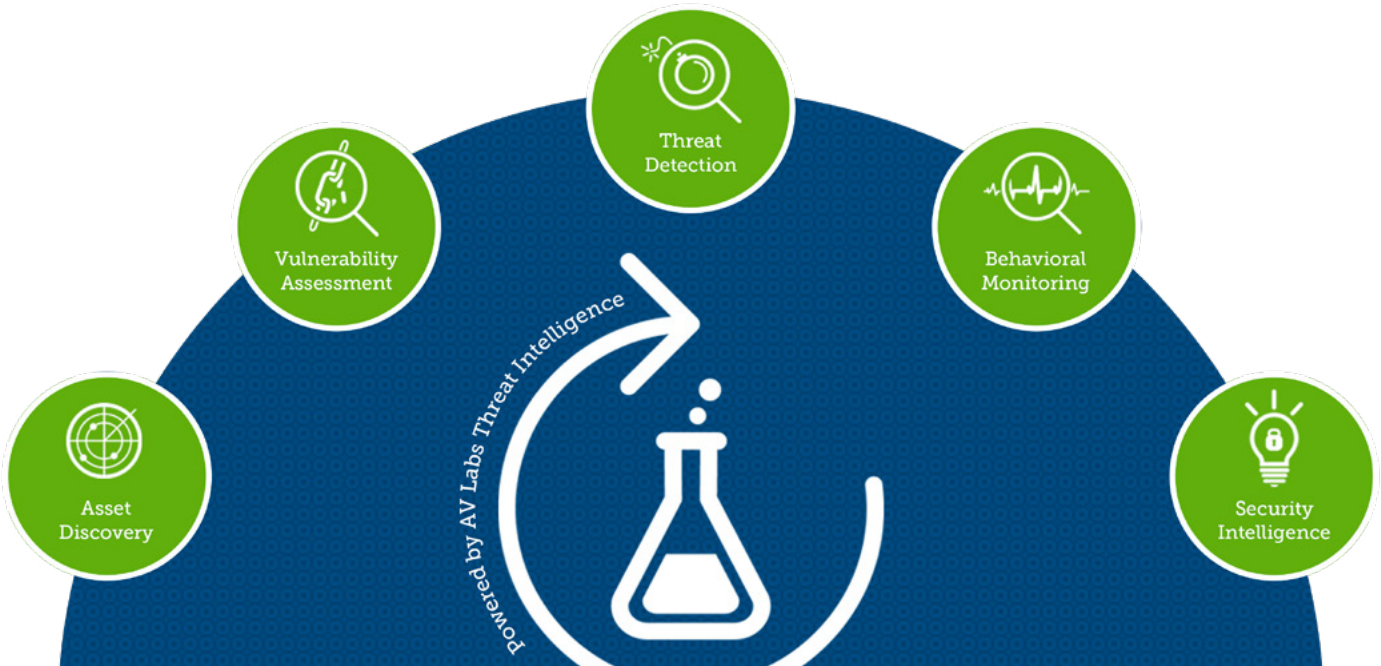
AlienVault USM combines five essential security capabilities managed by a single console, providing everything you need for complete security visibility and threat intelligence across your critical infrastructure. These capabilities include Asset Discovery, Vulnerability Assessment, Threat Detection, Behavioral Analysis, and SIEM event correlation and log management. These integrated features are powered by continuous threat intelligence updates from the AlienVault Labs Security Research Team and the Open Threat Exchange® (OTX™)—the world's largest crowd-sourced collaborative threat repository.

AlienVault offers the only unified security monitoring solution on the market to integrate these five essential security capabilities plus integrated threat intelligence. 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 cloud and on-premises environments
- Respond quickly to incidents and conduct thorough investigations
- Measure, manage, and report on compliance (PCI, ISO, SOX, and more)
- Optimize your existing security investments and reduce risk

USM also offers simplicity, streamlined installation and use, and the ability to update all security functions concurrently. These concurrent updates allow AlienVault to do something no other solution on the market can do: AlienVault Labs Security Research Team can write, maintain, and verify all the necessary correlation rules, delivering the highest levels of security visibility.

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



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 the AlienVault Security Research 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 on staff who are dedicated to researching the latest threats and how to detect them, as well as staying constantly engaged in dialogue with other threat experts around trends in the threat landscape.

The Security Research Team maximizes the efficiency of your security-monitoring program by continuously delivering the following to your AlienVault Unified Security Management (USM) deployment, including 8 coordinated rulesets that unify your entire technology stack:

- **Network-based and host-based IDS signatures** — Detect the latest threats in your on-premises environments
- **Asset discovery and inventory database updates** — Identify the latest operating systems, applications, and device types across your critical infrastructure
- **Vulnerability database updates** — Find the latest vulnerabilities on all your systems and services with dual database coverage
- **Data visualization and analysis tools** —Gain new insight into the data in your environments
- **Incident response templates** — Access "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 in-house expertise to monitor changes to the threat landscape as well as to manage all the technologies they have deployed in their environments.

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
- **Normalization** — Parse, normalize, and integrate log data into built-in SIEM analysis engine
- **Cross Correlation** — Apply hundreds of correlation rules to asset, vulnerability, traffic, and threat data. The pre-built correlation rules library in USM is continuously updated by the Security Research Team as threats evolve and new threats emerge in the wild
- **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 SIEM's ability to detect threats — you would need to write the correlation rules, do the research, integrate threat feeds, and continuously update correlation rules. If your team is putting out other fires or you fundamentally believe that you should be leveraging your resources to monitor your environment rather than manage 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 the entirety of their critical infrastructure. 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** — Identifies 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

AlienVault Open Threat Exchange (OTX)

Adding to the difficulties faced by security professionals 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 Open Threat Exchange (OTX) enables anonymous sharing of threat intelligence with anyone who joins.

OTX is the largest and most authoritative crowd-sourced threat intelligence exchange in the world, providing security for you that is powered by all. Every day, more than 53,000 participants from 140+ countries contribute over 10 million threat indicators to OTX. The Security Research Team automatically analyzes raw OTX data using a powerful discovery engine to determine the nature of the threat and uses a similarly powerful validation and machine learning engine to continually curate the database and certify the validity of those threats.

The AlienVault Labs Security Research Team builds insights from the OTX community into the continuous threat intelligence updates they deliver to the USM platform, ensuring that your security plan always reflects global insights into the latest attack trends and bad actors operating in the wild.

> Threat data is automatically cleansed, aggregated, validated, curated, and published by the AlienVault Labs Security Research Team

AlienVault Capabilities Matrix

CAPABILITY	ALIENVAULT	SIEM
Asset Discovery — Discover and track hosts, services, and installed software and services present in your environments for improved correlation and context for incident response	✓	
Vulnerability Assessment — Identify vulnerabilities across your critical infrastructure and track historical record for compliance purposes	✓	
Threat Detection — Monitor your environments 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	✓	
Event Correlation — Aggregate and analyze information from all security controls and environments to correlate disparate behavior and provide a platform for forensic investigation	✓	✓
Threat Intelligence — Receive actionable threat intelligence delivered directly to USM via continuous updates from the the AlienVault Security Research Team, which leverages more than 10 million daily threat indicators from 53,000 contributors across 140+ countries 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	✓	
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 across your environments without active scanning	✓	
Active Network Scanning — Actively scan the network to identify vulnerable services with authenticated scanning	✓	
Network IDS — Perform deep-packet inspection of network traffic 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	✓	

TECHNOLOGY	ALIENVAULT	SIEM
Cloud IDS — Leverage direct hooks into cloud APIs to natively collect and analyze a rich set of cloud log data from your Azure and AWS environments	✓	
File Integrity Monitoring — Monitor changes to critical files in your on-premises environments to identify potential security issues on critical hosts.	✓	
Service Availability Monitoring — Identify service availability in your on-premises environments 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 across your critical infrastructure; critical for most compliance use cases	✓	✓

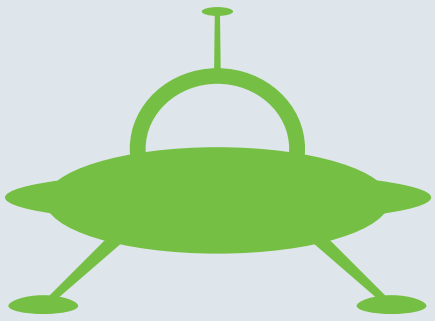
Learn More About AlienVault USM with These Resources:

GARTNER MAGIC QUADRANT

CUSTOMER STORIES

FREE TRIAL

LIVE 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.