The SIEM Evaluator’s Guide
Using SIEM for Compliance, Threat Management, & Incident Response

Security information and event management (SIEM) tools are designed to collect, store, analyze, and report on log data for threat detection, incident response and compliance management. The following set of criteria provides a useful reference for evaluating SIEM tools. Additionally, you’ll learn how AlienVault Unified Security Management (USM) delivers optimized SIEM functionality, by building in the essential security capabilities you need for complete visibility – helping you achieve security and compliance faster, easier, and more affordable.
# Table of Contents

The Evolution of SIEM and Security Intelligence 3  
1. Deployment and management simplicity 4  
2. Built-in essential security capabilities 5  
3. Real-time monitoring and correlation 6  
4. Collaborative threat intelligence 7  
5. Flexible log query and search 8  
6. Unified management console 9  
7. Log source coverage and management 10  
About AlienVault USM 11  
About AlienVault 13
The Evolution of SIEM and Security Intelligence

Over the past few years, the primary use cases for SIEM products have evolved beyond compliance management, as organizations realize the benefits of security intelligence in improving their ability to respond to emerging threats. Even Gartner has changed its SIEM evaluation criteria to include targeted attack detection in addition to compliance controls. Why? Due to the rise in successfully targeted attacks, organizations have expanded their requirements for utilizing their log data and SIEM correlation capabilities have shifted to improve security monitoring, early breach detection, and incident response. If your SIEM doesn't have these capabilities it likely means you will be purchasing the functionality from a separate vendor, then going through the effort of integrating them.

SIEM Evaluation Criteria

When evaluating any technology, it’s essential to outline your primary use cases and success factors for the technology. That said, the following SIEM checklist is broad enough to address the common incident response and compliance management use cases for SIEM. In addition to adding in some “Pro Tips”, we’ve also included a quick explanation of how AlienVault USM meets each of these key requirements.

1. Deployment and management simplicity
2. Built-in essential security capabilities
3. Real-time monitoring and correlation
4. Collaborative threat intelligence
5. Flexible log query and search
6. Unified management console
7. Log source coverage & management
1. Deployment and management simplicity

- Flexible deployment options
- Centralized configuration management of all security components
- Simplicity of log integration
- Investment in user interface design
- Intuitive and customizable workflows
- Flexible and customizable dashboards
- High levels of automation
- Remediation guidance
- Collaborative investigation
- Case management and ticketing

Why It’s Important: One of the biggest headaches with traditional SIEM technology is that deployments are complex and take way too long to complete. Why is this? Most single purpose SIEM tools rely on third party data sources for the basics in security visibility – and the integration of asset inventory, vulnerability, and threat detection data – complicates matters significantly. As a result, it can take weeks or months before the first alert or report is generated.

AlienVault USM: All aspects of AlienVault USM were designed with the underlying focus of reducing complexity and enabling rapid, successful, sustainable deployments. Deployment wizards, support for virtual, physical, and EC2 environments, and centralized essential security capabilities all contribute to simplified USM implementations.

Pro Tip: The real trick is finding a solution with the proper balance of ‘easy to use’ and ‘complete product’. Minimizing the number of point products in the overall solution will significantly reduce the integration effort, allowing you to demonstrate progress much faster.
2. Built-in essential security capabilities

- Asset discovery and inventory
- Vulnerability assessment
- User activity monitoring
- Data access monitoring
- Application monitoring
- Network analysis/NetFlow (packet capture)
- Wireless intrusion detection (WIDS)
- Host-based intrusion detection (HIDS)
- Network-based intrusion detection (NIDS)
- Behavioral monitoring and profiling
- File integrity monitoring
- Log management

*Why It’s Important:* In the past, these essential security capabilities were delivered via point products, requiring the investment and time to integrate with the SIEM’s event correlation engine. When setup was complete you still had disparate interfaces to juggle when it came down to managing the products and actually investigating security incidents.

*AlienVault USM:* Significantly simplifying deployment and overall management, all AlienVault USM offerings include the industry’s most complete set of essential security capabilities, managed through a single web-based interface. This helps you greatly reduce licensing costs, accelerate time to value, and most importantly, enhance incident response and compliance management.

*Pro Tip:* At deployment time focus on integrating your infrastructure event data. Start with those data sources that provide the most relevant content and context. For example, firewall logs, domain controller logs, anti-virus logs, etc. are a good place to start.
3. Real-time monitoring and correlation

- Customizable reports and dashboards
- Dynamic event validation
- Dynamic incident response guidance
- Built-in threat intelligence
- IP and domain reputation monitoring
- Robust set of canned correlation rules
- Wizard for custom correlation rules
- Open API for external data sources

**Why It’s Important:** Real-time monitoring and correlation is crucial for threat management, allowing you to track and analyze the progression of an attack across components and systems. It also allows you to assess threats based on user behavior, transactions, and data access events.

**AlienVault USM:** The AlienVault USM correlation engine leverages the largest collaborative threat intelligence system, the Open Threat Exchange (OTX), to establish relationships between events generated by devices, users, systems and applications. Leveraging the OTX infrastructure, AlienVault Labs analyzes over 500,000 malware samples per day, giving you the most robust built-in correlation rules available. That means before you write your first custom rule you’re already ahead of the game.

**Pro Tip:** Leverage 1500+ out-of-the-box event correlation rules that come with USM rather than struggling to write your own, on your own. Then define a process for implementing custom rules on a cadence (i.e. once per month), with an exception process for critical situations.
4. Collaborative threat intelligence

- Open and shared threat intelligence
- Highly diverse data set
- Global collection points - 9,500+
- IP and domain reputation monitoring
- Dynamic incident response guidance

Why It’s Important: The best security technology in the world is only as good as the threat intelligence that is powering it. Who, what, when and how is my network being attacked? The most reliable threat intelligence relies on access to the most diverse data set available, along with the expertise of the researchers analyzing it. And open, shared, and collaborative threat intelligence delivers on this promise.

AlienVault USM: AlienVault USM is underpinned by threat intelligence from the largest collaborative threat intelligence system in the world, the Open Threat Exchange (OTX). That’s how we analyze more than 500,000 malware samples per day, gathered from more than 9,500 global collection points in more than 140 countries.

Pro Tip: Monitor your own organization’s reputation by signing up for the free OTX Reputation Monitor Alert service. This service does not require you to be an AlienVault customer, and will give you a glimpse into the power of collaborative threat intelligence.
5. Flexible log query and search

- Search and structured analysis
- Query performance
- Asset-centric analysis and workflows

**Why It’s Important:** When suspicious activity is flagged by the monitoring system and correlation rules, analysts need to be able to drill in to details about the source, user or targeted device to identify the root cause, and scope of the issue. It’s important to be able to iteratively query the event to deduce the problem, and “pivot” from any data element to the next.

**AlienVault USM:** While other solutions have you clicking aimlessly through event detritus, AlienVault USM’s simplified search and structured analysis capabilities provide a quick and easy way to get to the raw log events that matter.

**Pro Tip:** When investigating an incident, focus on the specific target asset and all of the surrounding events associated with that asset. Investigate the network traffic the asset has generated before and after the incident, review vulnerability and configuration data, and identify the software installed on that device to determine next steps.
6. Unified management console

- Unified management of essential security capabilities
- Configurable and extensible dashboards
- Intuitive alarm taxonomy
- Built-in report modules and compliance reports
- Wizard-driven custom reporting
- Dynamic incident response guidance
- Open API
- Interactive online demo

**Why It’s Important:** Simplified SIEM deployment and management is a critical success factor. Security is complicated enough - your SIEM solution should make threat identification easier, not more difficult - with accurate threat detection, and clear guidance on what to do when threats are discovered.

**AlienVault USM:** AlienVault USM was designed to address the security analyst and incident responder perspective. Each alarm is categorized by the attacker’s intention – so you can quickly address System Compromise events, leaving Reconnaissance and Probing events to evaluate later. Additionally, each alarm includes customized incident response guidance so you know exactly what to do next to remediate the issue.

**Pro Tip:** Check out the interface yourself by visiting the interactive demo. In a few short minutes you’ll see the difference good design can make.
7. Log source coverage and management

- Broad data source support
- Ease of identifying and integrating new data sources
- Community of plug-in contributors
- Open API architecture

Why It’s Important: The first step in analyzing logs and events is integrating them, and this is an area where many SIEM solutions fall down. Issues that plague deployments include difficulty identifying sources, lack of normalization capabilities, and complicated processes for adding support for new sources. Not only should a SIEM solution provide broad, automated out-of-box support for data sources, it should have an extensible framework to support new sources.

AlienVault USM: AlienVault USM automatically discovers all IP-enabled assets in minutes. It identifies these as potential data sources and enables you to immediately begin integrating event log data from them. And because it’s based on the open source OSSIM, AlienVault USM is the only solution that leverages community support for crowd-sourced plugins. This gives you access to the largest community of open source SIEM contributors in the world.

Pro Tip: Use asset discovery to identify all IP-connected devices on your network. Evaluate installed software, system configuration and available services to determine relevance of the asset’s log data for security analysis. Consider implementing host-based IDS on devices that require in-depth monitoring as well as are in scope for compliance.
About AlienVault USM

AlienVault’s Unified Security Management™ (USM) platform provides a fast and cost-effective way for organizations with limited security staff and budget to address compliance and threat management needs. With all of the essential security controls built-in, AlienVault USM puts complete security visibility within fast and easy reach of smaller security teams who need to do more with less.

AlienVault USM combines the following essential security capabilities, including SIEM, for single-pane-of-glass security visibility and management.

- Asset Discovery and Asset Inventory
  - Active Network Scanning
  - Passive Network Scanning
  - Asset Inventory
  - Host-based Software Inventory
- Vulnerability Assessment
  - Network Vulnerability Testing
- Threat Detection
  - Network IDS
  - Host IDS
  - Wireless IDS
  - File Integrity Monitoring
- Behavioral Monitoring
  - Log Collection
  - Netflow Analysis
  - Service Availability Monitoring
- Security Intelligence / SIEM
  - SIEM Event Correlation
  - Incident Response

Ready to try AlienVault USM? Download our free 30-day trial today.
AlienVault USM: How it Works

AlienVault USM is comprised of three core components:

**AlienVault Sensor**: Sensors perform four of the five essential capabilities of AlienVault: Asset Discovery, Vulnerability Assessment, Threat Detection, and Behavioral Monitoring. Sensors receive raw data from event logs, monitor network traffic, and activate discovery and vulnerability scans. Sensor Processes perform initial processing (normalization) on that raw data, then transmit normalized events to the AlienVault Server for correlation and reporting.

**AlienVault Server**: The AlienVault Server provides a unified security management and configuration capability for all monitored assets. The Server receives normalized data from one or more Sensors, correlates and prioritizes the security events occurring across all assets, then displays these as alarms and security events in a variety of summary and detailed reports and dashboard views.

**AlienVault Logger**: The AlienVault Logger provides the Server with the ability to archive log files for purposes of forensic analysis and to fulfill compliance requirements for log archival and management.

AlienVault Labs Threat Intelligence

Cyber criminals and attackers are constantly evolving their methods, that’s why your AlienVault USM implementation is fueled with emerging threat intelligence from AlienVault Labs. AlienVault Labs curates raw threat data from more than 9,500 global collection points across 140 countries to deliver the following dynamic content:

- **Network and host-based IDS signatures** – detects the latest threats in your environment
- **Asset discovery signatures** – identifies the latest OS’es, applications, and device types
- **Vulnerability assessment signatures** – dual database coverage to find the latest vulnerabilities on all your systems
- **Correlation rules** – translates raw events into actionable remediation tasks
- **Reporting modules** – provides new ways of viewing data about your environment
- **Dynamic incident response templates** – delivers customized guidance on how to respond to each alert
- **Newly supported data source plug-ins** – expands your monitoring footprint

Malware changes fast! Stay informed subscribing to the OTX Threat Newsletter. You’ll get the AlienVault Labs research team’s thoughts on emerging global threats and how to defend against them.
About AlienVault

At AlienVault, we believe that open and collaborative is the best way for all companies to gain the security visibility they need. Built on proven security controls and updated continuously with the latest threat intelligence, AlienVault’s Unified Security Management™ (USM) platform provides a complete, simple and affordable way for organizations with limited security staff and budget to address compliance and threat management. With the essential security capabilities already built-in, USM puts enterprise-class security visibility within easy reach of security teams who need to do more with less. For more information visit www.AlienVault.com or follow us on Twitter.