AlienVault SIEM

It is possible to have too much of a good thing – too much security data and tool management overhead often overwhelms operations, actually obscuring security. There's too much hay to spot the needle.

AlienVault's SIEM, the cornerstone of the Unified Security Management (USM) Platform combines Security Automation, Unified Management, and Shared Intelligence to correlate data, to spot anomalies (the needle in the hayfield), reduce risk, and improve operational efficiency.

Security Intelligence is the cornerstone of the Unified Security Management (USM) platform. USM enables you to more easily and efficiently configure, manage, and operate the five 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.

Security Automation—Reduces the time spent investigating security incidents

AlienVault offers superior security automation to standard SIEM event correlation. Like others, it collects, normalizes, and correlates events from your environment to detect security risks and breaches. It also leverages the threat, vulnerability, and asset information as context to offer a more comprehensive accurate assessment of security incidents. Moreover, the two way data flow between event correlation and the integrated USM security controls provides dynamic event validation to automate the initial steps of incident response. AlienVault's comprehensive security automation produces highly accurate, actionable alerts allowing analysts to spend less time tuning the system and investigating false alarms and more time preventing attacks.

Unified Management—Reduces security total cost of ownership

Unified management reduces complexity and simplifies operation of the USM. This allows security experts to spend more time doing what we need them to do; securing the systems, not managing their tools. Easily navigating between event status and the full suite of USM security tools makes it easier for the user to identify an attack, ascertain its success, determine the extent of the compromise, and isolate the breach. A unified reporting framework can create dashboards and generate reports based on any part of the system.

Shared Intelligence—Enables a collaborative defense, improving security

AlienVault's Open Threat Exchange™ (AV-OTX™) enables anonymous sharing of threat intelligence. AV-OTX™ shares and receives threat updates from installations across more than 50 countries. When an attack is observed by an OTX participant the information is sent to AlienVault Labs for validation and is distributed to all other OTX participants. A collaborative defense model offers AlienVault users an improved level of security over standalone alternatives.

SECURITY INTELLIGENCE

Security Intelligence in Action

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 internal host. A lookup in an asset database automatically identifies the risk profile of the internal host - the host is critical to business operations creating a critical security incident. The compromised host is then scanned for other vulnerabilities and it found to be missing a critical security patch. The compromised host is patched and returned to service. A complete forensic analysis for the past 30 days is run for the compromised host to determine if additional corrective action is required. The incident is automatically reported the AlienVault Labs OTX so other OTX-enabled AlienVault installations are protected from a similar exploit. The whole process is run from AlienVault's USM unified management console.

	FEATURE	BENEFIT
UNIFIED MANAGEMENT	Unified Management of Security Tools	Reduced cost of ownership through central monitoring and configuration for Sensors, Agents, and Logger.
	Multi-Tenant Management	Roll-based management allows separation of duties mandated IT organizational requirements and/or regulatory bodies.
	Over 100 Pre-Defined Compliance & Threat Reports	Easily generate reports for incidents, alarms, vulnerabilities, trouble tickets, assets, service availability, and network health.
	Wizard-Driven Custom Reporting	Rapidly fulfill an organization's unique compliance and operational reporting requirements.
	Over 2500 Report Modules	Reduced time spent on creating custom reports by reusing modules of existing reports.
	Configurable & Extensible Dashboards	Creates custom views of threat, compliance, and operational data for each user.
	3D Visualization Support	View 3D network and security applications like Geo-location and botnet maps.
	Open Extension API	Integrate other open source or commercial best of breed security and operational tools into the unified security management platform.
SECURITY AUTOMATION	Real Time Correlation	Improves productivity of security operations by converting raw events into actionable alerts.
	Over 600 Pre-Defined Correlation Rules	Reduces time required to automate security operations.
	Wizard to Create Custom Correlation Rules	Easily create correlation rules to meet the specific security and compliance requirements of your organization.
	Contextual Behavior Analysis	Assess the risk of the anomalous activity by correlating it to environmental information like importance of the asset.
	Pattern Recognition & Behavior Analysis	Accelerates corrective action by correlating current threat intelligence with the security incident.
	Dynamic Event Validation	Automates initial troubleshooting by querying built-in security tools to gather more information on status of network and assets.
SHARED INTELLIGENCE	Interface to Open Threat Exchange (OTX)	A security community watch program to ensure your security systems always have the latest intelligence.

AlienVault™
WWW.ALIENVAULT.COM