

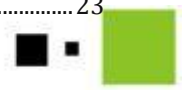


AlienVault SIEM System Description

© COPYRIGHT ALIENVAULT 2010



INTRODUCTION	4
ARCHITECTURE	5
Components	5
Sensors	5
Collectors	6
SIEM.....	7
Logger	7
Scalability and Performance.....	7
Distributed Topologies and Load Balancing	7
Performance	8
High Availability.....	9
Role Management and Multi-Tenancy	9
REPORTING.....	10
Dashboards	10
Predefined Reports.....	11
Custom Reports.....	12
Scheduling	14
3D Visualization	14
SIEM	15
Intelligence.....	15
Risk Assessment	15
Correlation	16
Logical correlation	16
Cross-correlation.....	17
Inventory correlation	17
Daily Feed Subscription.....	17
Real Time Policy Manager	17
Collection	18
Methods	18
Data Source Connectors / Collection Plugins	19
Custom Collection	19
Analysis	19
Forensic Analysis.....	19
Drill-Down Analysis	20
Risk Oriented Analysis	20
Alarms	21
Search Capacities.....	21
Automatic Analysis.....	22
Real Time Analysis.....	23



Incident Management	23
Ticket System	23
Knowledge Base	24
Asset Management	24
Asset Structure	24
Automated Asset Inventory	25
Network Discovery	26
Asset Topology Maps	27
Availability and Resource Monitoring	27
Network Profiling	29
Configuration Management	29
LOGGER	30
Unlimited Storage	30
Legal Integrity	31
COMPLIANCE AUTOMATION	31
Custom Compliance	31
SITUATIONAL AWARENESS	33
Network Profiling	33
Bandwidth and Flow Monitoring	33
Inventory Monitoring	34
Availability and Resource Monitoring	34
DETECTION	34
Intrusion Detection and Prevention (IDS and IPS)	34
Anomaly Detectors, NBA	34
Host Security / Endpoint Security	35
AUDIT	36
Vulnerability Assessment	36
Job Management	37
Threats database	37



Introduction

The AlienVault Professional SIEM® is a family of Security Information and Event Management solution (SIEM) products. SIEM products are designed to provide a framework for control of information security infrastructures. The AlienVault Professional SIEM achieves these goals by integrating an unlimited range of security and network tools into a single management interface.

The AlienVault professional SIEM is based on the Open Source Security Information Management tool (OSSIM), created and developed by AlienVault. This document describes the AlienVault professional SIEM version which includes OSSIM functionality as well as enterprise-level performance, reliability, forensics, reporting, contextual correlation, quality assurance, scalability and support.



The Technology

AlienVault Professional SIEM technology offers advanced intelligence capable of synthesizing the underlying risks associated with complex distributed attacks on large networks. The system considers the context of each threat and the importance of the assets involved, evaluates situational risk, discovers network inventory and distinguishes actual threats from the thousands of false positives that are produced each day in every network.

The AlienVault Professional SIEM features:

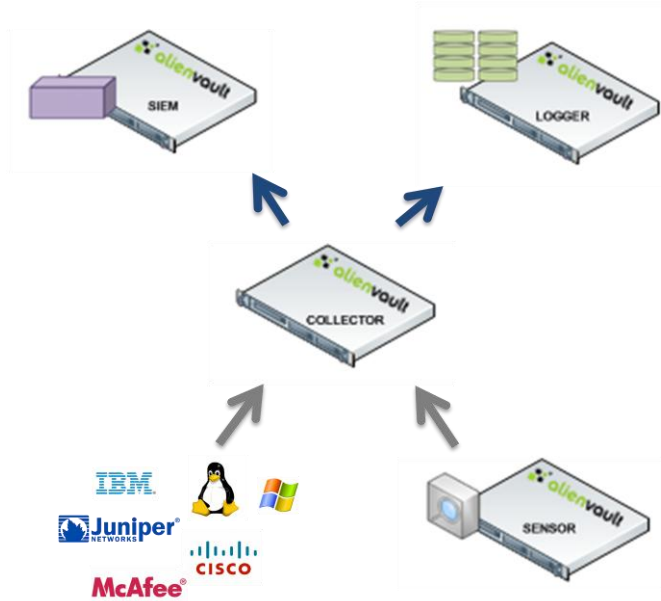
- Compliance automation
- Low level real-time detection of threats and anomalous activity
- Network, host and policy auditing
- Contextual network behavior analysis
- Forensic log management
- Risk-oriented security analysis
- Executive and technical reports
- Scalable high-performance architecture



Architecture

Components

In order to integrate and analyze the information generated by every type of application or device, the AlienVault Professional SIEM supports a distributed architecture organized in four components as shown below:



AlienVault Professional SIEM ships as a family of appliances optimized to enable efficient deployment and expansion of any size, from single-appliance implementations to distributed deployments of unlimited scale.

Sensors

AlienVault Sensors have been designed for managing security. Each Sensor collects a wide range of information about its local environment, processes this information and coordinates detection and response with the rest of the distributed AlienVault deployment. An individual AlienVault Sensor compiles an arsenal of security technology into a single device: the combined effect of numerous detection and control points being global visibility and compliance management available to operations and executive staff.

AlienVault Sensors are installed on network segments and remote locations, inspect all traffic, detect attacks through various methods and collect information on attack context without affecting network performance.



AlienVault sensors utilize more than ten expert systems that identify attacks along five different axes:

- Intrusion Detection
- Anomaly Detection
- Vulnerability Detection
- Discovery, Learning and Network Profiling
- Inventory Management

AlienVault's technology locates both known and unknown attacks in near-real time by way of the Learning Engine and Anomaly Detection intelligence built into the products.

Vulnerability Detection systems discover and identify latent network threats and can correct them before an attack occurs. This information, stored by the Management Server, is of vital importance when an attack is in progress. Prior knowledge of vulnerabilities in systems is critical when assessing the risk associated with an attack, prioritizing, alerting, and launching countermeasures.

The network information gathered by AlienVault Sensors provides detailed status in near real-time regarding network usage of each host and stores this data for analysis. Every AlienVault deployment automatically creates a highly detailed usage profile of each element on the network it is monitoring.

Collectors

AlienVault Collectors gather the events generated by the AlienVault Sensors and any external system. Collectors classify and normalize the events before sending them to the AlienVault SIEM and Logger. In order to support the maximum possible number of applications and devices, collectors use Data Source Connectors (also called Collection Plugins):

- Each Connector defines how events generated by each device will be collected and normalized
- Connectors can be configured using a simple configuration file and regular expressions to define the format of each type of event
- The Collector component can be deployed as a standalone system or included in the Sensor or SIEM appliance, depending on the performance need



SIEM

The SIEM component provides the system with Security Intelligence and Data Mining capacities, featuring:

- Risk Assessment
- Correlation
- Risk Metrics
- Vulnerability Scanning
- Data Mining
- Real-Time Monitoring

The AlienVault SIEM component uses an SQL database which stores normalized information, allowing strong analysis and data mining capabilities. AlienVault Professional SIEM is tuned for high performance and scalability of many million events per day.

Logger

The Logger component stores events in raw format in a forensically secure appliance. Events are digitally signed and stored ensuring their admissibility as evidence in a court of law. The logger component allows storage of an unlimited number of events for forensic purposes.

Logger should be deployed in a fashion that ensures optimal “Chain of Custody” management, and is capable of supporting encrypted communications from the originating device where that device supports the ability. The OpenVPN client is included with AlienVault Logger can be used to create a secure channel for events from host sources.

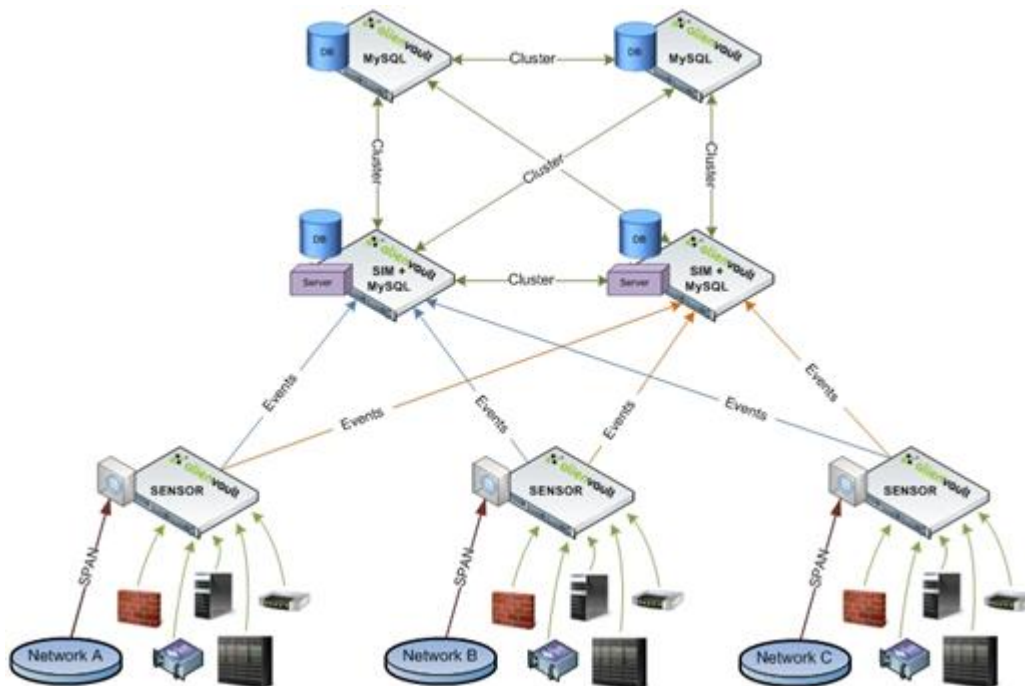
Scalability and Performance

Distributed Topologies and Load Balancing

For large, distributed networks, multiple SIEM, Sensor, Collector and Logger components can be deployed without limit. The AlienVault Professional SIEM architecture supports fully customizable, multi-hierarchical, multi-tenanted deployments such that data from hundreds of thousands of workstations can be easily monitored and synthesized.

Responsibility for analysis and storage of information can be assigned to different nodes which report up to a central system that in turn provides a global view of enterprise information risk at any given moment from a single console.





AlienVault Professional SIEM allows for both horizontal and vertical load distribution. This architectural flexibility also enables highly customizable and scalable management scenarios.

- Horizontal distribution of security information is useful for high performance and high availability configurations
- Vertical distribution will allow different levels of abstraction and reporting

For example, groups of management servers may be organized to create multiple hierarchies of management servers. This sort of architecture facilitates monitoring of large, distributed networks and makes it possible to create various levels of correlation and storage.

Each of these hierarchies can then be rolled up into a global view that serves as a central console from which activity on any part of the network can be seen at any time, down to the smallest detail.

Performance

AlienVault Professional SIEM is capable of handling very large volumes of data. The engineering team at AlienVault has structured the system architecture with multiple optimizations and load distribution layers so that the AlienVault Professional SIEM now offers 30 times the performance of OSSIM in each of its components.



AlienVault Appliances have been tested in independent laboratories offering the following results:

Component	Performance per device
SIEM	5.000 EPS
Logger	15.000 EPS
Sensor	1 Gbps

Distributed deployments have been tested reaching the following performance levels:

Component	Global Performance
SIEM	200.000 EPS
Logger	1.000.000 EPS
Sensor	100 Gbps

High Availability

The system offers high availability capabilities in all the components using the distributed and balanced configurations as shown previously.

Active-active as well as active-passive configurations are possible using load balancing and heart-beat HA configurations.

Role Management and Multi-Tenancy

With the AlienVault Professional SIEM, user permissions can be set based on the strong asset management built into the product. The asset structure defines asset objects ranging from entire companies to single IP addresses or group of hosts. This allows administrators to easily configure the system using abstractions as well allowing a deep specificity of role management.

User role profiles are defined to provide three axes of permissions:

- Functionalities a user can access on the system
- Assets that are accessible for each type of functionality

This Role-Based management allows the separation of duties mandated by regulatory bodies, best practices and industry standards. Managers are provided global visibility while technicians might only have access to technical information for specific systems, for example.

This system of controls allows the AlienVault Professional SIEM to fit perfectly into MSSP environments. Multiple customer environments with overlapping IP address spaces and strict confidentiality requirements are easily and verifiably accommodated.



Reporting

AlienVault Professional SIEM includes a powerful reporting system. Reports are generated based on all the information collected and generated by the system including historical and real time data.

AlienVault ships with over 200 well-categorized reports (Availability, Security, Vulnerability Analysis ...) which users can customize and duplicate to fit their particular environment. A sophisticated Report Wizard makes ad-hoc creation of reports of any nature straight-forward while delivering the granularity of detail and presentation values necessary to meet enterprise and MSSP needs. Reports can be output in PDF, HTML, and Microsoft Word® format and delivered via email either by schedule or manually.

Dashboards

Each user account holder in an AlienVault deployment can configure his or her own dashboard panel through the web interface. Graphs or indicators that are of interest to the user and are within the user's permissions can be arranged to fit the needs of the environment.

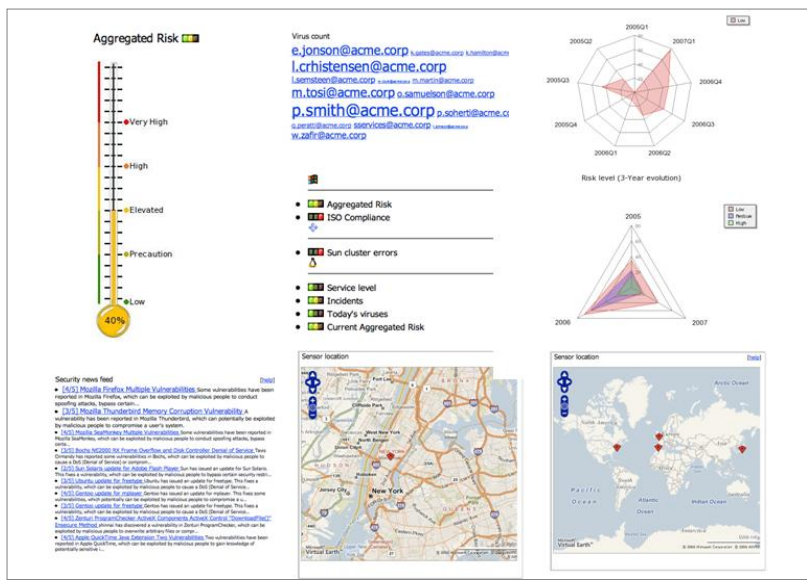


A plugin-based system allows users to import and export different objects into the dashboard of each user. The objects in the dashboard can be easily configured using a wizard that allows the following content and more:

- Graphs and metrics from a SQL query
- HTML Content



- Feed Atom / RSS
- Predefined Charts
- Metrics
- Tag-clouds

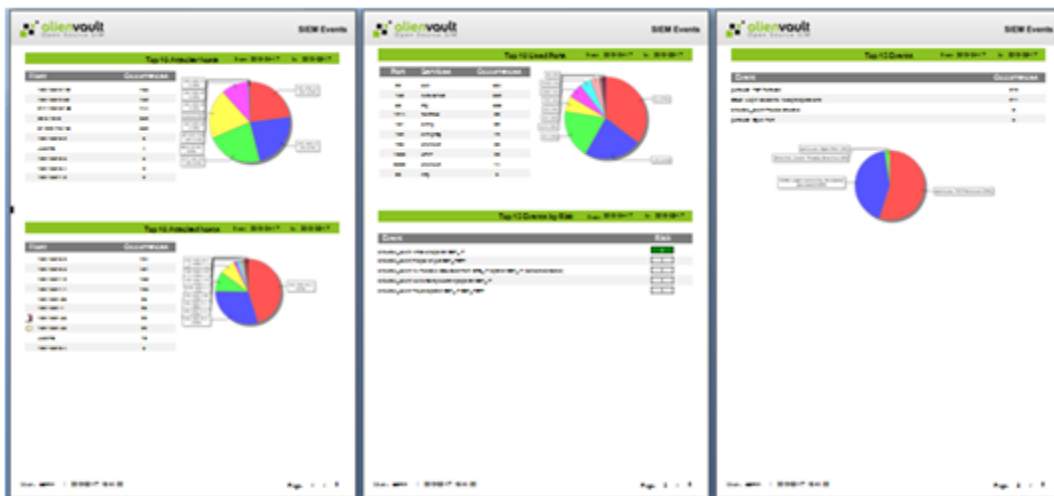


Predefined Reports

The system includes more than 200 of predefined reports classified into the following categories:

- Security
 - SIEM DB
 - Logger DB
 - Alarms
- Incidents
- Vulnerabilities
- Availability
- Network Statistics
- Asset information and Inventory
- Ticketing system
- Network





Custom Reports





Each user is able to create and save his or her own reports. Any or all of these reports may or may not be shared with other users on the system at the user's discretion. For example, a user can choose to share a report only with users that belong to their department, to everyone in their company, or to those monitoring the same assets in the corporation.

The report creation process is simple. The user will also be able to select the time period that will be included in the report as well as the appearance of the report.



Custom parameters

Name:

	Background Color	Foreground Color
Title		
Subtitle		
<input type="button" value="Restore Original"/>		

* Click To Zoom

* Only .gif, .png and .jpg files

Left footer:

Right footer:

Creating new report Designs

If the user needs to define subreports and a complete new report style it can be done with Jasper Reports ETL reporting system included in AlienVault.

The reporting systems is Based in Jasper, an Open source report engine which generates reports designed with iReport, displays them on screen or exports them in a final format like PDF, OpenOffice, DOCX and many others.

AlienVault Professional SIEM includes JasperServer to provide: the functionality necessary to manage, schedule, and run the reports; a repository to store all the report resources such as images, fonts, data sources and much more; a security service to decide who can execute which report; and a web services API to execute the reports from external applications (so you can generate reports from any kind of environment, like PHP or .NET).

When you design a report using iReport you are creating a JRXML file, which is an XML document that contains the definition of the report layout. The layout is completely designed in a visual way, so you can ignore the real structure of the JRXML file. Before executing a report, the JRXML must be compiled in a binary object called a *Jasper file*.

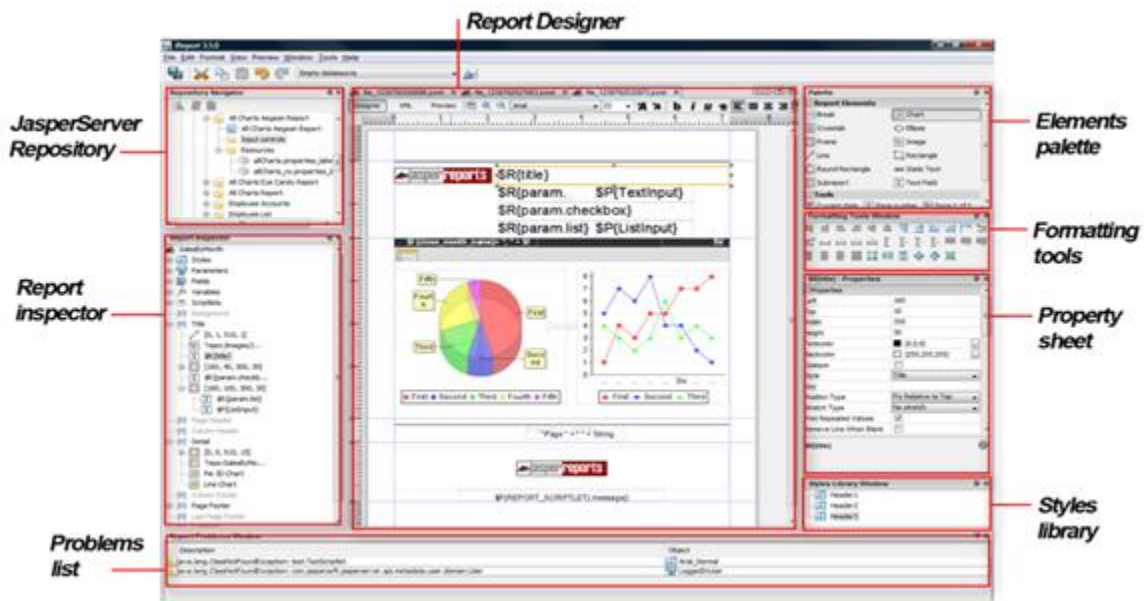
The reports life cycle is:

Report Design with iReports

Reports can be designed from scratch or from one of the many ready-to-use templates that are available. iReport will assist designers during all the phases of the report development: JRXML design, Jasper compilation, report execution, and document export or visualization. The figure below shows the main user interface components of iReport.

- Create the report from AlienVault front-end
- Select the template
- Select Controls and Resources
- Assign the data source
- Define the query
- Customize the report



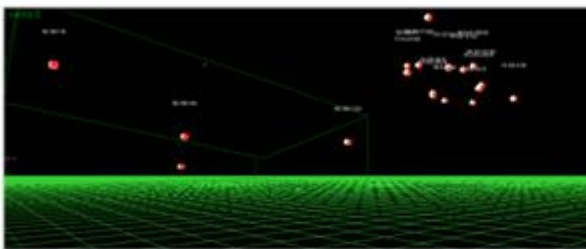


Scheduling

Reports can be scheduled so that they are generated automatically at a given time. Once the report has been created, they can be sent to an email address or external repository.

3D Visualization

AlienVault has developed a number of 3D visualization tools, which it implements as specific projects for SOC's and MSSP's.



3D Visualization



World Botnet map 12/9/200



Geo Localization

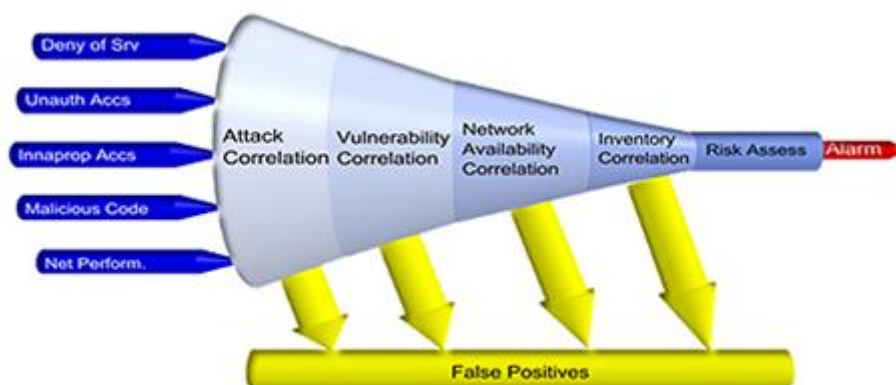


SIEM

Responding effectively and on a timely basis to threats requires the analysis of an enormous number of events collected continuously. Without an automated tool to help enterprise find patterns, filter, clean and analyze all the data that form the context of an attack, the task of protecting the organization becomes exceedingly complex, time-consuming and resource intensive. The AlienVault SIEM solution provides intelligence through continuous collection, correlation and analysis of events from multiple data sources which it then analyzes and either prioritizes or rules out as a possible attack.

Intelligence

AlienVault's intelligence excels at complex situation analysis. Four levels of correlation combine with near-real-time risk assessment for each event received provides a powerful engine for extracting tactical and strategic information. The AlienVault correlation engine is able to track complex patterns and includes in its analysis all the variables that define context. These include: vulnerability of targeted asset; degree of anomaly in associated traffic over time; current and historical network status; service availability; network inventory and topography; and value of the assets involved.



Discovering and tracking new patterns is fundamental to the task of identifying the distributed or abstract attacks that classic detection systems miss. A number of powerful threat mitigation tactics are made possible through the correlation of context data. For example, combining knowledge of known vulnerabilities, inventory and asset value with network data allows for filtering out attacks that will not affect a target, prioritizing attacks involving known-vulnerable service and for monitoring the status of a network subject to a denial of service attack.

Risk Assessment

This understanding of context information allows the AlienVault Professional SIEM to maintain a highly accurate risk assessment. Decisions made concerning immediate threats must always be performed on the basis of thorough analysis of risk parameters such as the asset value at risk, the nature and degree of the threat to which it is subjected and the reliability of the data used to identify the attack. Risk assessments performed to this level allow for differentiation between an attack on a critical system and one targeting a development system.



Correlation

AlienVault Professional SIEM includes a powerful correlation engine which performs analysis of billions of events. The purpose of the correlation engine is to reduce this torrent of information into a manageable number of actual incidents that require human operators, and to offer detailed information on those to the operator.

In the process of performing their function, IDS and other security devices create an enormous volume of false-positive indicators. With today's 7x24 threat landscape, it is impossible for any human operator to manually react to each of these, therefore real compromises are overlooked.

AlienVault correlation directives check these events by looking for evidence to verify if they are real or not. By default we give a low value to the "Reliability" parameter of most events, which will only grow as far as the checks within the correlation engine produce positive results.

After a possible Trojan or exploit attempt, for example, a correlation directive will check if an attack response signature is produced by the attacked host. It will also check if the channel persists in terms of time or transmitted data and if the attacked machine behaves anomalously during the following hours. As each of these checks becomes positive the system's awareness that it is dealing with a real attack is increased. At configurable thresholds, the system creates an Alarm and presents the human operator with the details of the incident.

AlienVault Professional SIEM uses three forms of correlation. Correlation directives are executed using Logical Correlation. Inventory Correlation and Cross Correlation are also very efficient false-positive killers on the data landscape. These three methods are described below.

Logical correlation

The primary purpose of Logical Correlation is to determine if a security event is accurate or whether it is a false positive. Of millions of events a day on an average network almost all of them will be false positives.

AlienVault's Logical Correlation engine features:

- Hybrid source, accepting both pattern input from detectors and indicator input from monitors
- Recursive architecture: the output of the correlation process is events which are correlated again by other Correlation Directives
- Hierarchical distributed architecture: define n levels of correlation in a distributed topology
- Flexible object-oriented and time range definitions for each directive stage
- Implemented by *Correlation Directives* which implement a tree of logical condition nodes

The system includes more than 500 preset Correlation Directives. A Daily Feed from AlienVault's Vulnerability Research Team updates directives with intelligence on current attacks.

User-defined Correlation Directives are easily created using the interface, either by duplicating and modifying existing Directives or from scratch based on live context from the installed environment.



Cross-correlation

Cross Correlation allows AlienVault to prioritize or deprioritize events for which targets are or are not vulnerable to by correlating information from Detectors and Vulnerability Scanners.

Inventory correlation

AlienVault's Inventory Correlation checks if the attacked machine uses the OS and/or service for which the attack is designed. Where an attacked machine uses the OS or service it can be confirmed that a risk exists, if not it can be confirmed that the event is a false positive.

Daily Feed Subscription

The AlienVault Professional Feed helps your organization stay up to date with the latest enterprise threats through the expertise of the AlienVault VRT (Vulnerability Research Team), a group of security experts that analyze and respond to the latest trends in risk.

Subscribers to the Professional Feed receive immediate access to:

- Certified Correlation Rules: The newest certified directives as soon as they are released.
- Predefined Policies: Each designed to address requirements common to numerous enterprise scenarios
- Compliance Requirements: Intelligence that facilitates compliance with PCI, ISO 27001 and other regulatory processes
- Cross Correlation and Inventory Correlation updates
- Priority and Reliability updates for new and old plug-ins
- Feed Support: Answers to your question quickly and easily

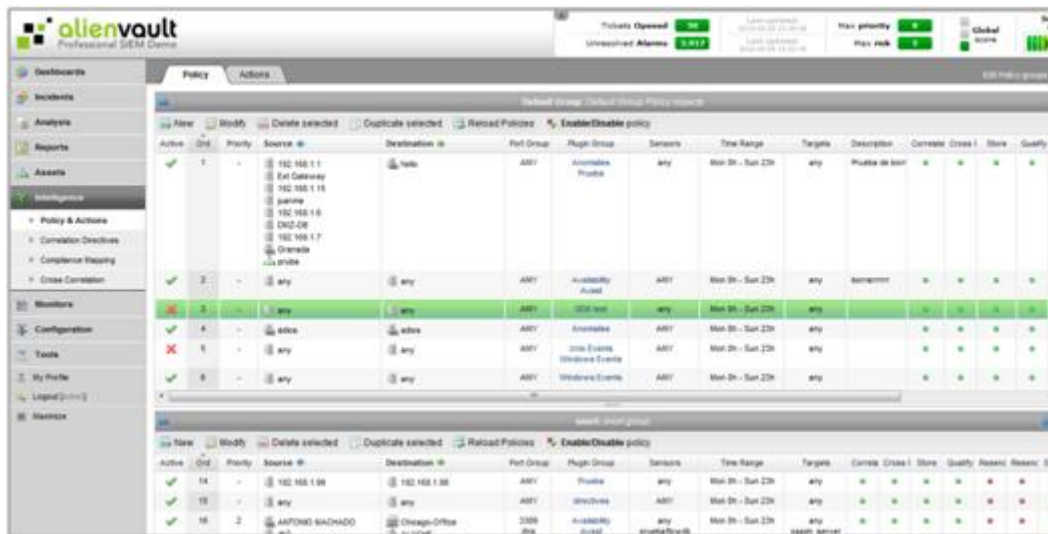
Real Time Policy Manager

Using policies in AlienVault Professional SIEM it is possible to easily tune system behavior and create exceptions appropriate to a given environment. Operators are able, for any specific event, to:

- Calculate a risk for the event
- Correlate the event
- Forward the event to another server
- Execute an action (send an e-mail, run a command,...)
- Store the event

For example, the system can be configured so certain events will only be stored for a given time and so other events will have greater importance when they occur in relation to a specific machine.





Active	ID	Priority	Source IP	Destination IP	Port Group	Plugin Group	Sensors	Time Range	Targets	Description	Correlate	Create	Store	Quality
✓	1	-	192.168.1.1 Ext Gateway 192.168.1.18 joomla 192.168.1.6 DN2-08 192.168.1.7 Oranville JJA-SNBA	any	ANY	Availability Probe	ANY	Mon-Sat - Sun 23h	any	Planta de San	✓	✓	✓	✓
✓	2	-	any	any	ANY	Availability Audit	ANY	Mon-Sat - Sun 23h	any	Sansemm	✓	✓	✓	✓
✗	3	-	any	any	ANY	SQL tool	any	Mon-Sat - Sun 23h	any		✓	✓	✓	✓
✓	4	-	adms	adms	ANY	Availability	ANY	Mon-Sat - Sun 23h	any		✓	✓	✓	✓
✗	5	-	any	any	ANY	SQL Events Windows Events	ANY	Mon-Sat - Sun 23h	any		✓	✓	✓	✓
✓	6	-	any	any	ANY	Windows Events	ANY	Mon-Sat - Sun 23h	any		✓	✓	✓	✓
✓	14	-	192.168.1.88	192.168.1.88	ANY	Probe	any	Mon-Sat - Sun 23h	any		✓	✓	✓	✓
✓	15	-	any	any	ANY	Windows	ANY	Mon-Sat - Sun 23h	any		✓	✓	✓	✓
✓	16	2	ASFORNS BACHADO ad	Chicago-Office ad	3389	Availability Audit	any snmpTool	Mon-Sat - Sun 23h	any	ASFORN BACHADO	✓	✓	✓	✓

Collection

AlienVault SIEM collects and analyzes logs coming from AlienVault Sensors or from any number or type of network devices such as firewalls, IPS, routers and switches, operating systems or applications.

Distributed hierarchical collection architectures can be deployed such that data from hundreds of thousands of workstations can be easily monitored and synthesized. Responsibility for analysis and storage of information can be assigned to different nodes which report up to a central system, which in turn provides a global view of enterprise information risk at any given moment.

Methods

The system can collect events using one of the following methods:

- Syslog and Syslog-ng
- SNMPv2 and SNMPv3
- Opsec
- HTTP
- SQL, ODBC
- WMI
- FTP, SFTP
- Socket Unix
- Plain log
- SSH
- Rsync
- Samba
- NFS
- SDEE, RDEP
- OPSEC, CPMI

The modularity of the system allows for easy implementation of any other collection method.



Data Source Connectors / Collection Plugins

AlienVault includes over 3,200 Connectors that allow the collection of information from different data sources including a broad number of operating systems, devices and applications.

The most recently updated list of supported devices and applications can be found at the following URL:

<http://www.alienvault.com/community.php?section=Plugins>

If you cannot find your device or application on the list, contact AlienVault to determine if it has already been created. Plugins can be easily created by the user, and AlienVault and the open source community continually add more.

Custom Collection

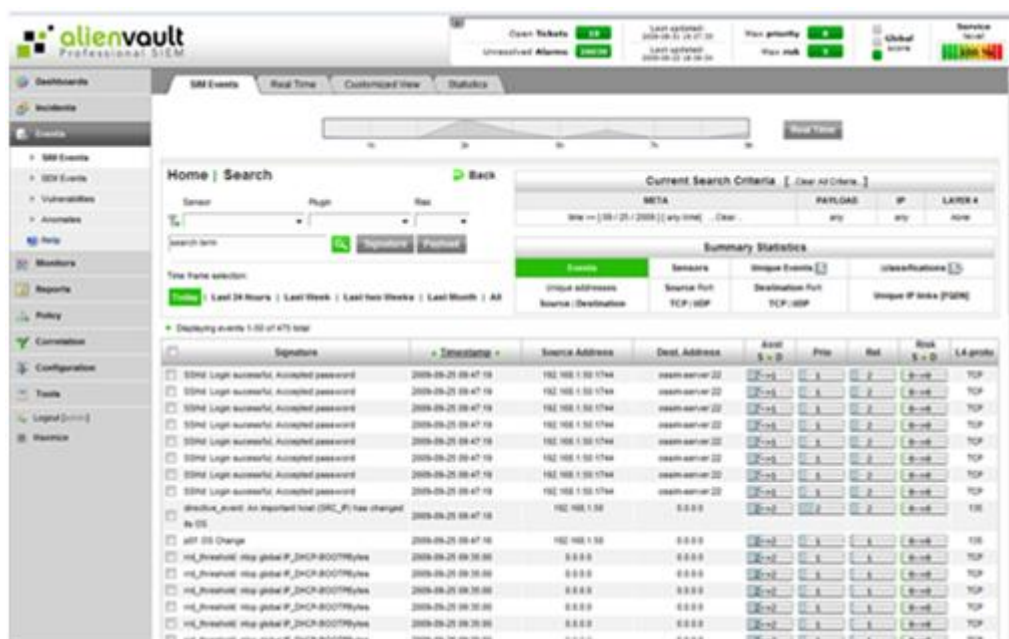
Custom-defined logs can be easily collected by creating new Connectors using a simple language. The creation of Connector requires a simple technical knowledge of the event format to create the normalization patterns necessary to process the new logs.

Analysis

Forensic Analysis

Information collected by the Management Server is stored securely and may be consulted to determine how a given system, device or other asset has been used, by whom, and when.

The analysis capabilities allow the operator to easily drill down and narrow the search of a pattern by choosing the predefined security analysis search filters.



Drill-Down Analysis

The system provides a robust ability to drill-down from higher level information to a more detailed and specific view of an event.

Every piece of information about an incident is linked, allowing immediate and unlimited drill-down. The right button allows access from any screen of the system to all the information gathered by the system for an asset, including:

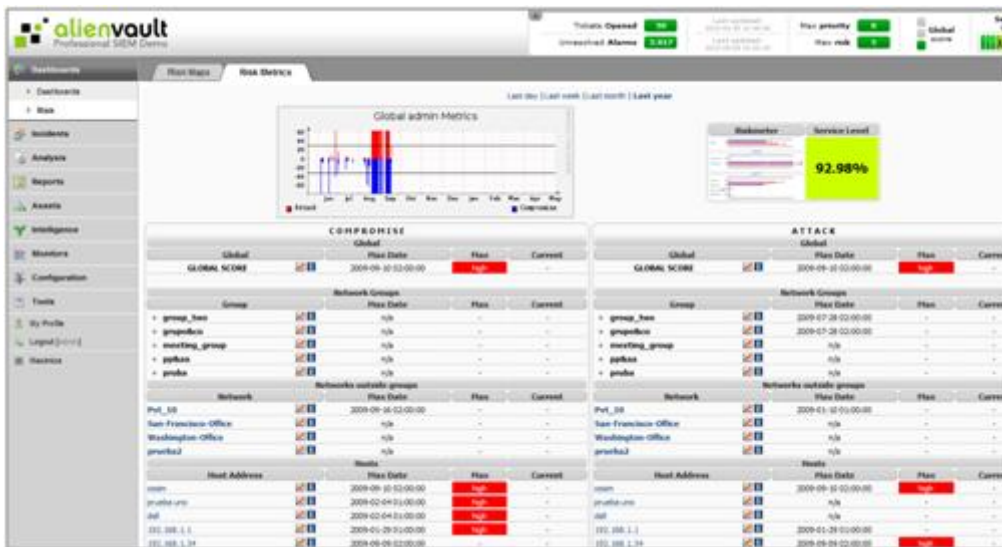
- Events, Alarms
- Incidents and related tickets
- Knowledge based information
- Vulnerabilities
- Asset information such as:
 - Inventory
 - Network
 - Profile information
 - Availability
 - Resource utilization



Risk Oriented Analysis

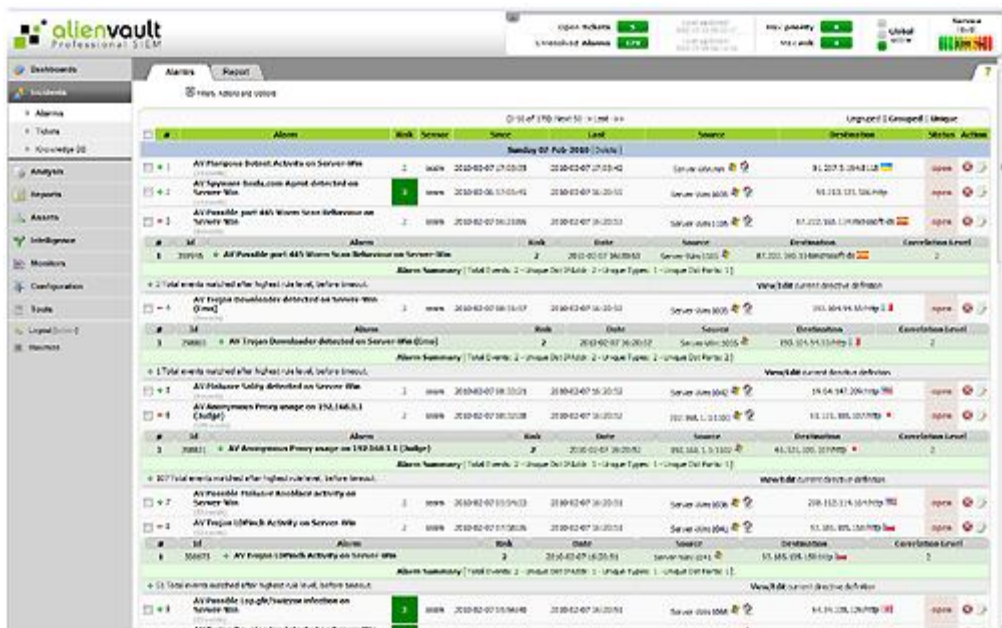
The AlienVault Professional SIEM calculates the risk of each of the billions of event it collects and reports that risk associated with the target asset value, the probability of the risk being realized and the impact value of the risk. The entire process is driven by this risk assessment: triggering automatic responses; alarm reporting; and the aggregate risk status of networks. The effectiveness of administration, tuning and forensic procedures performed with the system are enhanced by this holistic risk assessment process.





Alarms

The alarms panel shows the important events which have happened in the last day. Here is where the magic happens, reporting a maximum of a dozen alarms from millions of collected events.



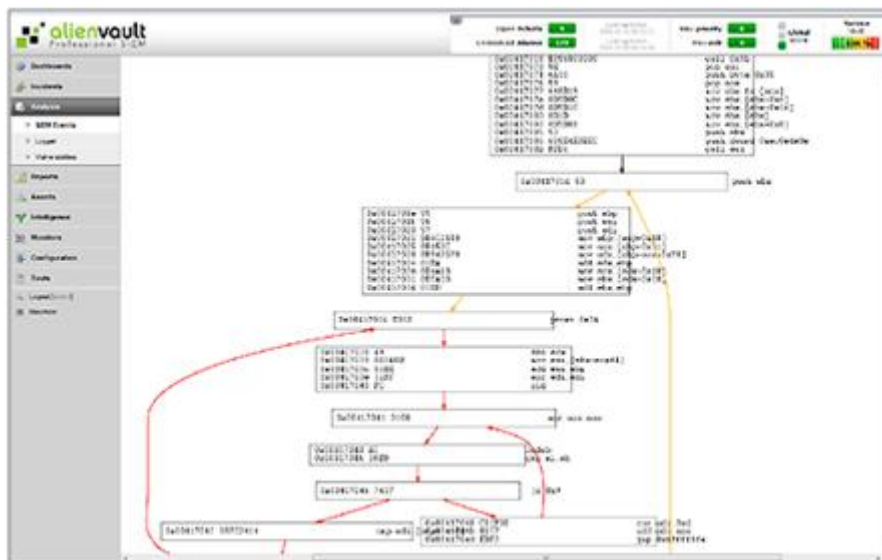
Search Capacities

Strong search capacities are offered by the system allowing complex queries.



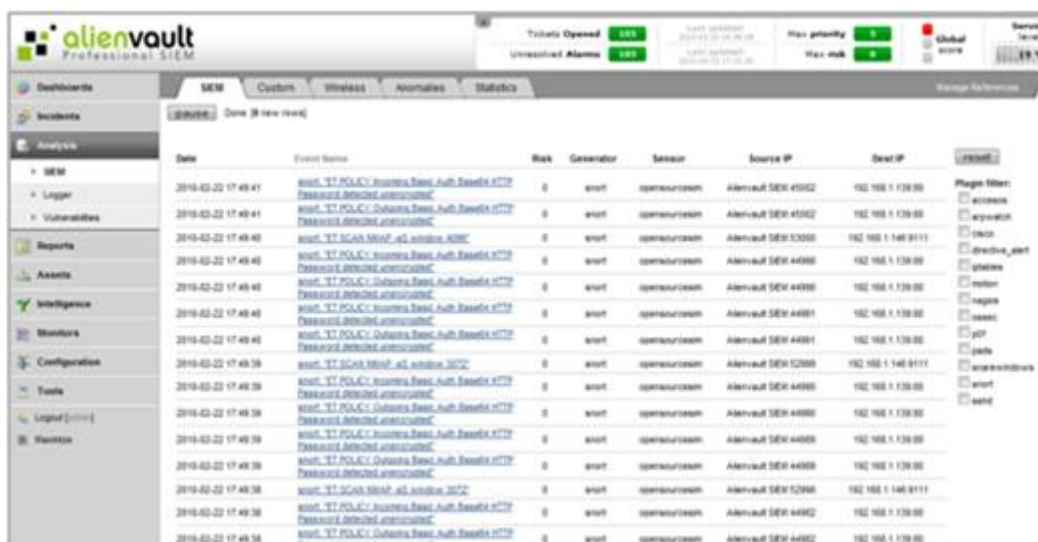
Automatic Analysis

AlienVault includes specialized security analysis tools in sandboxes which allow decompiling malware and shell code attacks.



Real Time Analysis

The real-time panel shows the events in real time as they are received by the system. A filter allows focusing on specific data sources.



Date	Event Name	Risk	Generator	Sensor	Source IP	Dest IP
2010-02-22 17:49:41	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4302	192.168.1.139:80
2010-02-22 17:49:41	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4302	192.168.1.139:80
2010-02-22 17:49:40	Alert: ST.SCAN: MySQL aL sensitive (300)	0	snort	opencourtesy	AlienVault SEW 5200	192.168.1.146:8111
2010-02-22 17:49:40	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4300	192.168.1.139:80
2010-02-22 17:49:40	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4300	192.168.1.139:80
2010-02-22 17:49:40	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4301	192.168.1.139:80
2010-02-22 17:49:40	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4301	192.168.1.139:80
2010-02-22 17:49:39	Alert: ST.SCAN: MySQL aL sensitive (300)	0	snort	opencourtesy	AlienVault SEW 5200	192.168.1.146:8111
2010-02-22 17:49:39	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4300	192.168.1.139:80
2010-02-22 17:49:39	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4300	192.168.1.139:80
2010-02-22 17:49:39	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4300	192.168.1.139:80
2010-02-22 17:49:39	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4300	192.168.1.139:80
2010-02-22 17:49:39	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4300	192.168.1.139:80
2010-02-22 17:49:38	Alert: ST.SCAN: MySQL aL sensitive (300)	0	snort	opencourtesy	AlienVault SEW 5200	192.168.1.146:8111
2010-02-22 17:49:38	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4302	192.168.1.139:80
2010-02-22 17:49:38	Alert: ST.POLICY: Outgoing Basic Auth Success (177)	0	snort	opencourtesy	AlienVault SEW 4302	192.168.1.139:80

Incident Management

AlienVault Professional SIEM includes an Incident Manager which controls the assignment of all the actions resulting from security events. It includes also a Knowledge Database in which all the information learnt from previous incidents as well as remediation procedures can be stored and referenced in order to “learn from the past”.

Ticket System

The Ticket System allows the creation of tickets from most of the AlienVault reporting tools such as the Alarm Panel, the Forensic Console or the Risk Dashboard.

Each ticket shows a Person in charge, Status, Actions to be taken and tracks the workflow from the creation of the ticket to the final resolution.

All tickets are stored in the Database and a search tool allows filtering them. It is also possible to report on incident trends and implement Metrics to measure the situation at the present moment and track the evolution over time.





Knowledge Base

The knowledge base allows storing and linking with the ticket system:

- Procedures
- Technical documents
- Maps, images, etc
- Threat Information

The database provides the following linking capabilities:

- Assets
- Tickets
- Images
- Users
- Keywords

Asset Management

Asset Structure

The AlienVault Professional SIEM allows for the creation of complex asset hierarchies to describe the structure of a company as a tree with different levels:

- Company
- Departments
- Network Group
- Network
- Host Group
- IP's

These asset objects can be used in any part of the system to easily define the range of action desired whether it is report visualization, policy implementation or permission definition.



Automated Asset Inventory

Inventory information is a basic source used by the system to implement security intelligence. AlienVault Professional SIEM has a strong inventory capability using a variety of techniques and methods, including:

- Network Scanning Inventory
- Passive Sensor Inventory
- Agent based Inventory
- Network Auto Discovery

The Inventory Database is maintained with an intelligent policy which factors in the data obtained by any of the previous methods and the reliability of this data.

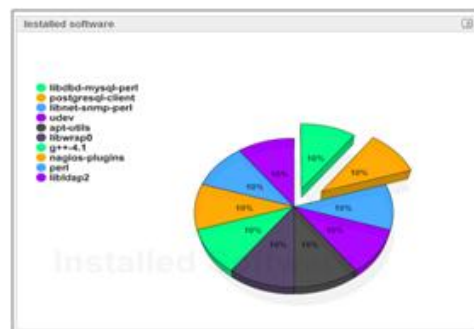


Network Scanning Inventory

AlienVault Professional SIEM includes an integrated Nmap scanner which allows for rapid inventorying of a broad network. For each asset this inventory includes:

- Type of network equipment
- Open ports
- Services running
- Operating system

Network inventory scanners allow auto discovery of systems in with low impact but with low detail and less than 100% reliability.



Passive Inventory

A number of passive sniffing tools are implemented in the AlienVault Sensor to automatically discover and create an out-of-the-box inventory without the need of human intervention. These techniques allow AlienVault to inventory:

- Netbios Names
- Physical Address
- Services running
- Operating system
- Users
- etc...

Passive inventory tools integrated with the AlienVault Professional SIEM such as *prads*, *p0f*, *pads*, *arpwatch*, and *ntop* allow auto discovery of systems in stealth mode but with a low detail and not 100% reliability.

Agent-Based Inventory

The OCS agent included with the AlienVault Professional SIEM keeps track of hardware and software configurations of each of the computers on the network. This requires deploying a local agent to control the servers and is therefore typically used to serve very specific needs. OCS runs on most common operating systems such as Unix, Linux, Mac, and Windows.

Agent-based Inventory provides a great deal of detail regarding the hardware and software inventory with complete reliability.

Network Discovery

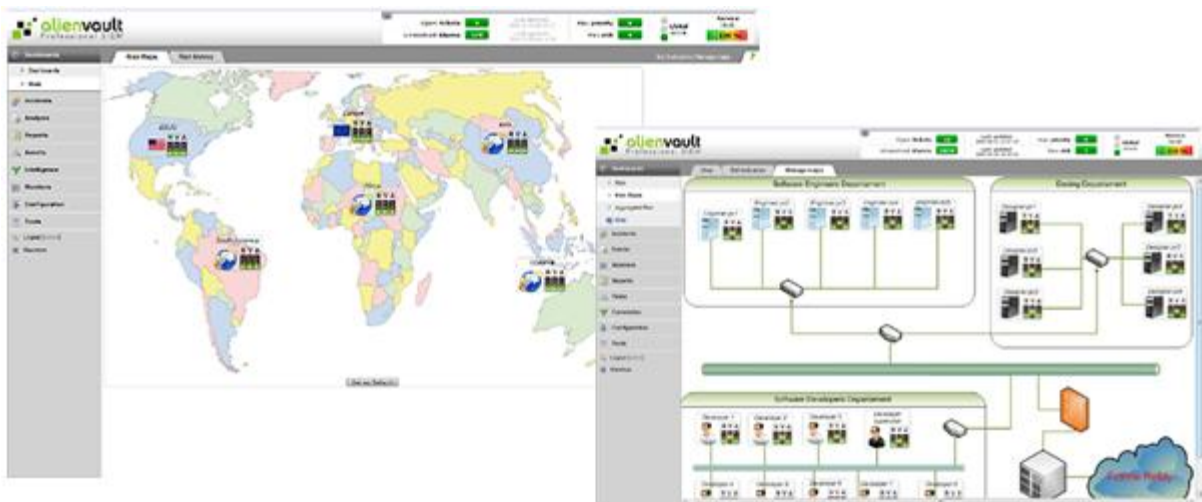
AlienVault Professional SIEM provides automated network topology discovery, creating an accurate inventory of network infrastructure and connectivity.

AlienVault Professional SIEM uses *Nedi* to recursively scan all network devices to determine where a host is connected, allowing the system to learn the hierarchical topology of the network. The system connects to network elements by snmp / telnet and downloads all equipment options and configurations (if it can connect by telnet / ssh).



Asset Topology Maps

Topology Maps can be uploaded and/or linked and can show security metrics offering high level visibility and abstraction as well as the capability to drill down through the topology.

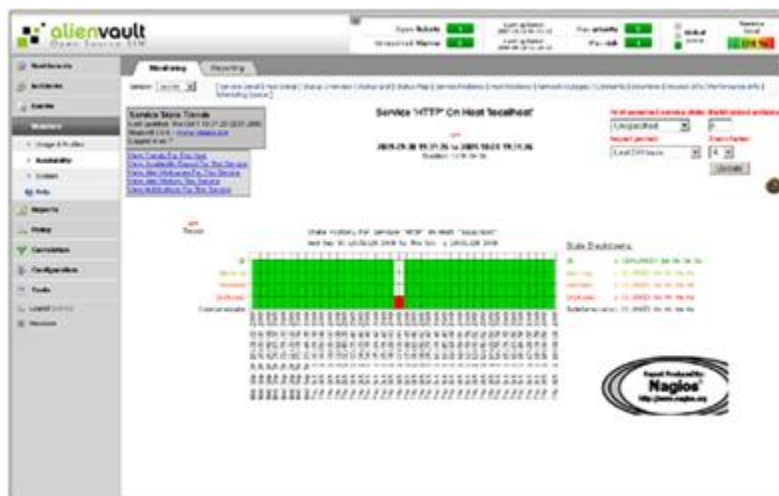


Availability and Resource Monitoring

AlienVault Professional SIEM includes *Nagios* availability-monitor which is capable of checking, displaying and reporting on host and network availability status. This functionality provides monitoring, reporting and historical trending of:

- Host Availability
- Service Availability
- Service Level
- System Resource utilization:
 - CPU
 - Memory
 - Network interfaces
 - Disk
 - Services running
 - Operating System metrics





Active Directory and LDAP scanners included with the AlienVault system allow retrieval of information regarding:

- Users and groups
- Organization tree structure
- Permissions

The WMI scanner allows retrieval of information regarding:

- Software installed
- Services and processes running
- Hardware configurations
- Users and groups

AlienVault Professional SIEM can use this information for security intelligence analysis, correlation, triggering alarms, and creating reports.

Monitoring methods include: SNMP (v1, v2, v3); WMI; LDAP; Active Directory and ADSI.

Custom MIB configuration, MIB walk, SNMP v1, v2 and v3 MIBS and Traps are supported.



Network Profiling

The network profiling system embedded in AlienVault Professional SIEM (*ntop*) classifies assets including an automatic profile for each system.

This profiling system can listen directly from the network or can be configured to receive flows.

The information learned by the system for each IP address includes:

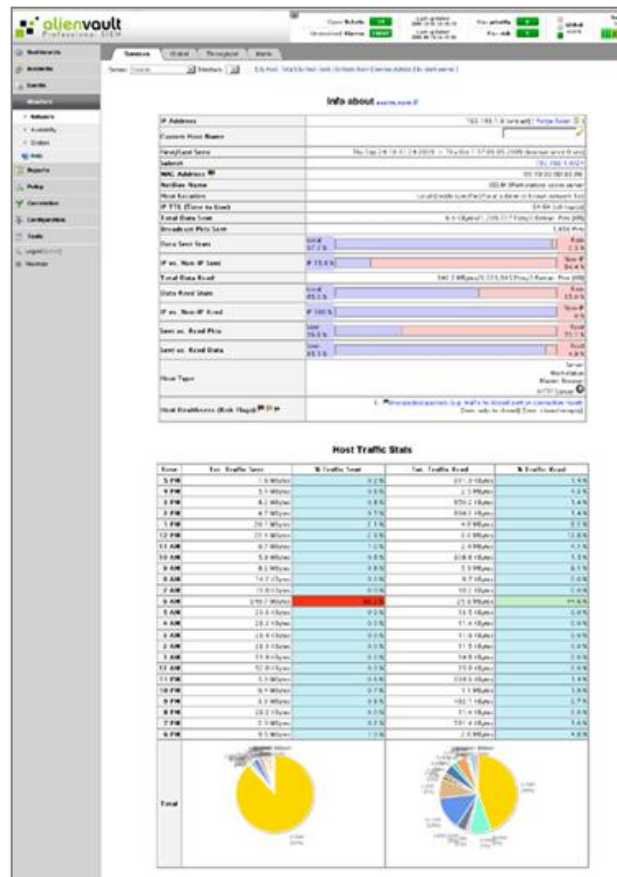
- Identification: IP, MAC, Netbios, usernames
- Time Usage
- Service usage profile
- Service profile as a server
- Typical destinations
- Current connections
- Throughput
- Bandwidth history for each protocol

Configuration Management

The system has the ability to collect device configurations and any detect changes in them. For this task, the solution uses different applications to collect from devices:

System Configuration

Using agents (OSSEC) installed on the computers allows the collection and detection of changes in configurations and files (as well as endpoint security detection capacities as shown in the *HIDS/ Endpoint Security* section).



The inventory agent (OCS) allows very detailed information retrieval from systems including:

- Software
- Patches
- Hardware
- Registry configuration

Network Device Configuration

AlienVault Professional SIEM performs Network Discovery (using *Nedi & Rancid*) that automatically collects configuration from network devices without the need of installing agents.

Organization Policy and Compliance

The audit capacities in the AlienVault Professional SIEM allow enterprise to define policies for software and configuration compliance. Any change or non-compliant system discovered will be immediately reported.



Configuration Analysis

All of the configuration information stored in the AlienVault Asset database is accessible from any screen of the AlienVault console with a simple right button click.

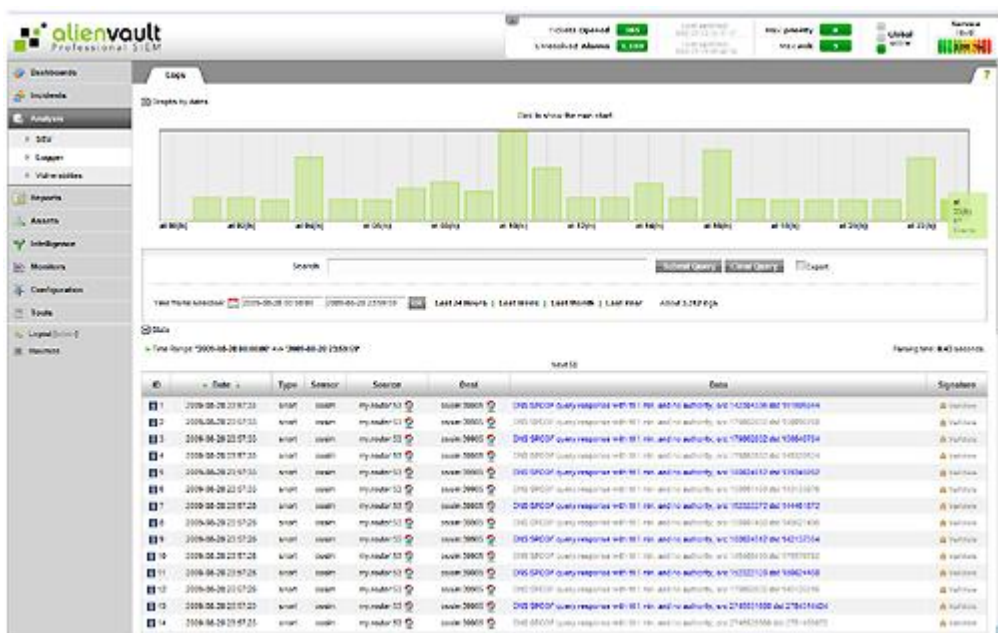
Change Detection and Alerting

AlienVault Professional SIEM allows for the creation of policies to detect the changes to network assets allowing monitoring, reporting and alerting of these changes in a wide range of formats.

Logger

Unlimited Storage

The AlienVault Logger provides the capacity and security to store large volumes of data while ensuring its admissibility as evidence in a court of law. The Logger provides an additional database to the AlienVault infrastructure specifically geared for massive, long-term forensic archiving.



The AlienVault SIEM database is designed for the rapid and versatile analysis required for attack detection and response. The AlienVault Logger database collects data in its native format, digitally signs and time-stamps the data, and securely stores the *raw format*, preserving data integrity.

There is no limit to the amount data that may be stored. The solution supports versatile queries of terabytes of data from multiple devices over spans of years, and provides detailed storage reports.

Events are stored encrypted and compressed in the Logger with a compression capability of 10:1.

Logger can be configured to store information in any NAS or SAN system.



Legal Integrity

AlienVault Logger stores information according to strict standards of the security market so the events collected by the system can be used as forensic evidence in court. Digital signature as well as encryption can be generated with the highest level encryption keys.

Data transport can further be forensically secured by implementing encrypted tunnels between the Logger appliance and the event source. AlienVault Logger supports most common encryption schemes and includes the *OpenVPN* client for use on network hosts.

Compliance Automation

AlienVault Professional SIEM includes a Compliance Module that helps companies monitor and report on the controls implemented in accordance with regulatory compliance issues. The system automates and facilitates corporate governance and risk analysis, significantly reducing the time, cost and resources typically committed to compiling reports and responding to audits.



The automated risk management model implemented in the Compliance Module offers a customizable set of Risk Analysis, Audit and Reporting features which combine to provide a unique solution which: identifies compliance risks; monitors and verifies conformity; and reports cases of non-compliance.

The Compliance Module correlates current information security legislation and legal precedents with technical controls, effectively converting the legal and regulatory requirements associated with international security standards such as ISO 2700x, PCI DSS and SOX (among others) into technical controls that are automatically and continuously monitored. All of this occurs through a standard framework that provides significant operational savings, improvements in control of the business, and reduction of response times to incidents. The Compliance module provides great flexibility to adapt to new requirements as they arise.

Custom Compliance

The AlienVault compliance framework is implemented around Business intelligence

Copyright AlienVault LLC, 2010 – alienvault.com – info@alienvault.com - +1 408 465-9989

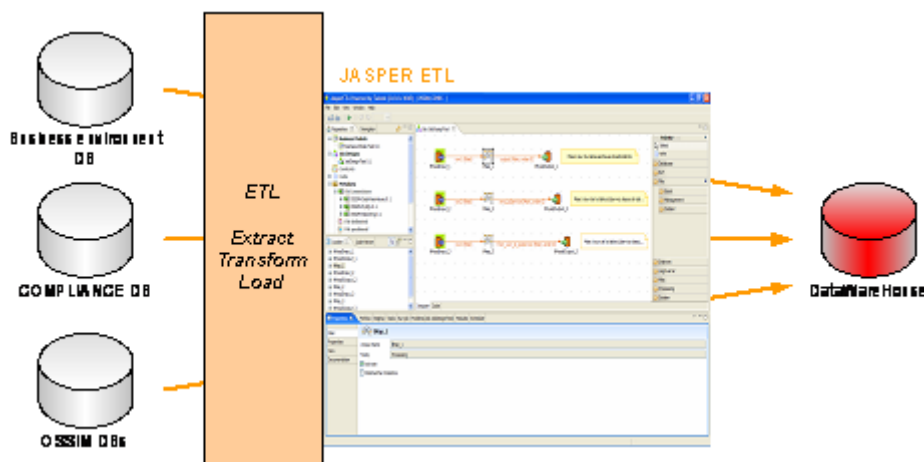


(BI) software bricks which provide efficient compliance information acquisition, normalization and processing.

- Report designer provides enterprises specifically crafted reports, forms and contents
- BI ETL (Extract, Transform, Load) provides data acquisition and consolidation in order to aggregate multiple compliance information source typologies
- Report generation processing, repository and visualization (Adobe, Word, Excel, HTML ...)
- Management interface which natively supports spreadsheet import/export to manage human-generated documents such as security audits, risk analysis, compliance audits, security controls implementation status ...

There are virtually no restrictions on the manner which the metrics and indicators can be presented and formalized for each compliance regime:

- General I.T. governance compliance such as ISO2700x family
- Regulation compliance such as PCI, Sox...
- Enterprise's internal specific I.S. Security policy compliance



Real-Time and On-Demand Reporting

Real-time compliance metrics and indicators are generated through a mapping between AlienVault correlation rules (i.e. AlienVault alarms) and compliance information. The objective is to identify which compliance security measures/controls are not fully implemented in the context of network activity.

As well, on-demand reporting provides direct information to drive security control implementation efforts through topological graphs and visibility into network trends.



Situational Awareness

The understanding of environmental elements involved in an attack is the key to AlienVault's ability to build the intelligence necessary for dramatic false positive reduction, accurate prioritization of incidents and detailed illustration of complex attacks.

The AlienVault Sensor includes a number of monitors providing situational awareness information in real time. This information from each Sensor constantly feeds the asset information databases and maintains historical information for incident and forensic analysis.

Network Profiling

The network information gathered by AlienVault Sensors also provides detailed information in near real-time about network usage for each network host and collects this data for analysis. The system automatically creates a highly detailed usage profile of each element on the network.

Bandwidth and Flow Monitoring

The Flow monitor can create flows which listen to the network and which can process flows from external devices. The system creates a searchable bandwidth database in which it searches for any origin / destination and port usage. Profiles can be configured to apply to different server and device types. The system can accept Netflow, C-Flow, S-Flow, J-Flow formats.

Network Behaviour Anomalies can be detected using flow information as explained in the *Anomaly Detection* section in the *Detection* chapter.



Inventory Monitoring

AlienVault Professional SIEM includes a powerful set of tools to automatically create and manage the inventory database used as foundational information for reducing false positives.

Detailed information about this is provided in the Asset Automatic Inventory section from the *SIEM* Chapter.

Availability and Resource Monitoring

Availability and resource information is used as basic information for the correlation process.

Detailed information about this is provided by the *Nagios* monitor as described in the *Asset Management* section from the *SIEM* Chapter.

Detection

AlienVault Professional SIEM includes in the Sensor a number of detecting technologies which provide information to the SIEM engine.

Intrusion Detection and Prevention (IDS and IPS)

AlienVault Sensors include Snort, the most widely used intrusion detection featuring:

- Thousands of pattern attacks
- High performance analysis up to 10Gpbs
- Daily signature update with the Subscription Feed

Snort can be implemented offline, as a sensor or inline as an IPS, stopping in real-time the selected attacks.

Anomaly Detectors, NBA

Anomaly Detection provides a point of view that is both different from and complementary to pattern detection. The AlienVault Professional SIEM learns by itself what normal network behavior is and will create alarms when behavior statistically deviates beyond normal bounds.

This technique provides a solution for access control of privileged users, as in insider attacks. No policy may be violated and no exploits carried out, yet an anomaly in the use and manner of use of a service can trigger the same alarm as an active exploit.

Some examples where anomaly detectors are effective:

Zero-Day attacks for which there are no signatures often produce an obvious anomaly yet circumvent pattern detection systems.

Worms that have been introduced into the organization, malware, a spamming attack, and even the use of P2P programs would generate a number of anomalous



connections that are simple to detect.

AlienVault Professional SIEM can likewise detect:

- Use of services that is abnormal in origin and destination
- Use at abnormal times
- Excess use of traffic or connections
- Changes in a machine's operating system, IP or MAC address, availability or services

Host Security / Endpoint Security

The HIDS Endpoint Security Agent (OSSEC) included with the AlienVault Professional SIEM can be installed on hosts allowing host IDS detection and endpoint security policy implementation through a range of detection techniques:

Log Analysis:

- Windows Event Logs
- File Integrity and access
- Registry Integrity and changes
- Active Responses

The system can deploy policies and detection rules for:

- Detecting Malware
- Monitoring Windows Internal files (OS) for changes
- Monitoring Registry Keys
- Monitoring process/services creation
- Detection of malware/spyware registry altering
- Detection of weak or suspicious ones configurations

Monitoring of processes:

- Hidden processes
- Hidden services
- Hidden files
- Hidden registry keys
- Hidden drivers
- Drivers hooking SSDT
- Drivers hooking IDT
- Drivers hooking IRP calls



Detection of potential entry points for malware infection, for example:

- External Drives (USB Disk Plugs)
- Acrobat Reader with Javascript enabled (Policy check)
- Internet Explorer Zone entries for ActiveX (Policy Check)
- Vulnerabilities on Office, Acrobat, Flash, Internet Explorer

Audit

Vulnerability detection systems discover and identify latent network threats and can correct them before an attack occurs. This information, stored by the AlienVault Management Server, is of vital importance when an attack is in progress. Prior knowledge of vulnerabilities in systems is critical when assessing the risk associated with an attack, prioritizing the incident, alerting, and launching countermeasures.

Vulnerability Assessment

AlienVault integrates vulnerability scanning technologies including *Nessus* and *Openvas* to perform and centralize scans and keep the vulnerability database current. Vulnerability assessment management tools include the ability to:

- Run scheduled scans automatically
- Distribute scans through multiple Sensors and aggregate the results into a single report
- Configure historical report storage
- Define profiles so different types of scan can be run based on severity or services
- Cross reference the Threat Database using common IDs such as CVE
- Perform False Positive management

As each vulnerability is discovered, more information is added to the Vulnerability database resulting in increasingly rich reporting and detection. Possible solutions to each detected vulnerability are provided to the system operators.

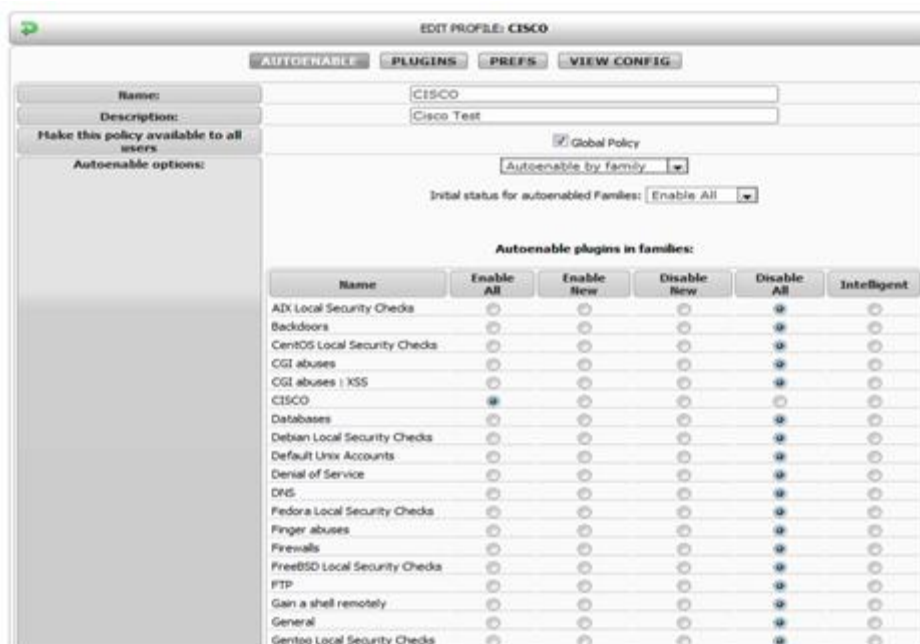




Job Management

Scanning jobs can be scheduled with the Job Manager, which allows:

- Easy profile creation through Families, Categories, or specific plugin configuration
- User and Role Management of scanning and reporting visualization



The screenshot shows the 'EDIT PROFILE: CISCO' configuration page. It includes the following elements:

- Name:** CISCO
- Description:** Cisco Test
- Global Policy:** Global Policy
- Autoenable options:**
 - Make this policy available to all users
 - Autoenable by family:
 - Initial status for autoenable Families:
- Autoenable plugins in families:** A table with the following columns: Name, Enable All, Enable New, Disable New, Disable All, and Intelligent.

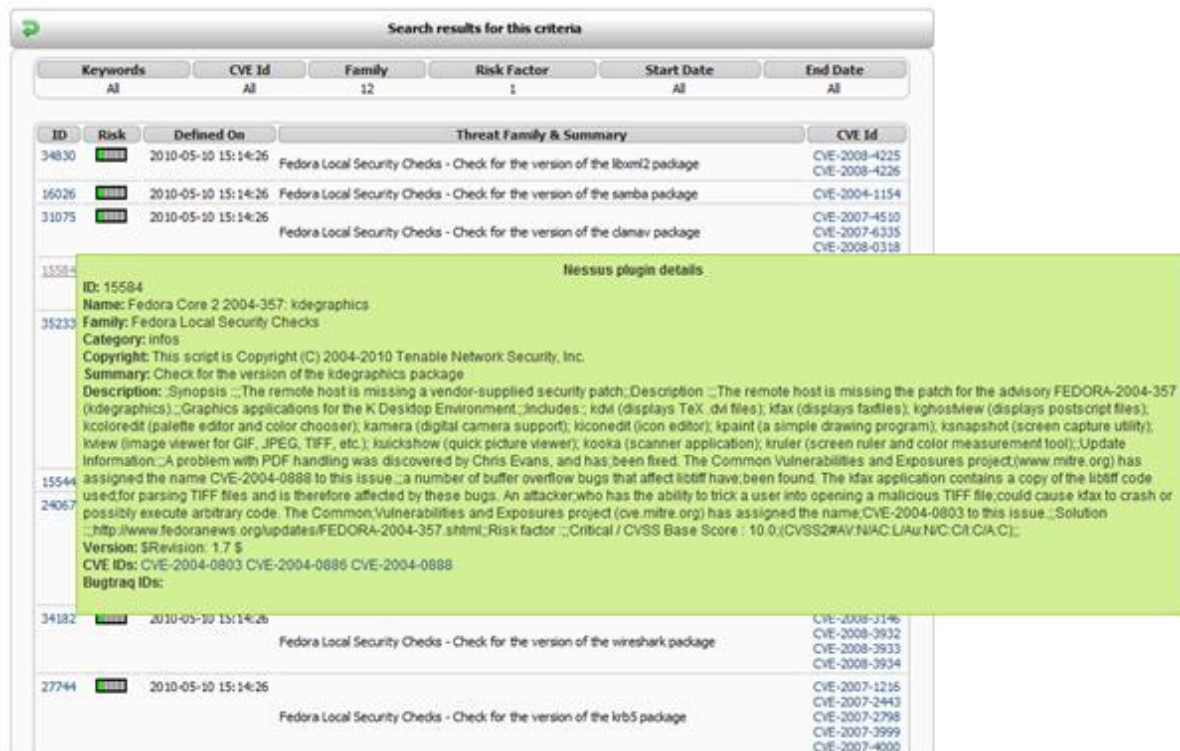
Name	Enable All	Enable New	Disable New	Disable All	Intelligent
ADX Local Security Checks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Backdoors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CentOS Local Security Checks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CGI abuses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CGI abuses XSS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CISCO	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Databases	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Debian Local Security Checks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Default Unix Accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Denial of Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DNS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fedora Local Security Checks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Finger abuses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firewalls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FreeBSD Local Security Checks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FTP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gain a shell remotely	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
General	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gentoo Local Security Checks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Threats database

The Open Source Vulnerability Database (OSVDB) vulnerability database is integrated



into AlienVault Professional SIEM and can be consulted from the management interface. This allows users to do searches and link results to incidents already opened or to the knowledge database. The correlation engine uses data stored in this database to identify vulnerable assets allowing for the automatic calculation of risk associated with an event.



Keywords	CVE Id	Family	Risk Factor	Start Date	End Date
All	All	12	1	All	All

ID	Risk	Defined On	Threat Family & Summary	CVE Id
34830	High	2010-05-10 15:14:26	Fedora Local Security Checks - Check for the version of the libxml2 package	CVE-2008-4225 CVE-2008-4226
16026	High	2010-05-10 15:14:26	Fedora Local Security Checks - Check for the version of the samba package	CVE-2004-1154
31075	High	2010-05-10 15:14:26	Fedora Local Security Checks - Check for the version of the clamav package	CVE-2007-4510 CVE-2007-6335 CVE-2008-0318
15584	High	2010-05-10 15:14:26	Fedora Local Security Checks - Check for the version of the kdegraphics package	CVE-2008-3196 CVE-2008-3932 CVE-2008-3933 CVE-2008-3934
34182	High	2010-05-10 15:14:26	Fedora Local Security Checks - Check for the version of the wireshark package	CVE-2007-1216 CVE-2007-2443 CVE-2007-2798 CVE-2007-3999 CVE-2007-4000
27744	High	2010-05-10 15:14:26	Fedora Local Security Checks - Check for the version of the lrb5 package	

Nessus plugin details

ID: 15584
 Name: Fedora Core 2 2004-357: kdegraphics
 Family: Fedora Local Security Checks
 Category: Infos
 Copyright: This script is Copyright (C) 2004-2010 Tenable Network Security, Inc.
 Summary: Check for the version of the kdegraphics package
 Description: Synopsis: The remote host is missing a vendor-supplied security patch; Description: The remote host is missing the patch for the advisory FEDORA-2004-357 (kdegraphics). Graphics applications for the K Desktop Environment; Includes: kdev (displays TeX .dvi files); kfax (displays faxfiles); kghostview (displays postscript files); kcoloredit (palette editor and color chooser); kamera (digital camera support); kiconedit (icon editor); kpaint (a simple drawing program); ksnapshot (screen capture utility); kview (image viewer for GIF, JPEG, TIFF, etc.); klickshow (quick picture viewer); kooka (scanner application); kruler (screen ruler and color measurement tool); Update Information: A problem with PDF handling was discovered by Chris Evans, and has been fixed. The Common Vulnerabilities and Exposures project (www.mitre.org) has assigned the name CVE-2004-0888 to this issue; a number of buffer overflow bugs that affect libtiff have been found. The kfax application contains a copy of the libtiff code used for parsing TIFF files and is therefore affected by these bugs. An attacker who has the ability to trick a user into opening a malicious TIFF file could cause kfax to crash or possibly execute arbitrary code. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2004-0803 to this issue; Solution: http://www.fedoranews.org/updates/FEDORA-2004-357.shtml; Risk factor: Critical / CVSS Base Score: 10.0; (CVSS2#AV:N/AC:L/Au:N/C:C/CIA:C);
 Version: \$Revision: 1.7 \$
 CVE IDs: CVE-2004-0803 CVE-2004-0886 CVE-2004-0888
 Bugtraq IDs:

Summary

The AlienVault Professional SIEM provides the rich set of functionality and heterogeneous support that enterprises, governments and Service Providers on six continents trust to manage their security infrastructures. In the words of Andrew Hay, Senior Analyst at The 451 Group:

“The AlienVault Professional SIEM product combines the breadth and flexibility of Open Source software with the features and functionality present in any of AlienVault's competition.”

As the most widely-deployed SIEM in the world, AlienVault is able to provide the evolving solutions necessary to address the escalating challenge of integrated security management.

