



# AlienVault SIEM System Description

© COPYRIGHT ALIENVAULT 2010





INTRODUCTION	
ARCHITECTURE	5
Components	5
Sensors	
Collectors	6
SIEM	7
Logger	
Scalability and Performance	7
Distributed Topologies and Load Balancing	7
Performance	8
High Availability	9
Role Management and Multi-Tenancy	9
REPORTING	
Dashboards	
Predefined Reports	
Custom Reports	
Scheduling	
3D Visualization	14
SIEWI	
Rick Assassment	15
Correlation	
Logical completion	
Logical correlation	
Cross-correlation	
Deile Feed Cele existing	
Daily Feed Subscription	
Real Time Policy Manager	
Collection	
Methods	
Data Source Connectors / Collection Plugins	
Custom Collection	
	10
Analysis	
Forensic Analysis	
Drill-Down Analysis	
Risk Uriented Analysis	
Alarms	
Search Capacities	
Automatic Analysis	
Real Time Analysis	



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





# 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 profession 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 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 fir 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<sup>©</sup> 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
  - o SIEM DB
  - o Logger DB
  - o 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.



		Cus	tom parameters
Name: Defa	ult		
	Background Color	Foreground Color	Click To Zoom
Title			* Only .gif, .png and .jpg files
Subtitle			
	Restore Origin	al	
Left footer:	User: #USER / #DAY #HO	UR	)
Right footer:	Page #PAGE / #TOTALPAG	ES	]

#### **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.





# 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.



alienve	ault						Table Street	t Opened 💽		int Lang	Tax privety	÷	-	***	
i Destinarits	100	NRCY.	CAB	ora i			1							-	-
gi Incelerite	100						Inter Colorado	the Party Street	-						1
- Analysis	iii Ae	¥. 2	Rode	Dente selected (3)	Suplicals selected 📴 Re	tiat Public .	, Truthe Disable	pellog					_	_	
12 Reports	A1918	dis.	Profile	Source .	Destination in	Pert Dread	Reprinter	Setars	Trailarge	Tageta	Description	Correlate	dress i	Stee.	Gubby I
Assess     Assess     Policy & Actions     Consider Dealers     Consider Dealers     Consider Teachers	ľ	+		102 146.11     102 146.11     10 20100.11     10 20100.11     10 20100.11     10 20100.10     102 146.10     202.00	<u>i</u> un	AMU -	Anomales Printe	**	Box 21 - San 226	**	Plata is ion		•		•
+ Smae Semilation	1	1	15	12 wy	diary.	489	August No.	100	Nov 31 - San 224	any	-				
12 Manifers		1.1	(increase)	C. ww	(Swy	345	10.000	-	Mat 24 - Dat 228					-	
¥ Configuration	1		1.00	ill also	illi, eden	ART	Anomalae	ANT	No. 8 - 5at 22	419					
Tasta	×		1.0	(ii wy	(ii. ery	ANY	Interferent County	ART	Mol. 24 - Sun 324	**		٠			•
2. Ny Poste	1		1.0	ill ev	3.00	ARC .	Wednesd treffs	ANT	No.21-54(23)						
Ne Laper(2014)	10.000	_	_												
W. Macrosov	-	_	_			_	And Inch.	-							. +
	36.54	10.00	Heaty-	Debe anischet	Naticale selected 🔅 Ri	esat Policies 👎	Couble Couble	pring							
	4,014	or.	Pronty	Sbariel #	Destination +	Pert Group	Huge Droat	Senare	Ten farge	Targets	Carrola Drake	i me i	Darty P	Instance P	leaser: Sa
	1	- 14		18 182 168 1.00	(E 102.1061.00	ANY	Prote	-	Roi 21 - Sat 221	= 14					
	~	18		ill ev	il ey	ANT	and the state of t	- 4401	Mari Dr Dan 228	419					
	1	16	3.	AAPONIC BIADHADD	Change-Office	2309 atra	Acakering Acake	any manafest	Nov-311-Sun.324	-		•	•	•	• •

# 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.

••

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



#### **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.

alien	roult	Sa co	ari Takata 📰 🖬	Last coloradi provide la la d'une Last coloradat	Tax plant		1	*	Barreton Galacian
Cantoriarda	Millionta Real Time Contornant II	www. Databas							
di monene	-								
Colorest Street		1				in March	i		
1 Millionte	-								
· IDELette	Home   Search	D Back		Current Search	Criteria I.	law with	inte 1		
* Universities		-				24.0	Call.		A DOT OF
T Annual C		-	ana 108-128-1	2008 ( any long . Cas				-	1018
-		a property in							
	Based	d Bernard B		Burry	nary Statisti	C8			in the second second
S. Workers	Time Tanks and then		Freedon .	Sensors	mages (re	-13		ass frations	-13
Reports	Last 24 Murrs   Last Week   Last feet Weet	District Addresses Source fort Destination Furt Internet Destination TCP (IDP TCP) (IDP			Unique IF India (Fi208)				
L Policy	A Design of the second second second								
Y Carrantee	· Defended strend into the Land							1.000	
	C Square	+ International +	Source Address	Dest, Address	S+D.	Print	And .	5+0	L4 grots
E Configuration	Stirld Logit Automatic, Automated password	2009-09-20 09-47 19	102.102.122.124	neam earver 20	EK-4	11-1	10.0	1.4-14	11.0
Tank .	10hd Logit succesful, Accepted pass ound	2009-20-20 00:47 19	102.108.1.55.5744	seam-server 22	Not 1	0.4	0.2		104
Concernant State	SSME Logit burnerful, Accepted personnel	2010-05-21 20-47-19	192,102,1,52,1744	east and will	Fred	D.1	1.1	1 (d-rd.)	707
College Street	Stind Logit subsectul. Accepted password	2008-09-25 (8-A <sup>2</sup> /9	192 10E 1.5E 17mi	1988/1-847/10/22	Eret	1.1	10.2	(test.)	10
a narran	30Hd Logie successful Accepted password	2010-09-20 09 47 19	192 108 1 30 1744	198877 AM*/107 22	- Prod	E. 1.	12.1	1.0.0	100
	10% Loge scoude: Accepted password	2009-09-20 09-47 19	452 HEE 4.52 1744	cash and at 22	Pret	2.1	1.1	1.4.14	10
	Elite Lage accessive Accepted pass and d	2016-25-25 38-47-19	102108113021744	coastro astrone 22	2-12	1.1	2.2	4.18	100
	35NE Logie accessifie Accepted personnel	2019-09-25 (8) 47:19	1902 1988 5 552 5744	costh-service 22	(X-a)	B.1	10.0	1.4.14	1.00
	Brother, and An Institution (BC, P) has charged in CS.	2005-05-25 08-47 18	102,108,1.58		Ref.	111.0		Canal	1.00
	E MIROWA	2009-09-25 09-47 16	162 168 1.50	0.000	Elf-ad-17	B-1	10400	1.4-4	1 106
	int_investorii niny gelosi #_3HDF-800778/ee	2009-29-25 09:35 50	8888		Line	E 1	1.	( e.e.	100
	Internet the plan #_2+Ch800790/ee	2008-09-20-09-20-00	668.8	4888	Elevel	E 1	1.1	Lt.et.	1.70
	H. Humaniel may place P. 24CP-2007MyAss	2605-09-25 (0.25.00	1111	10.00	[Ket_]	2.1	L	teret.	10
	I vie, hvervell into pater #_bitCh800799,444	2008-25-25 (0.30.00)	88.9.9	4444	12-12	0.1	1.1	(tert.)	700
	H. M. Reserved. Hop place P. 24CR-800179 year	2019-09-22 19:25 19	44.63	1010	Rest.	0.1	C.L	8.10	70
	1 vit, hvesholl rise place #_DHCh.800798,res	2019-09-21 09:70:00	1111	6888	Theat -	<b>I</b> -1-	15-6-	110-0	1.10





#### **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:
  - $\circ$  Inventory
  - o Network
  - Profile information
  - o Availability
  - o Resource utilization

alienvau	lt.	The second secon	
i Intern i Intern I Million I Million I Million	E.F.         Ten         Despect System           V de profestation         and CANTER APPropriate         Second Approx           Second Approx         Approx         Second Approx           Destation         act         act	n Paga San Paga Si Paga San Paga Si Para Pada Bar Paga Si	
)	Annandational deviations, two mecanities and p 2.7 (2) of the production of the production Objects wave	n & hoppen aller (h. allen 1. f. m. (h. 12. chille	
i tanjaran Tan Ganatin-1 Rama	100         0	and an analysis of the second se	
	Pagestal         Imagestal         -112           How         (1)         (2)         <	16月2日1日)	

#### **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.



alien	lenvoult					notional Alassian California		The private	1	-
C Ballinson	Hat Hat 7 Red Det	10								
+ Castlorada						the second state of the second				
+ tes			and a second	A STATE	and they have been	Constants ( 1994 Mark)				
di kankens		-1-	Croce administ	ogras			Balantes	Service Level		
. Analysis								1		
12 Beauty							-	92.98%		
Annelia		-		In			1			
-								ATTACE		
			Gobal					Global		
IC Monters	Children		Plac Date	Flast	Carrent	Colul		Plan Date	Flat	Castrol
1 Configuration	GLOBAL SCORE	80	3009-09-10 52-00-00	, high-		GLOBAL SCIRU	20	1004-05-11-00.00-04	140	
			Refuerk Groups					Network Groups		
C. Com	Group		Heat Date	Hat	Corrent	Seven .		Plax Date	Han	Correst
2 months	<ul> <li>group,het</li> </ul>	100	10			- group, hen	100	3529-67-38-02-00-08		
1745 mar 2010 c	- propolece	100	1/8			· properties	100	3009-07-28 02:00:00		
of released	<ul> <li>mexting_prop</li> </ul>	100				+ mexting_group	12.00			
III. Hankball	+ pphan	2010	- 10			- pphas	20	4.8		
	- proba	10		14		- probe	100	NA		
			norka autoble groups				1000	works outside provan		
	Belwerk.	1000	Max Date	Par	Current	Betweek		Plan Date	Fine	Correst
	Pol 10		3009-09-34-02-00-00			Pvt_10	200	2009-03-02-02-00-08		
	han franchise Office	1010	10			has francisco Office	100			
	Washington Office	100	. 10			Washington Office	10	8.8		
	prochad	10.00	4/8			pretad	<0-	1/8		
	Inc. A Balance		March Street	-	- Annual	Bard Address		Paula Date	1	- Course
	mail Address /	10.00	2008-05-01-02-00-00	-	Carrier	Theat Address	La ma	2006-06-10-00-00	-	
	100 March 100 Ma	100	2008-02-02-02-02-02	-		Contract of the second s	100	and a state of the		
	1000	20	1000-02-04-02-00-00	_		200	20			
	100 mm 1 1	100	Transaction in the second	_		and share a la	100	THE ALL REPORTS		
	and and a ba	1000	and an an arrange	-		and and a lat	100	and the second second	-	

#### 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.

alien	vault						oper schara		Maria and Annual and An		in a state
@ Datourds	Aurus Res	ur l									17
A bardenia	Stress Adda	and votion									
* Alarma	Course of the				0.94		and the second second		(amorit)	Consistent C Marine	-
+ Tuhine	- Charles	Alaser	100	-	-		Land	- Second	and as loss	-	-
* Noviety-10	and the second second	and the second second	1000	10.00	-		No 2000 [ NAM ]				
	D+1 AVMergon	e boteet. Activity on Server We		1000	2010-00-07 (7) (5) (5)		1000007-0100-0	Descriptions & O	81 207 S (048128		0.5
in tempera	El + 2 Arthurster	bade.com April detected on		-	21040-011701-41		10 40 40 40 10 - 20 40	in a second of 2	NEAR THE WAY	-	0.5
	3 Av Pussible	part 445 Woom Scan Bellevour on	1		20242-0716-2108		100-12-07 (6-20.51)		Maria an Desteration	-	07
W Internet	The second second					-		10100	Production of	· ·····	-
	1 June + Art	formable part 445 Warm Same Bellevin	at the lary		14	7	2010-02-07 DALEMAN	ferrer Hanitati &	ar the loss at the grant do		
in Monitora			Aires	-	ery [field ] web 2-3	-	william 2-Gran Types	1-line#Delfarts 1]			
- Configuration	+ 2 Total errenta matureste	eller hybest sile level, before innovi-							verwittele surrent descrive defenses		
2 los	-+ Greed	sevelender detected on tower was	3		21042-0718-16-07		10-10-10 M 10-10	Server 20m 1000 4 2	101. Mar 14. Marty 1.		0.7
C Room	1 2000 1 4	Alberta Traces Devenhader detected on Serv		Inel		2	Date:	Second Annual Second	Destanting	Convision in	net
R. Herbild	A COMPANY AND A		Alere	1	ary Third Dearst 2-2	nane i	NUMBER 2-Union Types	2-serve Detroite 21	the second se	-	
	<ul> <li>ETable events resizied.</li> </ul>	after highest rule level, before timeout,							Versitälit carried devilue defectors		
	E)+1 AVMshare	Using detected as Grover illu-	- 1-	-	301040-0718-1021		1004247552012	Server 200 100 # 2	18 (4 147 30kmap **		0.7
	D-1 Chulge)	ees Prorg usage on 253,166.8.1	1		2042-0730-2038		10424716/001	101 HALL DE 20 4 2	11.171.00.00700 ·	spre	05
	* 14 1 matri + Av	Alarm Anonymous Provy statur on 142 148	1104	-		**	Date Zonica in 2010	THE MAX & STORY &	Destination	Correlation Lo	-
			Alere	-	ery (field freeds 2-3	-	All Palie 1-Gran Torn	L-Shape Dal Faria: 13			
			0.7								
	E = 1 AVTreport	Offects Activity on Server We	1	-	2042-071520A	- 1	nan-ran tertakana	Several and AL	51.00.00.00.00.00		00
	a 16	Airm			. Kok		DAME	MARTER	Devision	Conversionee Law	eff -
	a 35675 + A	W hopes softenth Activity on Service a	-		3	3	0040471600.51	Several (24)	55.85.05.05.0500 htt	2	
	The second se		Abre	1.mail	My Traditional 2-3	nd.t	HIDRADE 1- IFIGH TUDHE	1. Under Der Remer 12.			
	+ 53 346 e-ent autoret	and share on and providence	_						ww.RdContent describe definition		
	1 + 3 Norman And	110-09/3witten informe on	1	-	2010/07/15/16/40	1	1042-073620-01	torio constant # 2	64.34.200,126.00p.00	-spen	02
	All the All Design D	contrader detected on Severe With						- 6		and the second se	1000

#### **Search Capacities**

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





金.		Bad Tave	
Home   Search	p Back	Mata Collecta	
alaan of Aarts	C. B Spatters Payment	Tensor (( sty famor )	
inter I Types Inter Same same time I Cast 24 Rivers   1	One Environ Bas Rome softwarks Politic Softwarks Politic Softwarks ( Softwarks) Politic Softwarks ( Soft Booth ) All	Event Group         [any put time]           Event Time         [an]           [init]         [init]           [init]         [init] <t< td=""><td></td></t<>	
		Payload Criteria Republic Criteria Input Criteria Disording Type ( Inscribit) ( a) Connert To (unless searching) ( Inscribit ( ) a) (	1 0 and P

#### **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.

alien	vault		Tile Unaste	i Opened 🔳		And a second sec		
Deshibiartis	SEN Cur	torn Triveless Alonades Stati	nta					Renge Kalemane
gi buidenta	(BRIDE) Des Hors	(test)						
E Analysis	-	Fuend Station		Genarator	Sensor	Jourge IP	(ext)P	(reset.)
+ sew + Leger	2010-02-07-09-07	mart, 17 PC/CV income base Auto baselis in Passault Mitchel Aterchants	. 12	and	spectrum seam	Alemant SEX 41952	102.1081.128.98	Plage filter:
+ Vuteralities	2010-02-22 17:49-41	WHAT TO POLICY Debatting from Auth Baselin II Presential American Longitudes	e 100	anat	-	Alervay SEX 4552	1982 1988 1 128-000	Departie
The second	3010-03-0217-49-40	anart. T.T. MCAN MINF, ed. actuation, ADMC		and .	springsround.	Allenvault SEX 10000	182 162 1 140 111	Date
	2010-02-22 17:46:46	south XT.POLCY many managers, how the lawering of	6 100	and	(personant)	Alerveut SEX 44985	192 198 1 129:00	Databas
Anarta	2010-42-22 17 49 48	Not. TI FLC: Deprint heat with Section 7	1 1	4141	-	Alervant SEX 44316	1621081129100	Croter
Y bibligence	2010/22/17:48:48	Mart. 17 KLC: marine Seat. Auto Baselo re Passault devided annumber	122 8	aven	-	Alerveut SEX 44801	102.104.1.108.00	Count
20 Bushes	2010-42-22 17 49 48	start. TC NUCC Outains Insc. Aub Develation Designed administrations.	1	avet	openany/seam	Alerveut SEX Addr.	102108-1120-00	Date
3. Configuration	3919-43-23 17 49 39	and STREAM AND ALL ADDRESS STORE		aut	operator team	Adamant Stick S2000	102108119409111	Deservoire
- Toola	2010-022117-08.38	Areast, TT POLICY, Incoming Street, Aust, Sametin, 5 Press, and Department, and an areas areas	- 11	and	openanur casaim	mervaut DEIX 44065	192,108.1.128.08	Detet
the Copyright of	216-0-217-039	stort, TJ POLC: Outputs Same, Aub Benefit In Instances America and control and	a 400	wort	operand team	Abryad SEX 44000	102.1081120.00	1.1464
II Names	2010-421-221 17 49:39	anal. TI POLET married base Ault Basels, N Transact Minibal annualitie	ш н	avert	special cases	AMPLIANE SEX MIDER	182 108 1 128 00	
	2010/42/22 17:49:39	Inst. 12 POLCY Optima Seec. Auto Benefit of Personal Administration	1	anat	Operator same	Adenvised SIDIE 44000	192 198 1 1 20 10	
	2010-02-2217-4838	start '97 SCAR MAR' all amilton 2072		anat	contenue canon	Alerveut SEX 12948	192 188 1 146 9111	
	2010-02-07 49:38	elist, 32 POLCY Rusten, Beer Auto Beerbillt Deexviral Mitchel Jonarization	en 10	8107	operaturbative	Alerved DEX 44902	192 198 1 139 00	
	2010-02-22 17 49-58	anort. 37 POLCI Outsitive Based Auth Energies In	412	and	igenative county	Ademount Sittle Addition	1922 1988 1 1209 000	

### **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.





alienvault		-consequent constant allows			 Line Sel
0 meteren //	and the later the second the second	Bowter Cyrofiana			 - 17
1 Decidicards		3		3	
gi nomen					
	Tickets Closed by Month	Ticket Ty	pes		
- Imparts					
t, Asses		1			
Y			Animaka Turat		
iji Mushun			Concession of the second secon		
§ Configuration					
- Kude					
t Renter	Torpe Anaday University				
		×			
	Ticket Status	Ticket Resolutio	n Time		
		the their	13an 43an 18an 4	- from	

#### **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*, *pOf*, *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:
  - o CPU
  - o Memory
  - Network interfaces
  - o Disk
  - o Services running
  - o Operating System metrics





alien	vault		Transford Name	ANT STOL	Taratak		Terret State
-	Badang Strong	Lucia and the second					
() between	seer lain 31 (teaster	al wolves ( the Dense ) in		n ( nationalises ) famale	Alam Street Store	en (research arts of	(she environment
i tem i tem i tempitiste i tempitiste i tempi	Landes Tapa Teniti Languet Incol Cong Jonation Languet Incol Cong Jonation	1	Service HTTP On He	n localhan Nais Ikinak	(Legt)its	- 31	- 3 (Acces)
	DOLARDARY STREAM						
- Tale - Tale - Sector		itala vytur, ty av ty i usta	1976 197 19 80 100 1978 19 19 19 19 19 19		tastadoes a i unas pras i unas		
E Manage					C	Naglos	

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*) clasiffies 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
- Parches
- 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 – <u>alienvault.com</u> – <u>info@alienvault.com</u> - +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 humangenerated document s 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 accepts Netflow, C-Flow, S-Flow, J-Flow formats.

Network Behavour 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



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



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 though 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.





alienvault		Totay B University			To: state			
· Adapta		Testification					-	
gi kalanta			10.24	nen i Inc. i				
E Anders - State - State						II try ty II second II selant II selant II selant	non e (specije) claninje) e (spile) (s)	
i Agente	8 .		=	1	-	alter the	1009008 340009008	
2. Austra		6-1	-		7	antere la	a-prenipt animologi	
Y sudges						<ul> <li>Interview</li> </ul>	eenes .	
I Mater	tes all tell-suite			Tap 38 Kods				
5 Carllyandes	Barris Harrison (1994)	-1	<b>-</b> 1 8	( march and a 1 ( ( a)				
- franke								
n (uppel)===) E Hantin				PE 10.10 PE 10.10 PE 10.10 PE 10.11 PE 10.11 PE 10.11 PE 10.11				
					ex E			
		.0	mint Vuberdellers				-	
			Carto Cravel # 1	in the				
6	Dat P	Date Tank	India	- Sector	I HAD THINK	. Los bits		
					4 0	41 345	244	
	**** 012.044.0				1.1	1.0	284	
		20001023231.4048	345		. 8 . 8	3.4	14.4	
		2000-02.07 (2.86.0).	(afait			1 10	344	
		2000-00-02 12 (M-11)	344			1.1	348	

#### Job Management

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

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

	EDIT	ROFILE: CISC	0					
1	AUTOFNABLE	PREFS	VIEW CO	NFIG				
Bame:	CISCO	2						
Description:	Cisco	Test						
Hake this policy available to all users	Clobal Policy							
Autoenable options:	Autoenable by family							
		Autoe	nable plugins ir	able plugins in families:				
	Name	Enable	Enable	Disable	Disable	Intelliger		
	ADX Local Security Checks	0	0	0		0		
	Backdoors	0	0	0		0		
	CentOS Local Security Checks	0	0	0		0		
	CGI abuses	0	0	0		0		
	CGI abuses   XSS	0	0	0		0		
	casco		0	0	.0	0		
	Databases	0	0	0		0		
	Debian Local Security Checks	0	0	0		0		
	Default Unix Accounts	0	0	0		0		
	Denial of Service	0	0	0		0		
	DNS	0	0	.0		0		
	Fedora Local Security Checks	0	0	0		0		
	Finger abuses	0	0	.0		0		
	Frewals	0	0			0		
	FreeBSD Local Security Checks	0	0	0		0		
	FTP	0	0	0		0		
	Gain a shell remotely	0	0	0		0		
	General	0	0	0		0		
	Gentoo Local Security Checks	0	0	0		0		

### **Threats database**

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

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



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.

			Search	results for this criteria			
	Keyword Al	s CVE Id Al	Family 12	Risk Factor	Start Date Al	End Date All	
ID	Risk	Defined On		Threat Family & Sum	mary	CVE Id	
348.30		2010-05-10 15:14:26	Fedora Local Security Ched	ks - Check for the version of t	the libxml2 package	CVE-2008-4225 CVE-2008-4226	
16026		2010-05-10 15:14:26	Fedora Local Security Ched	ks - Check for the version of t	the samba package	CVE-2004-1154	
11075		2010-05-10 15:14:26	Fedora Local Security Ched	ks - Check for the version of t	the damav package	CVE-2007-4510 CVE-2007-6335 CVE-2008-0318	
1558-4				Nest	us plugin details		È
15544 24067	Copyrigh Summar Descripti (kdegrap koolored) koolored kolew (im Informati assigned used,for possibly htp://www. Version: CVE IDs: Bugtrag (	t This script is Copy p: Check for the versi on: Synopsis "The hics", Graphics applied t (palette editor and c age viewer for GIF, J on: A problem with P the name CVE-200- parsing TIFF files an execute arbitrary cod wir fedoranews copy SRevision: 1.7 \$ CVE-2004-0803 CVE Dis:	right (C) 2004-2010 Tenal on of the kdegraphics pac remote hoat is missing a zi- ciations for the K Desklop oblor chooser); kamera (di PEG, TIFF, etc.): kuickshor DF handling was discove - 0688 to this issue ::a nu d is therefore affected by th e. The Common/utinerab pdates/FEDORA-2004-35 : 2004-0886 CVE-2004-01	ble Network Security, Inc. kage wendor-supplied security p Environment, Includes. : gital camera support), kick ( quick picture viewerk, k red by Chris Evans, and h mber of buffer overflow bu hese bugs. An attacker, wh littles and Exposures proj 7. shtml_Risk factor ;; Critt 988.	batch "Description The re cdv (displays TeX, dv files oncetit (icon editor); kpaint locka (scanner application) as been fixed. The Comm gs that affect listift have be to has the ability to trick a u ed (ove mitre org) has ass cal / CVSS Base Score : t	mote host is missing the pa ); ktax (displays tartles); kg (a simple drawing program kruler (screen ruler and co nr Vulnerabilities and Expor nound. The Idar applicati (ser into opening a maliciou (speed the name; CVE-2004) 0.0.(CVSS2#AV/NAC: LIAu:N	atch for the advisory FEDORA-2004- host/ww (displays postscript files); (; ksnapshot (screen capture utility); hor measurement tool); Update sures project; www.mitre.org) has on contains a copy of the libbit code is TIFF file; could cause ktax to crash -0803 to this issue.; Solution wC-CH-CA-C);
34182		2010-05-10 15:14:26	Fedora Local Security Ched	ks - Check for the version of t	the wireshark package	CVE-2008-3146 CVE-2008-3932 CVE-2008-3933 CVE-2008-3934	
27744		2010-05-10 15:14:26	Fedora Local Security Ched	ks - Check for the version of I	the krb5 package	CVE-2007-1215 CVE-2007-2443 CVE-2007-2798	

# 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.