

SIEM

Implementación de un correlacionador de eventos

Juan Carlos Flores Ibarra
Edgar Israel Rubí Chávez

Antecedentes SIEM

- SIM – Security Information Management
 - Sistema de Gestión de activos
 - Incorpora sistemas de seguridad de la información
 - Reportes deben ser mapeados a un sistema envolvente

Antecedentes SIEM

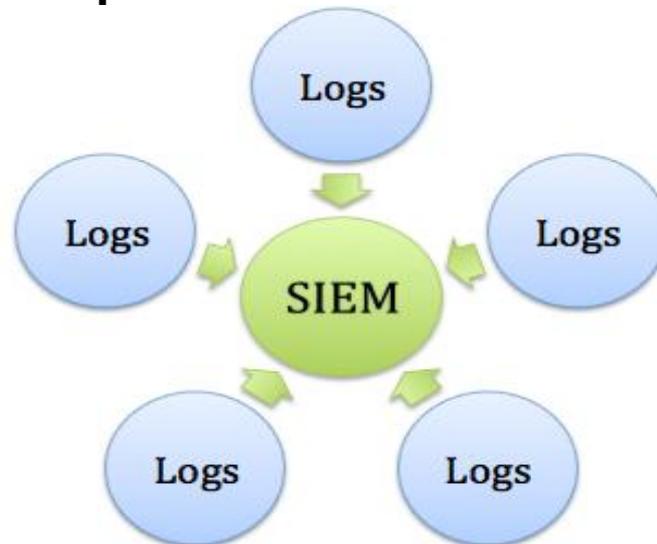
- SEC - Security Event Correlation
 - Analiza eventos y bitácoras
 - Busca patrones de comportamiento inusual
 - Alerta al responsable

SIEM – Security Information and Event Management

- Convierte términos generalizados a información administrable
- Implementar controles de seguridad e infraestructura
- Combinación de los sistemas SEC y SIM

Objetivo

- Implementar un correlacionador de eventos que centralice las bitácoras de los servicios brindados por la Subdirección de Seguridad de la Información en un solo servidor para identificar comportamientos no deseados.





SIEM – Open Source

- Cyberoam iView
- AlienVault Ossim
- Bitsum
- Logalyze

Comparativo SIEM

SIEM	Rendimiento	Red	Log	Ataques	Agentes windows	Agentes Linux	Otro Agentes	Reportes	Servicio Web (correo, sitios, etc.)	URL
OSSEC	✓	✓	✓	✓	✓	✓	Cisco, Juniper, Netscreen	✓	✓	http://www.ossec.net
<u>Cyberoam iView</u>	✓	✓	✓	✓	✓	✓	Fortinet, SonicWall	✓	✓	http://www.cyberoam-iview.org/
<u>AlienVaultOSSIM</u>	✓	✓	✓	✓	✓	✓	Fortinet, Cisco	✓	✓	http://communities.alienvault.com/
<u>Logalyze</u>	✗	✓	✓	✓	✓	✓	Cisco, Juniper, etc.	✓	✓	http://www.logalyze.com/
<u>bitsum</u>	✓	✗	✓	✗	✓	✗	✗	✓	✗	http://bitsum.com/

ALIEN VAULT OSSIM



ALIEN VAULT OSSIM

Install AlienVault USM 4.2 (64 Bit)
Install AlienVault Sensor 4.2 (64 Bit)

Press [Tab] to edit options

#Install OSSIM

<http://www.alienvault.com>

Instalación

- USM (Unified Security Management):
 - Es la instalación completa para los servicios de administración.
- Sensor:
 - Es la instalación de un sensor que reporta a un USM instalado en otro equipo.

Configuración AlienVault

```
AlienVault Setup :: alienvault :: OSSIM 4.3.3.1
```

```
AlienVault Setup
AlienVault Setup
  0 System Settings
  1 System Updates
  2 Configure Sensor
  3 Maintenance
  4 Tools
  5 Jailbreak this Appliance
  6 About
  7 Apply changes
< OK >      < Exit >
```

Configuración sensor

```
AlienVault Setup :: alienvault :: OSSIM 4.3.3.1
```

Configure Sensor

Configure Sensor

- 0 Select Listening interfaces (promiscuous mode)
- 1 Configure Server IP
- 2 Configure Framework IP
- 3 Monitored networks
- 4 Select Data Sources**
- 5 Select Netflows Generator

< OK > < Back >

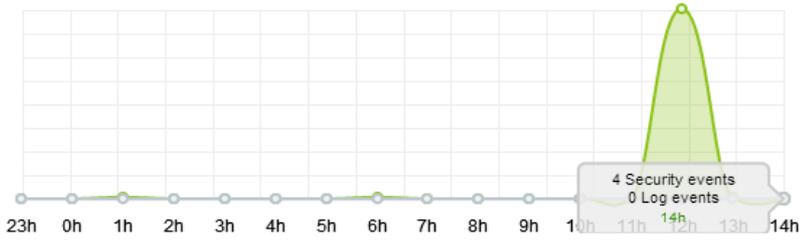
Connect to the AlienVault Web interface opening the following URL: <http://10.>

Recursos

- Arpwatch
- Cisco-router
- DHCP
- Fortigate
- Nagios
- Pam-unix
- SSH
- Sudo
- Syslog
- Rsyslog
- Snort
- PHP
- Switch-Cisco
- Nmap-monitor

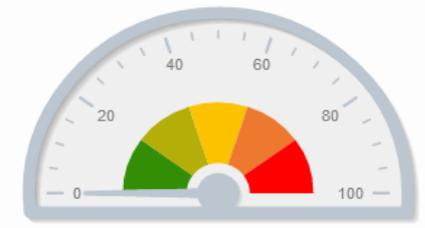
Resumen

Latest SIEM vs Logger Events ?

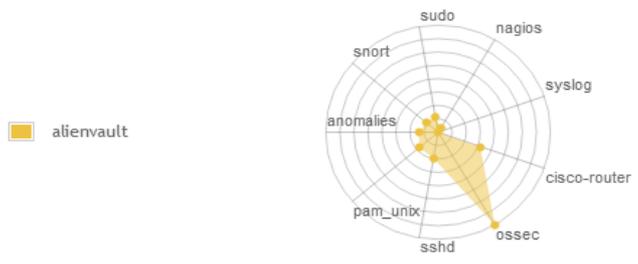


Threat Level ?

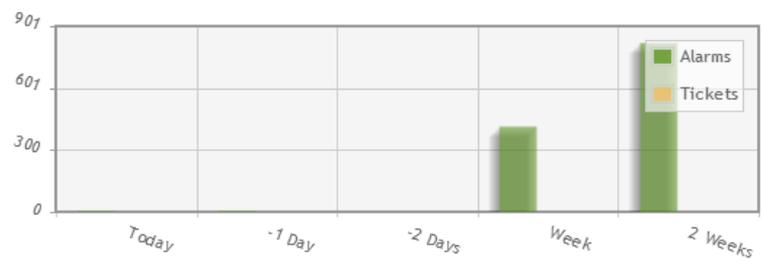
- Very High
- High
- Elevated
- Precaution
- Low



SIEM: Events by Sensor/Data Source ?

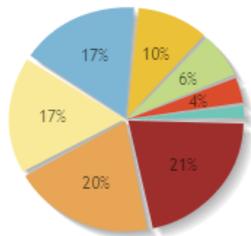


Unresolved Alarms vs Opened Tickets ?



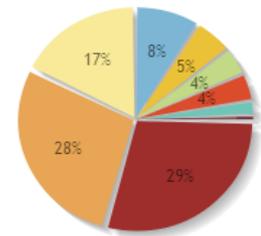
SIEM: Top 10 Events by Product Type ?

- Intrusion Detection
- Operating System
- Authentication and DHCP
- Router/Switch
- Server
- Anomaly Detection
- Infrastructure Monitoring
- Alarm
- Application



SIEM: Top 10 Event Categories ?

- Authentication
- System
- Application
- Exploit
- Suspicious
- Recon
- Alert
- Availability
- Alarm
- Policy



Análisis

- Eventos de seguridad.
- Alarmas.
- Tickets.

Eventos de seguridad

- Eventos capturados por Alien Vault:
 - Sensor que lo detectó.
 - Nombre.
 - Fecha.
 - IP origen.
 - IP destino.

Event details

Normalized Event	Date	Alienvault Sensor	Interface		
	2013-10-11 17:06:20 GMT-5:00	alienvault: [redacted]	eth0		
Normalized Event	Triggered Signature	Event Type ID	Category	Sub-Category	
	snort: "ET SCAN Potential SSH Scan OUTBOUND"	2003068	Recon	Misc	
Normalized Event	Data Source Name	Product Type	Data Source ID		
	snort	Intrusion Detection	1001 		
Normalized Event	Source Address	Source Port	Destination Address	Destination Port	Protocol
	[Host: [redacted]]	48495	[redacted]	22	TCP
SIEM	Unique Event ID#	Asset S → D	Priority	Reliability	Risk
	32c111e3-9d64-0024-e847-bdee5bd590be	2->2	2	1	0
Context	Event Context information is only available in AlienVault USM Server				
KDB	<ul style="list-style-type: none"> ▶ AlienVault Incident Response: Recon / Misc [Taxonomy] ▶ AlienVault Incident Response: Recon [Taxonomy] 				
Payload	none				
	 Snort rule Detection				

Alarmas

- Número máximo de ocurrencias de un mismo tipo de evento.
 - Fecha.
 - Estado de la alarma.
 - Método usado.
 - Nivel de riesgo.
 - IP origen y destino.

Date	Status	Intent & Strategy	Method	Risk	Attack pattern	Source	Destination
12:49:33	open	 Bruteforce Authentication	SSH	1			alienvault
4 hours		 WebServer Attack	XSS	1			alienvault

Tickets

- Asignar a usuario el seguimiento de evento.

New Ticket

Title *	ossec: SSHD authentication success.
Assign To *	User: <input type="text" value="- Select one user -"/>
Priority *	<input type="text" value="1"/>
Type *	<input type="text" value="Anomalies"/>
Source Ips	<input type="text" value="██████████"/>
Dest Ips	<input type="text" value="██████████"/>
Source Ports	<input type="text" value="4547"/>
Dest Ports	<input type="text" value="0"/>
Start of related events	<input type="text" value="2013-10-11 19:49:42"/>
End of related events	<input type="text" value="2013-10-11 19:49:42"/>

Activos

Host: [REDACTED]

IP Address [REDACTED]	FQDN -	Device Type -	Description -
Operating System Linux:2.6	Networks Pvt_010 ([REDACTED]/24)	Asset Type Internal	
Asset Value 1 2 3 4 5	Sensors [REDACTED] (alienvault)	Host Status Unknown	

Snapshot

0
Software Packages

0
Users

37
Vulnerabilities

Yes
Alarms

Yes
Events

- HIDS
- Automatic Asset Discovery
- Availability Monitoring

General | Activity | Notes

Software | **Services** | Users | Properties

[Edit Availability Monitoring](#)

	IP Address	Port	Name	Vulnerable	Available
+	[REDACTED]	22	ssh	Yes	Yes

Nagios

View Service Status Detail For All Host Groups
 View Host Status Detail For All Host Groups
 View Status Summary For All Host Groups
 View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
9	1	0	0

All Problems	All Types
1	10

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
33	0	0	4	0

All Problems	All Types
4	37



Service Overview For All Host Groups

PING (PING)

Host	Status	Services	Actions
Host: [redacted]	UP	4 OK	[Icons]

Windows_Server (Windows_Server)

Host	Status	Services	Actions
Host: [redacted]	UP	4 OK	[Icons]

ajp13 (ajp13)

Host	Status	Services	Actions
Host: [redacted]	UP	4 OK	[Icons]

All Servers (all)

Host	Status	Services	Actions
Host: [redacted]	UP	3 OK	[Icons]
Host: [redacted]	UP	4 OK	[Icons]
Host: [redacted]	DOWN	4 CRITICAL	[Icons]

Debian GNU/Linux Servers (debian-servers)

Host	Status	Services	Actions
localhost	UP	6 OK	[Icons]

dns (dns)

Host	Status	Services	Actions
Host: [redacted]	UP	1 OK	[Icons]

Análisis de vulnerabilidades

Modify Scan Job

Job Name:

Select Server:

Profile: [Edit Profiles]

Schedule Method:

Begin in Year Month Day

Weekly

Frequency Every week(s)

Time Hour Minutes

► Advanced

Only scan hosts that are alive (greatly speeds up the scanning process)

Pre-Scan locally (do not pre-scan from scanning sensor)

Do not resolve names

Type here to search assets (Hosts/Networks)

Pvt_010 /24

All Assets
Hosts
Host Groups
Networks
Network Groups

[X] Delete all

Escaneo vulnerabilidades

Overview | **Scan Jobs** | Threat Database

New Scan Job | Import nbe file | Profiles | Settings

Running Scans

No Running Scans

Scheduled Jobs

Name	Schedule Type	Time	Next Scan	Status	Action
scan net [redacted]	Weekly	00:00:00	2013-10-22 00:00:00	Enabled	[edit] [delete]
Scan net [redacted]	Weekly	00:00:00	2013-10-24 00:00:00	Enabled	[edit] [delete]
scan net [redacted]	Weekly	00:00:00	2013-10-25 00:00:00	Enabled	[edit] [delete]

All Scans

Job Name	Launch Time	Scan Start Time	Scan End Time	Scan Time	Next Scan	Action
SCHEDULED - scan net [redacted]	2013-10-18 00:00:02	2013-10-18 12:23:27	2013-10-18 14:05:02	101 mins	-	[warning] [Scan failed] [delete]
SCHEDULED - Scan net [redacted]	2013-10-17 00:00:02	2013-10-18 12:22:03	2013-10-18 14:25:46	123 mins	-	[warning] [info] [edit] [delete] (42)
SCHEDULED - scan net [redacted]	2013-10-15 12:03:02	2013-10-18 12:21:03	2013-10-18 14:25:42	124 mins	-	[warning] [info] [edit] [delete] (0)
SCHEDULED - Vulnerabilidades	2013-10-07 18:00:02	2013-10-07 18:00:03	2013-10-07 21:19:36	199 mins	-	[warning] [info] [edit] [delete] (1853)
SCHEDULED - scan net [redacted]	2013-08-21 17:54:22	2013-08-22 10:58:03	2013-08-22 11:51:57	53 mins	-	[warning] [info] [edit] [delete] (303)
SCHEDULED - scan net [redacted]	2013-08-21 15:00:02	2013-08-21 15:00:02	2013-08-21 21:07:46	367 mins	-	[warning] [info] [edit] [delete] (0)
SCHEDULED - scan net [redacted]	2013-08-21 14:30:03	2013-08-21 14:30:03	2013-08-21 14:36:13	6 mins	-	[warning] [info] [edit] [delete] (0)

[edit] [delete all]

Edit Availability Monitoring

	Vulnerable	Available
+ [redacted]	22	ssh
	Yes	Yes

Reporte de vulnerabilidades



▼ Current Vulnerabilities

Asset Vulnerability Details								
Host - IP	Date/Time	Profile	SEVER	HIGH	MED	LOW	INFO	
All	.	.	22	122	116	1926	755	
Host- [REDACTED]	2013-08-21 20:24:22	Ultimate	0	0	16	42	15	
Host- [REDACTED]	2013-10-07 21:16:35	Ultimate	0	6	4	37	15	

Directivas

- ▶ **User Contributed** [4 directives]
- ▶ **Alienvault Scada**
- ▶ **Alienvault Network**
- ▶ **Alienvault MISC** [1 directive]
- ▶ **Alienvault Scan** [15 directives]
- ▶ **Alienvault Policy** [10 directives]
- ▶ **Alienvault DoS**
- ▶ **Alienvault Malware** [33 directives]
- ▶ **Alienvault Attacks** [10 directives]
- ▶ **Alienvault BruteForce** [15 directives]

Edit Directive

Name for the directive

Taxonomy

Intent:

Strategy:

Method:

Priority

0
1
2
3
4
5

Directivas modificadas

▼ User Contributed [4 directives]

- ▶     AV-FREE-FEED Web attack, XSS attacks detected against DST_IP
Exploitation & Installation, WebServer Attack, XSS
- ▶     AV-FREE-FEED Network scan, SSH outbound scanning behaviour detected from SRC_IP
Reconnaissance & Probing, Scan from internal network, SSH Scanning
- ▶     AV-FREE-FEED Network scan, Microsoft Remote Desktop service discovery from SRC_IP
Reconnaissance & Probing, Service discovery, Microsoft Remote Desktop
- ▶     AV-FREE-FEED Network scan, SSH outbound scanning behaviour detected from SRC_IP
Delivery & Attack, WebServer Attack, Attack Pattern Detection

▼     AV-FREE-FEED Web attack, XSS attacks detected against DST_IP
Exploitation & Installation, WebServer Attack, XSS

▼ Rules

Name	Reliability	Timeout	Occurrence	From	To	Data Source	Event Type	[...]	Action
▼ XSS (Cross Site Scripting) attempt	4	None	1	◆ [REDACTED]	◆ ANY	◆ ossec-attack (7059)	◆ SIDs: 31154	▶ More	+
▼ XSS (Cross Site Scripting) attempt	6	360	1	◆ 1:SRC_IP	◆ 1:DST_IP	◆ ossec-attack (7059)	◆ SIDs: 31154	▶ More	◆     
XSS (Cross Site Scripting) attempt	8	43200	10000	◆ 1:SRC_IP	◆ 1:DST_IP	◆ ossec-attack (7059)	◆ SIDs: 31154	▶ More	◆     

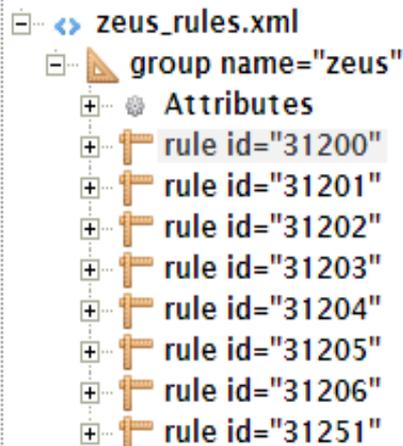
▶ Directive info

Reglas

Rules Files

Rule Editor

zeus_rules.xml



```
25 <group name="zeus,">
26   <rule id="31200" level="0">
27     <decoded_as>zeus</decoded_as>
28     <description>Grouping of Zeus rules.</description>
29   </rule>
30
31   <rule id="31201" level="0">
32     <if_sid>31200</if_sid>
33     <regex>^\[S+ \S+] INFO:|^\[S+ \S+] SSL:</regex>
34     <description>Grouping of Zeus informational logs.</description>
35   </rule>
36
37   <rule id="31202" level="4">
38     <if_sid>31200</if_sid>
39     <regex>^\[S+ \S+] WARN:</regex>
40     <description>Zeus warning log.</description>
41   </rule>
42
43   <rule id="31203" level="9">
44     <if_sid>31200</if_sid>
45     <regex>^\[S+ \S+] SERIOUS:</regex>
46     <description>Zeus serious log.</description>
47   </rule>
```

Alertas por correo

You can use the following keywords within any field which will be substituted by it's matching value upon action execution:

- DATE
- PLUGIN_ID
- PLUGIN_SID
- RISK
- PRIORITY
- RELIABILITY
- SRC_IP_HOSTNAME
- DST_IP_HOSTNAME
- SRC_IP
- DST_IP
- SRC_PORT
- DST_PORT
- PROTOCOL
- SENSOR
- BACKLOG_ID
- EVENT_ID
- PLUGIN_NAME
- SID_NAME
- USERNAME
- PASSWORD
- FILENAME
- USERDATA1
- USERDATA2
- USERDATA3
- USERDATA4
- USERDATA5
- USERDATA6
- USERDATA7
- USERDATA8
- USERDATA9

Name *	mail alert
Description *	<u>mail alert</u>
Type *	Send an email message ▼
Condition	<input type="radio"/> Any <input checked="" type="radio"/> Only if it is an alarm <input type="radio"/> Define logical condition
From: *	@alienvault.mx
To: *	
Subject: *	Alarm from known hostile host
Message: *	alarm SID_NAME triggered SRC_IP to target DST_IP over PROTOCOL

Update

Administración AlienVault

User login *	<input type="text"/>
User name *	<input type="text"/>
User email 	<input type="text"/>
User language *	English 
Timezone *	America/Mexico_City 
Company	UNAM CERT
Department	<input type="text"/>
Enter user password *	<input type="password"/> <div style="border: 1px solid orange; padding: 2px; display: inline-block;">strong</div>
Re-enter user password *	<input type="password"/>
Ask to change password at next login	<input checked="" type="radio"/> Yes <input type="radio"/> No
Make this user a global admin	<input checked="" type="radio"/> Yes <input type="radio"/> No
<p>▼ Allowed Menus</p> <p>Select / Unselect all</p> <hr/>	
<input checked="" type="checkbox"/>	Dashboard -> Overview
<input checked="" type="checkbox"/>	Dashboard -> Overview -> Manage Dashboards
<input checked="" type="checkbox"/>	Dashboard -> Overview -> Metrics
<input checked="" type="checkbox"/>	Dashboard -> Risk Maps
<input checked="" type="checkbox"/>	Dashboard -> Risk Maps -> Manage Risk Maps
<input checked="" type="checkbox"/>	Dashboard -> OTX (Open Threat Exchange)
<hr/>	
<input checked="" type="checkbox"/>	Analysis -> Security Events (SIEM)
<input checked="" type="checkbox"/>	Analysis -> Security Events (SIEM) -> Real Time
<input checked="" type="checkbox"/>	Analysis -> Security Events (SIEM) -> Delete Events
<hr/>	

Beneficios

- Aprendizaje de la red
- Centralizar bitácoras
- Detección de posibles ataques.
- Es compatible con la mayoría de los dispositivos actuales
- Actualización constante del sistema
- Presenta informes ejecutivos y técnicos
- Fácil Administración

Puntos débiles

- Limita al usuario *root*
- Conocer ampliamente el entorno de red
- No permite administrar la base de datos
- *No resuelve los problemas de seguridad*

```
root:~$ ls /  
*** forbidden path -> "/"  
*** You have 18 warning(s) left, before getting kicked out.  
This incident has been reported.  
root:~$ |
```

Oportunidades de mejora

- Comprar licencia AlienVault
- Sensores en diversas dependencias de la UNAM

¿Preguntas?