DGTIC UNAM CERT

2do Coloquio de Proyectos de Becarios en Seguridad Informática

SIEM
Implementación de un correlacionador de eventos

Juan Carlos Flores Ibarra

Edgar Israel Rubí Chávez

Antecendentes 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

Antecendentes SIEM

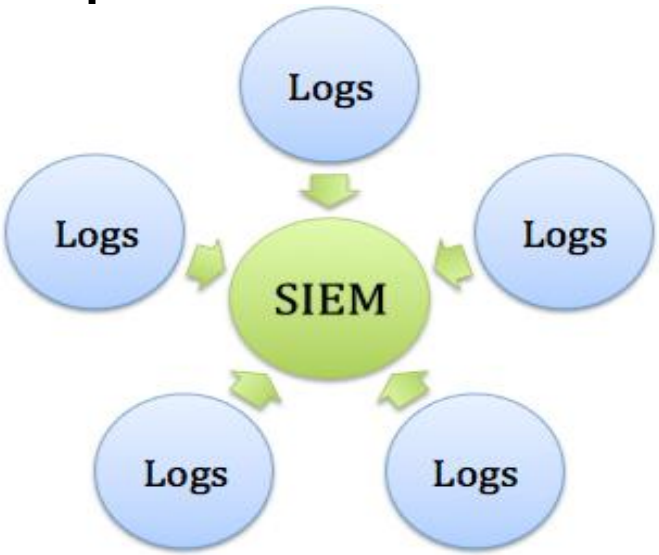
- SEC - Security Event Correlation
  - Analiza eventos y bitácoras
  - Busca patrones de comportamiento inusual
  - Alerta al responsable

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.




Análisis de vulnerabi-lidades
Monitoreo de servicios
Detección de ataques
SIEM
IDS
Conjunto de reglas

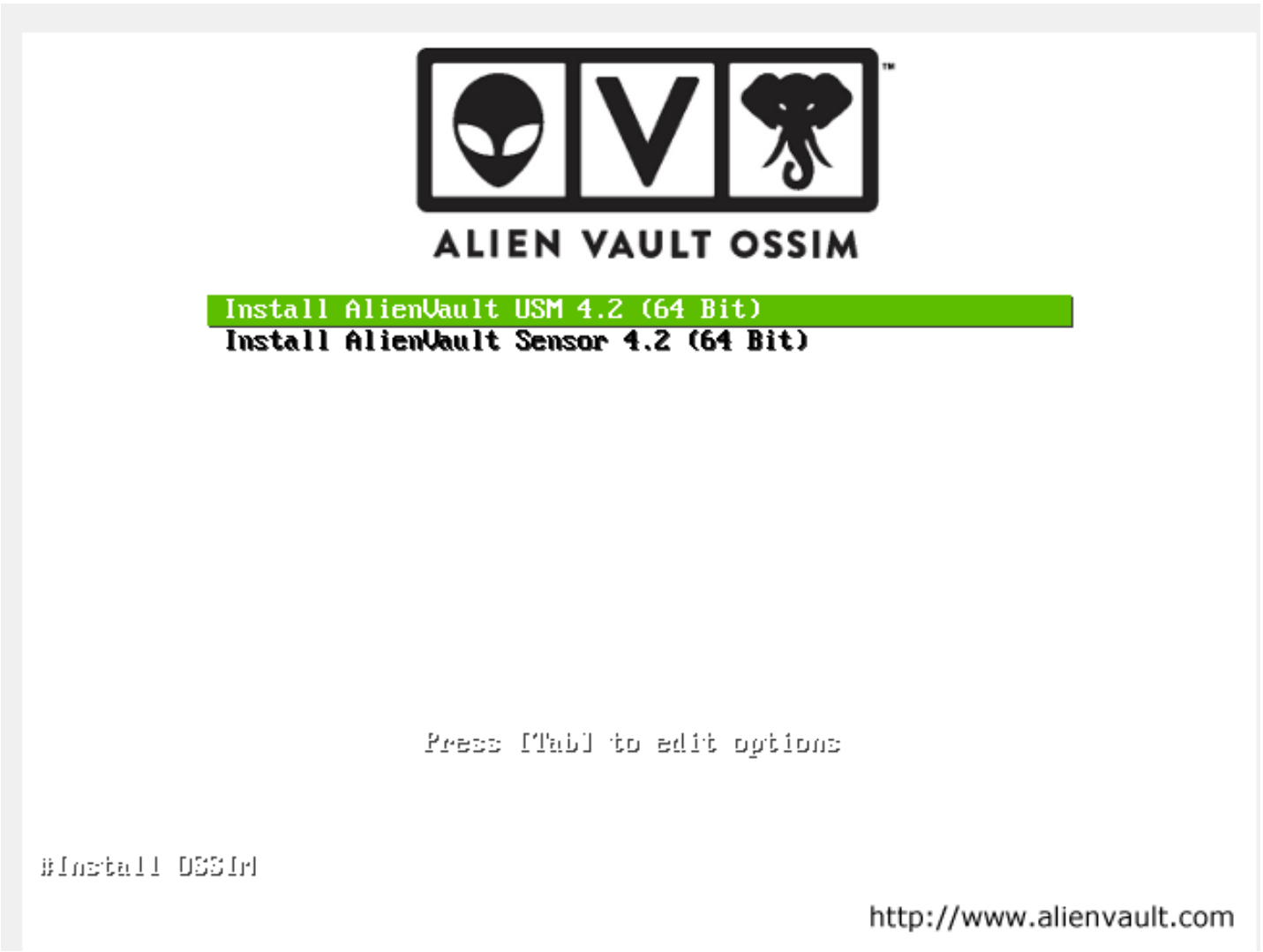
SIEM – Open Source

- 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
Cyberoam iView	✓	✓	✓	✓	✓	✓	Fortinet, SonicWall	✓	✓	http://www.cyberoam-iview.org/
AlienVaultOSSIM	✓	✓	✓	✓	✓	✓	Fortinet, Cisco	✓	✓	http://communities.alienvault.com/
Logalyze	✗	✓	✓	✓	✓	✓	Cisco, Juniper, etc.	✓	✓	http://www.logalyze.com/
bitsum	✓	✗	✓	✗	✓	✗	✗	✓	✗	http://bitsum.com/

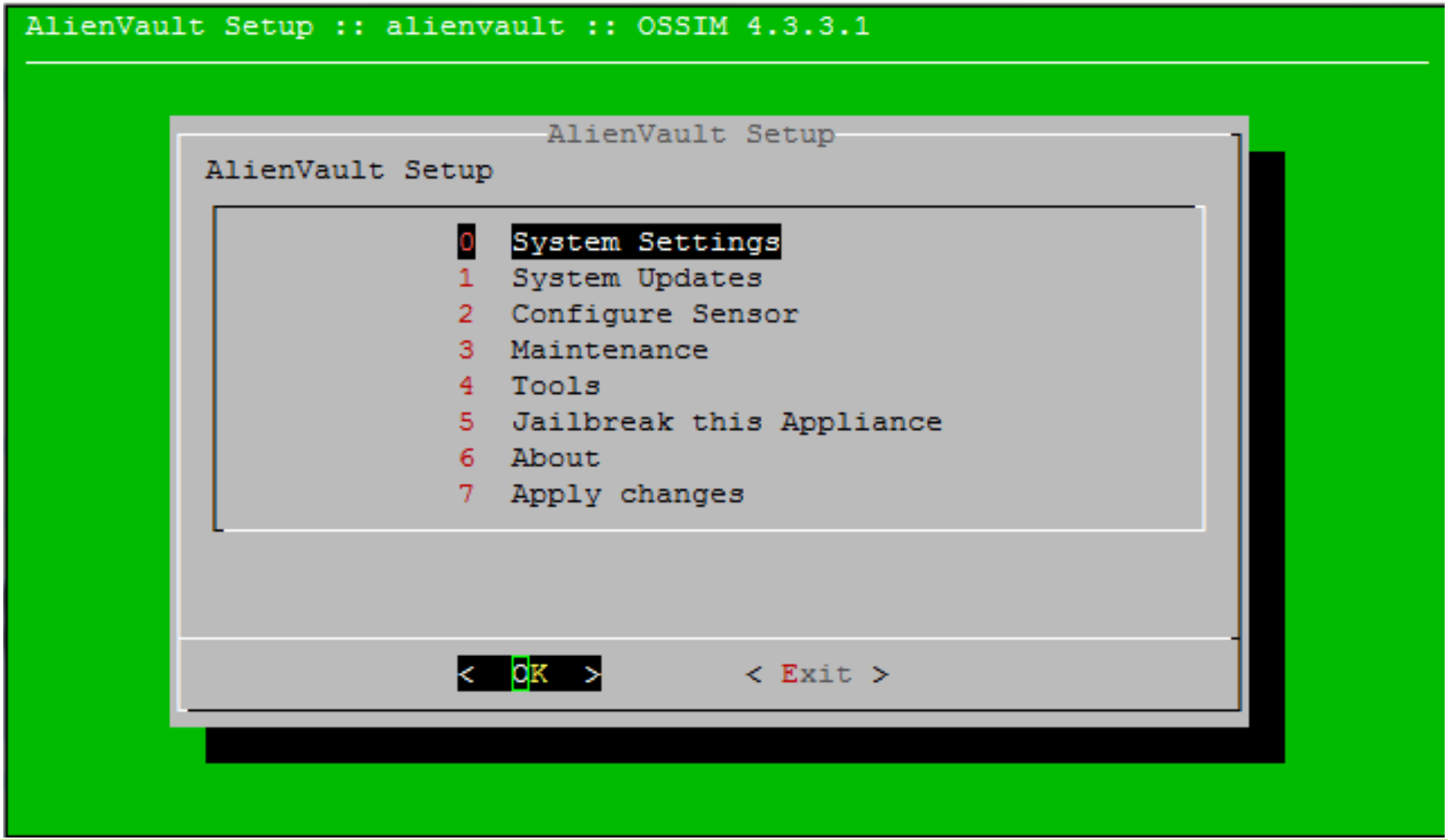
ALIEN VAULT OSSIM



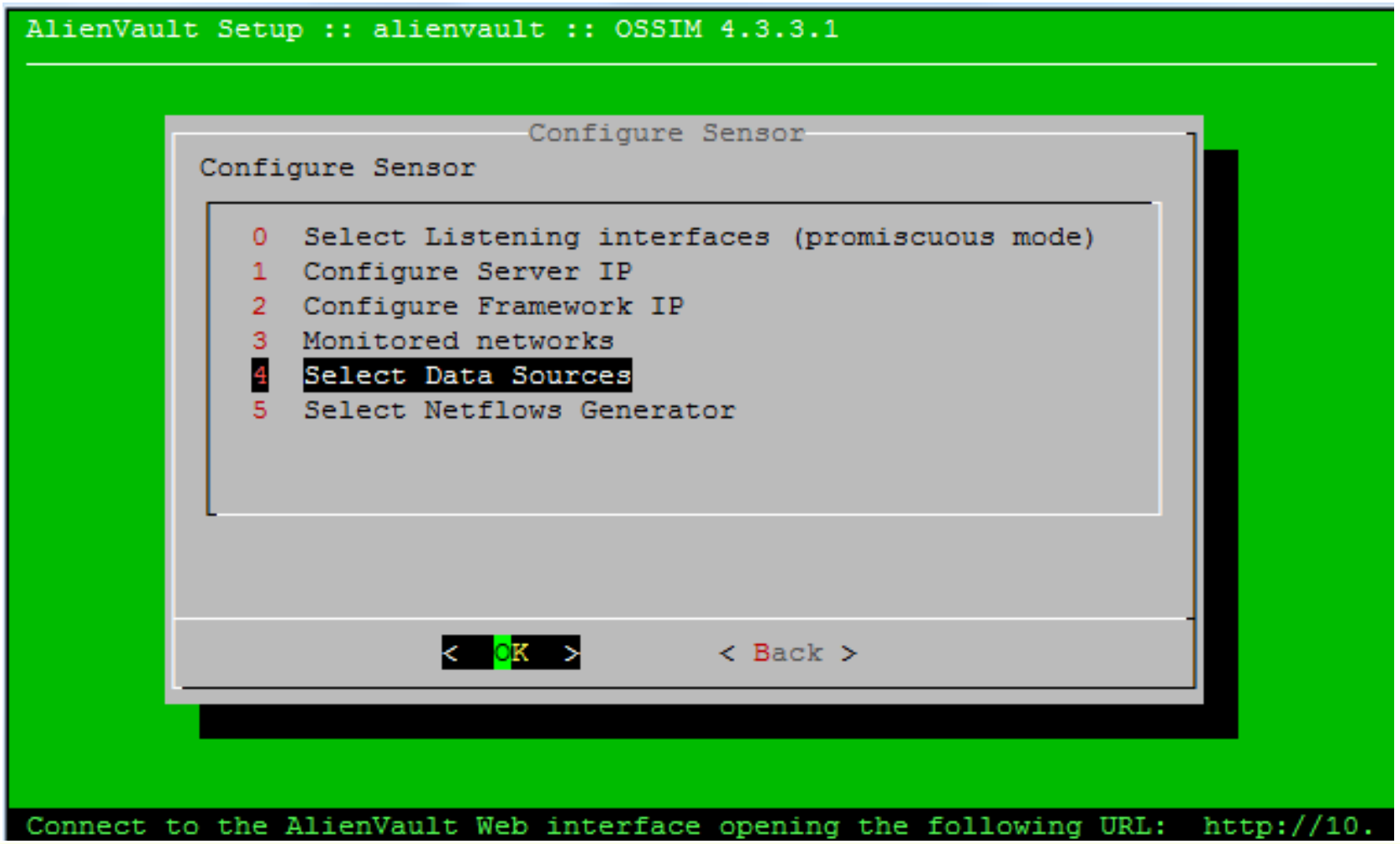
Instalación

- 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



Configuración sensor



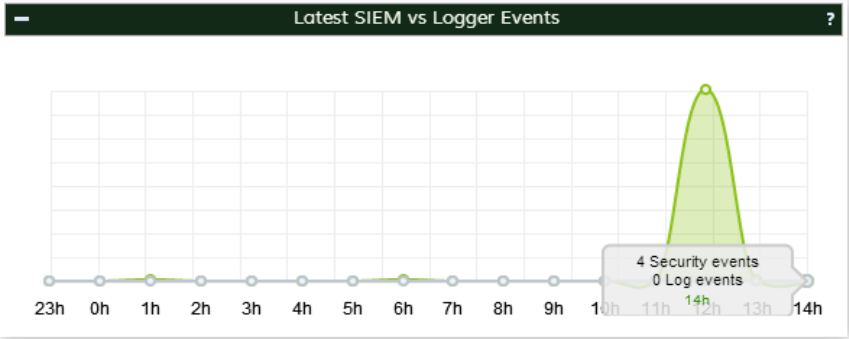
Recursos

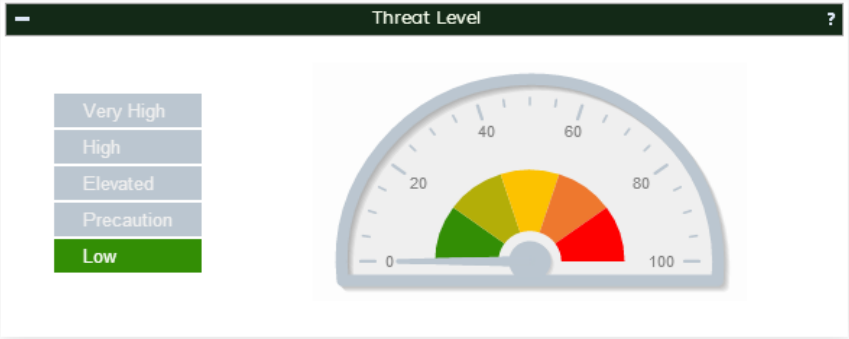
- Arpwatch
- Cisco-router
- DHCP
- Fortigate
- Nagios
- Pam-unix
- SSH
- Sudo
- Syslog
- Rsyslog
- Snort
- PHP
- Switch-Cisco
- Nmap-monitor

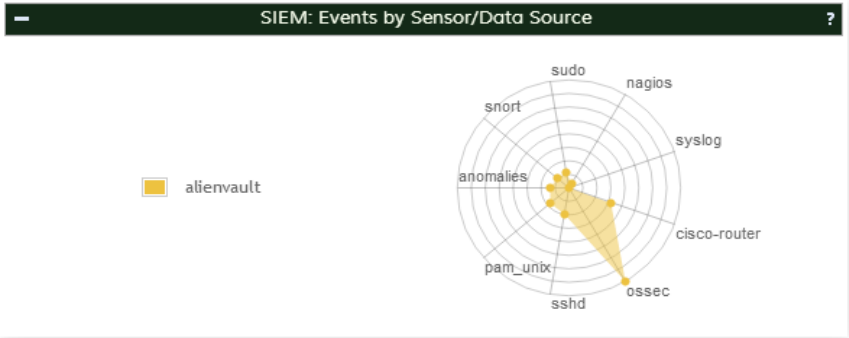
DGTIC UNAM CERT

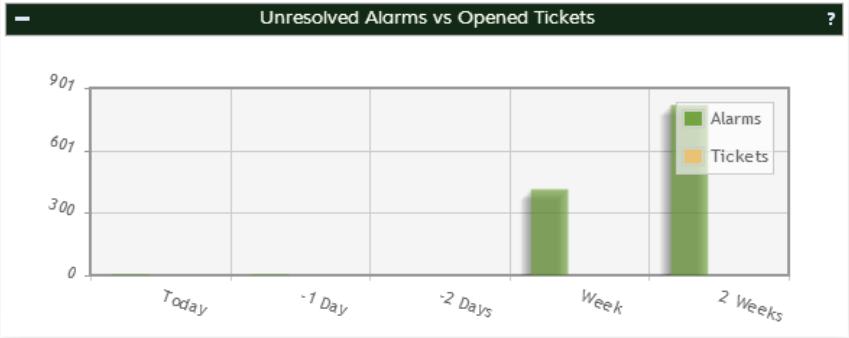
2do Coloquio de Proyectos de Becarios en Seguridad Informática

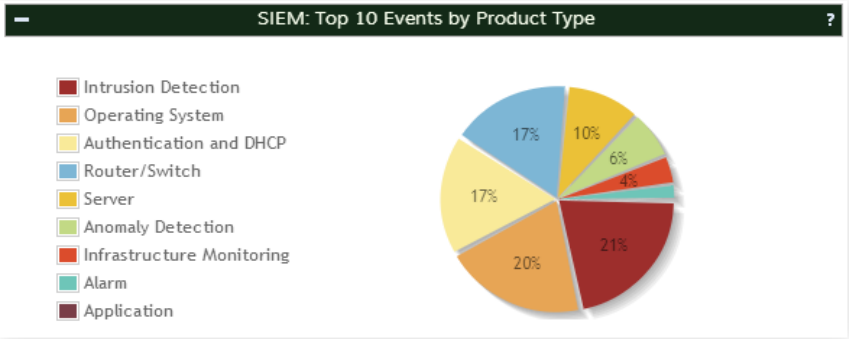
Resumen

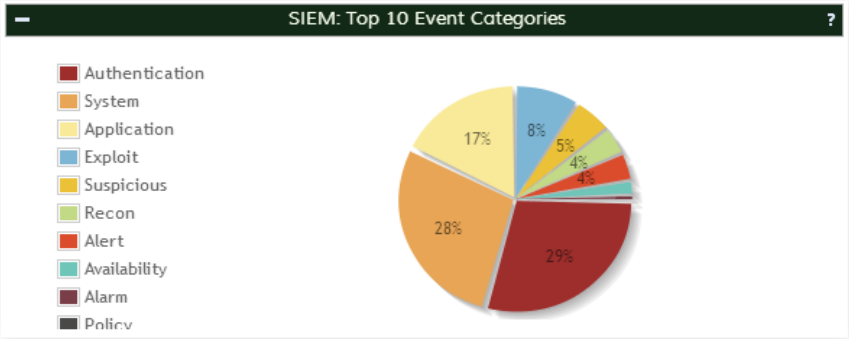










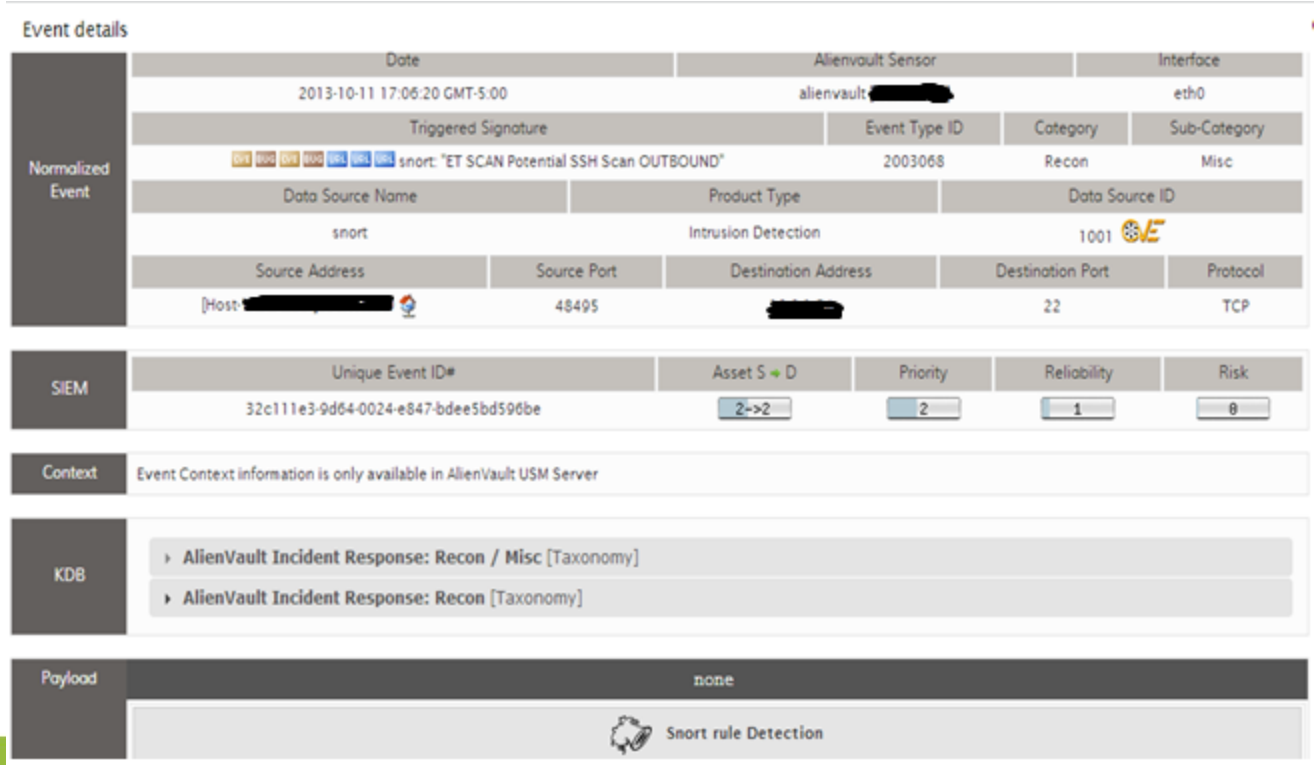


Análisis

- Eventos de seguridad.
- Alarmas.
- Tickets.

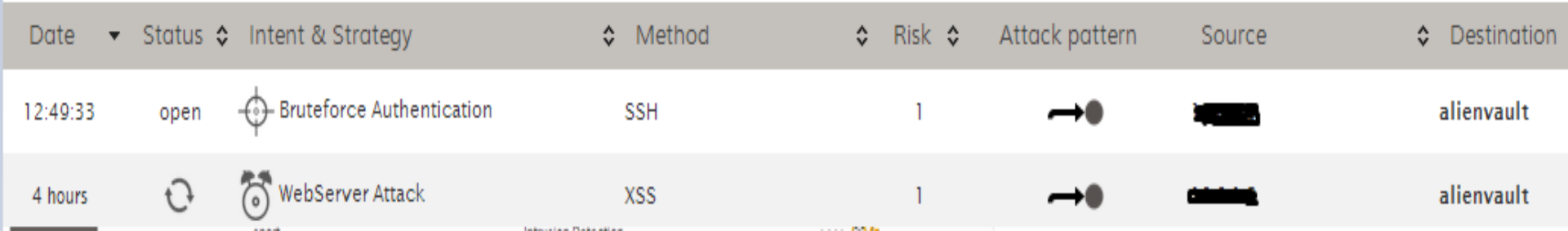
Eventos de seguridad

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



Alarmas

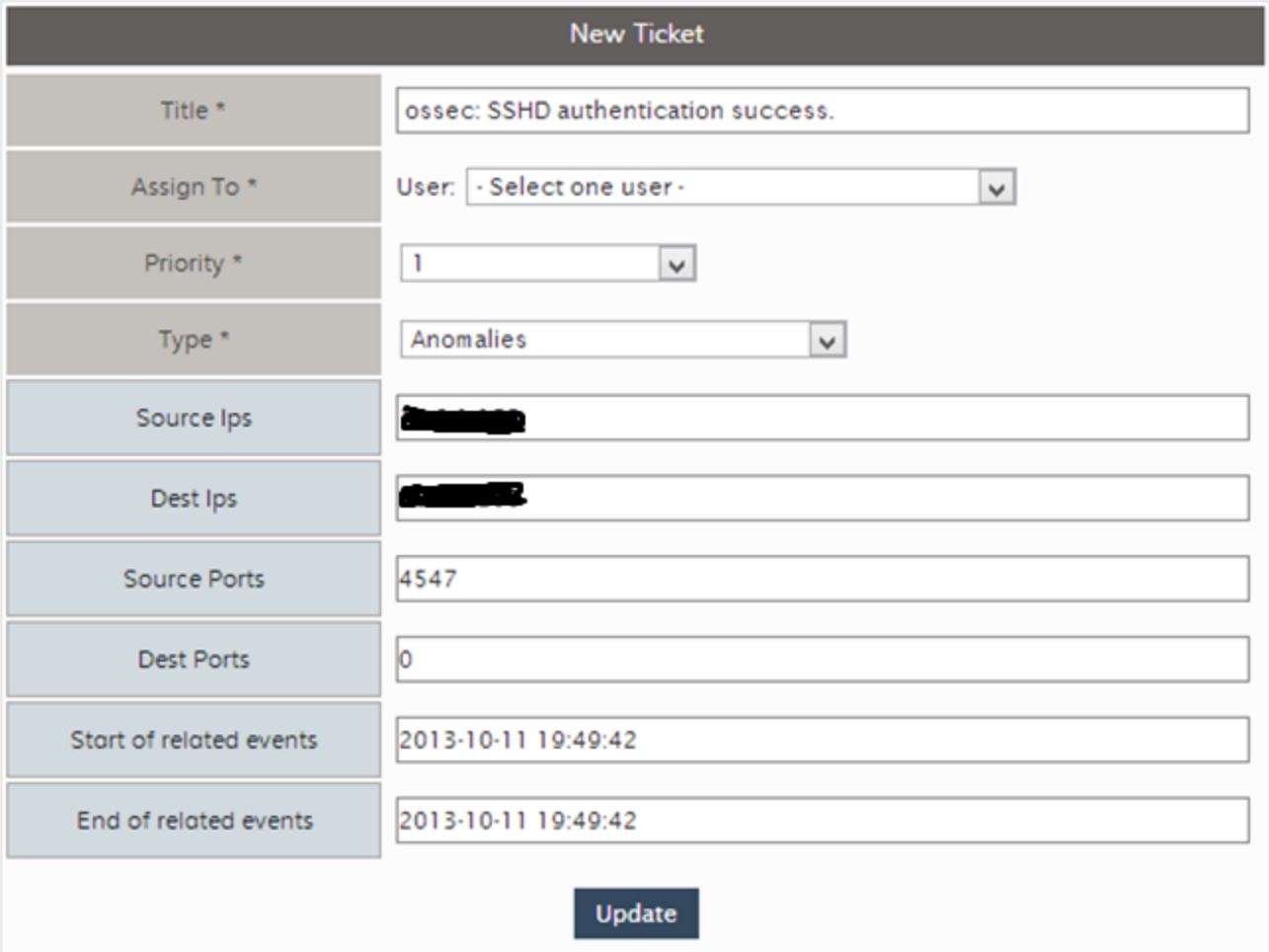
- Número máximo de ocurrencias de un mismo tipo de evento.
  - Fecha.
  - Estado de la alarma.
  - Método usado.
  - Nivel de riesgo.
  - IP origen y destino.



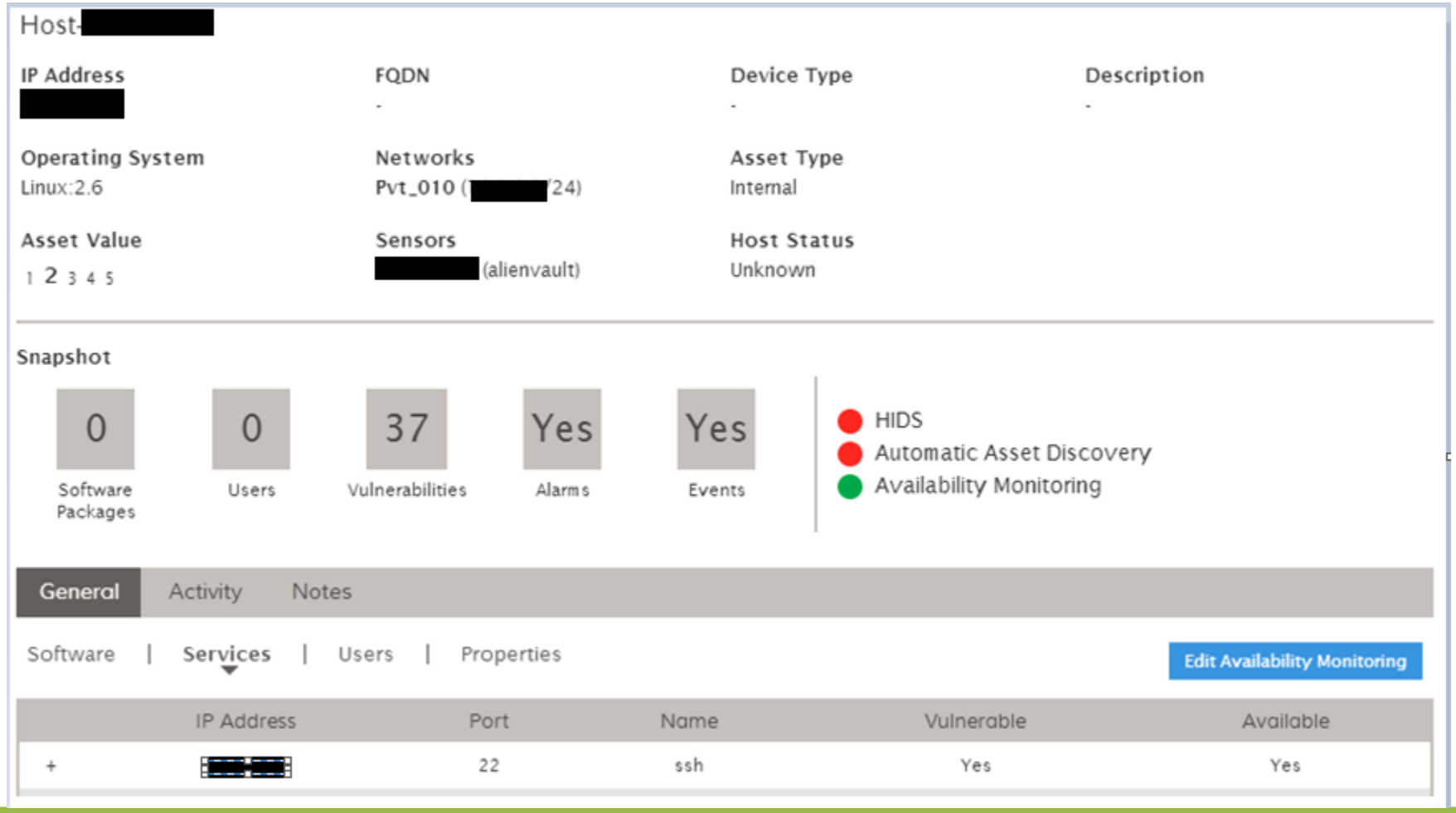
Date	Status	Intent & Strategy	Method	Risk	Attack pattern	Source	Destination
12:49:33	open	Bruteforce Authentication	SSH	1		[redacted]	alienvault
4 hours		WebServer Attack	XSS	1		[redacted]	alienvault

Tickets

- Asignar a usuario el seguimiento de evento.



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	

Windows_Server (Windows_Server)

Host	Status	Services	Actions
Host-[redacted]	UP	4 OK	

ajp13 (ajp13)

Host	Status	Services	Actions
Host-[redacted]	UP	4 OK	

All Servers (all)

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

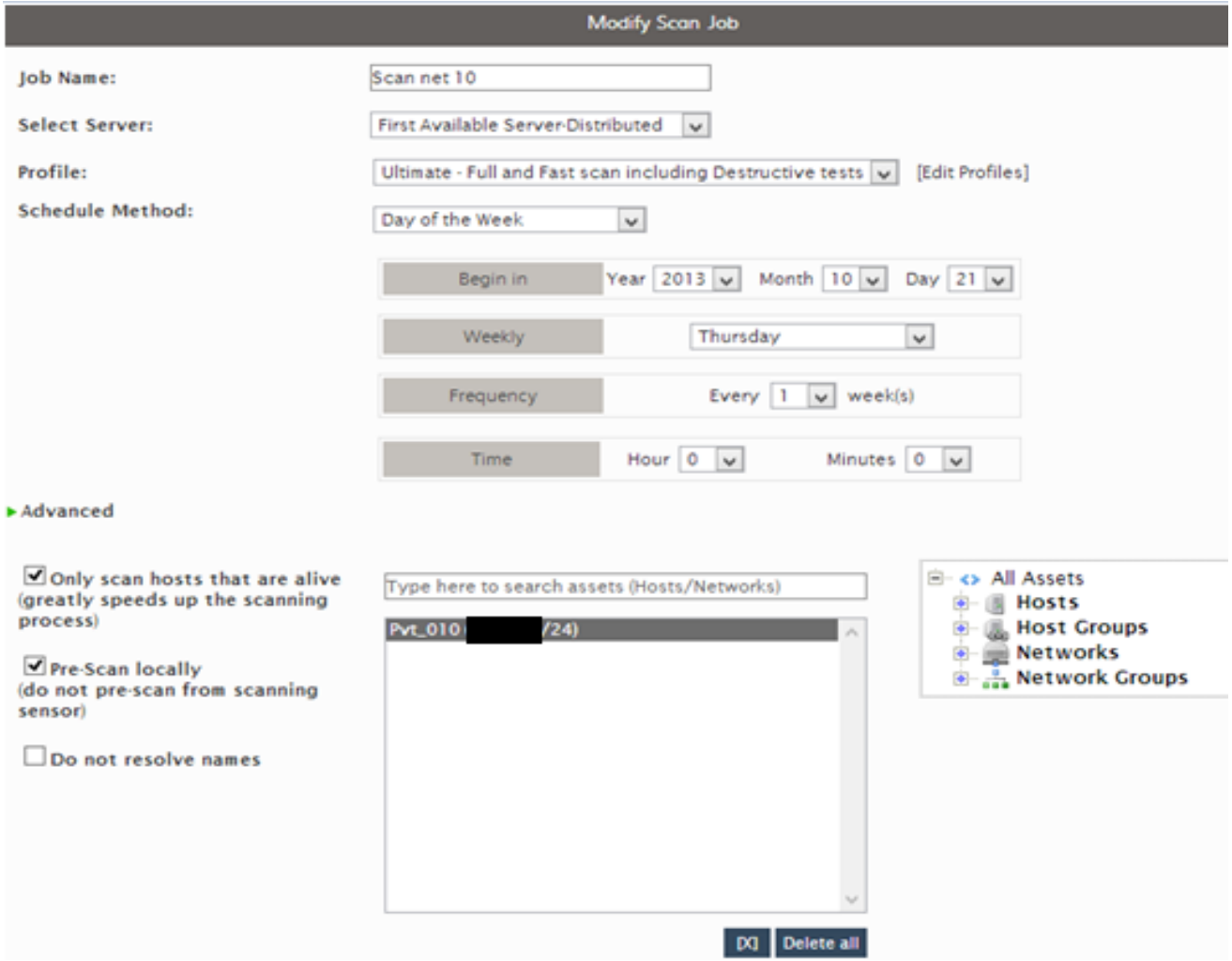
Debian GNU/Linux Servers (debian-servers)

Host	Status	Services	Actions
localhost	UP	6 OK	

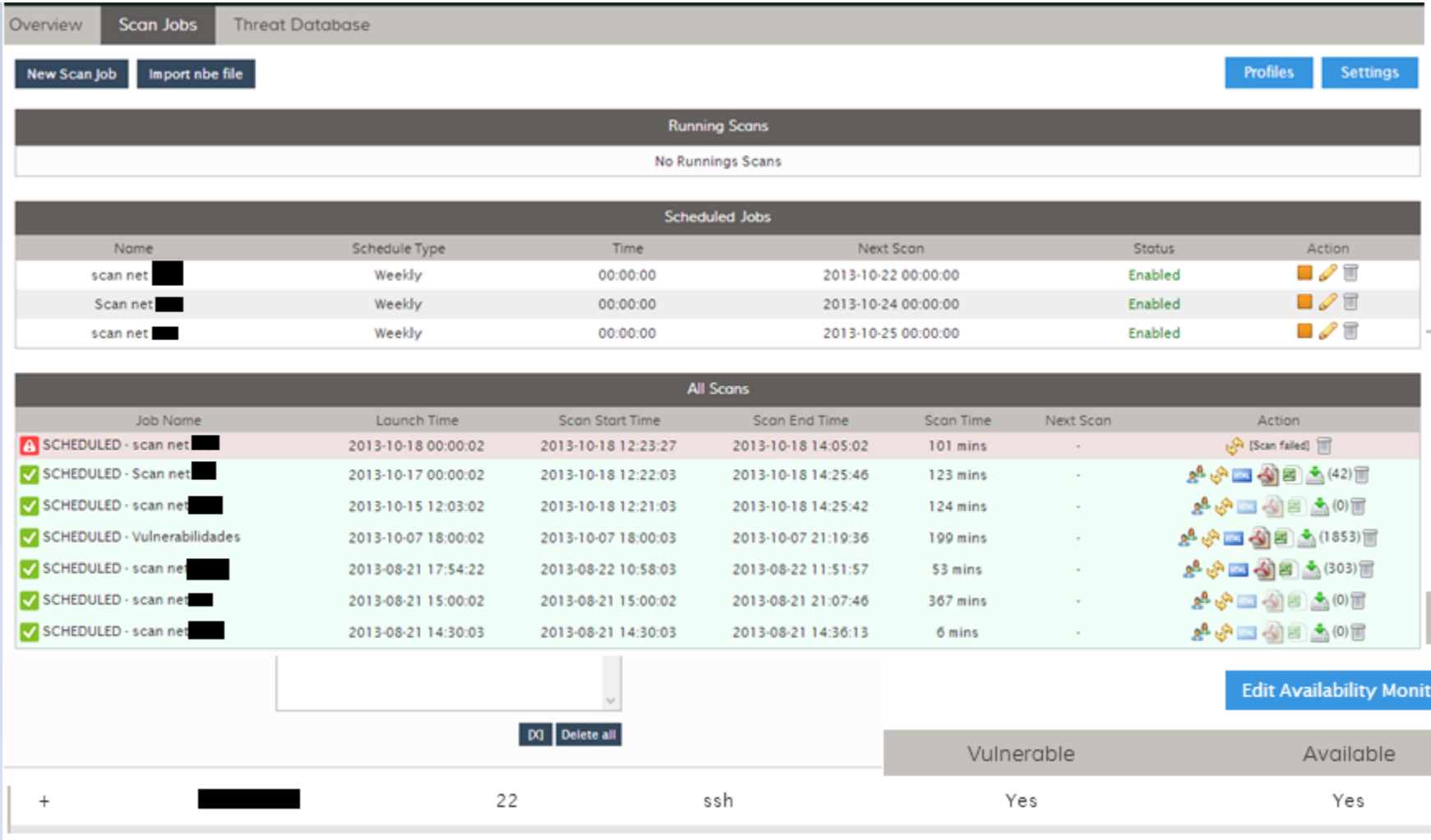
dns (dns)

Host	Status	Services	Actions
Host-[redacted]	UP	1 OK	

Análisis de vulnerabilidades



Escaneo vulnerabilidades



Reporte de vulnerabilidades

▼ Current Vulnerabilities

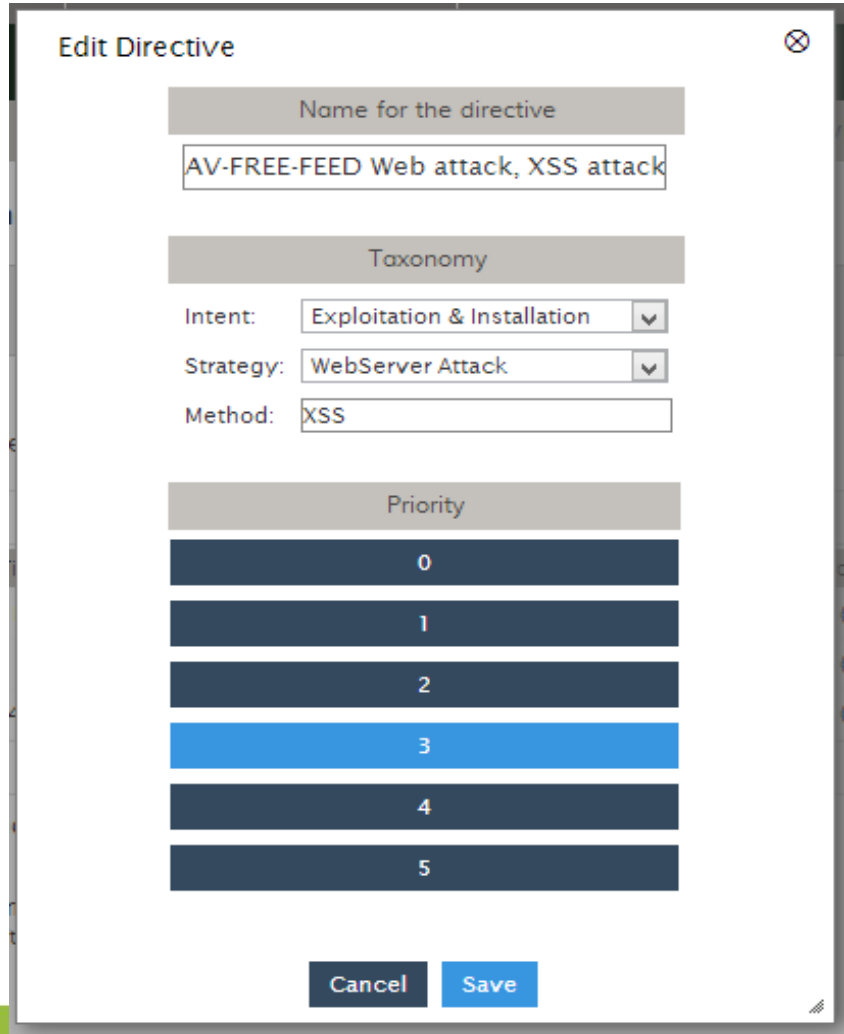
Asset Vulnerability Details

New Scan Job | Service | Free text | Host/Net | Find

Host - IP	Date/Time	Profile	SERI	HIGH	MEDI	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]



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

DGTIC UNAM CERT

2do Coloquio de Proyectos de Becarios en Seguridad Informática

Reglas

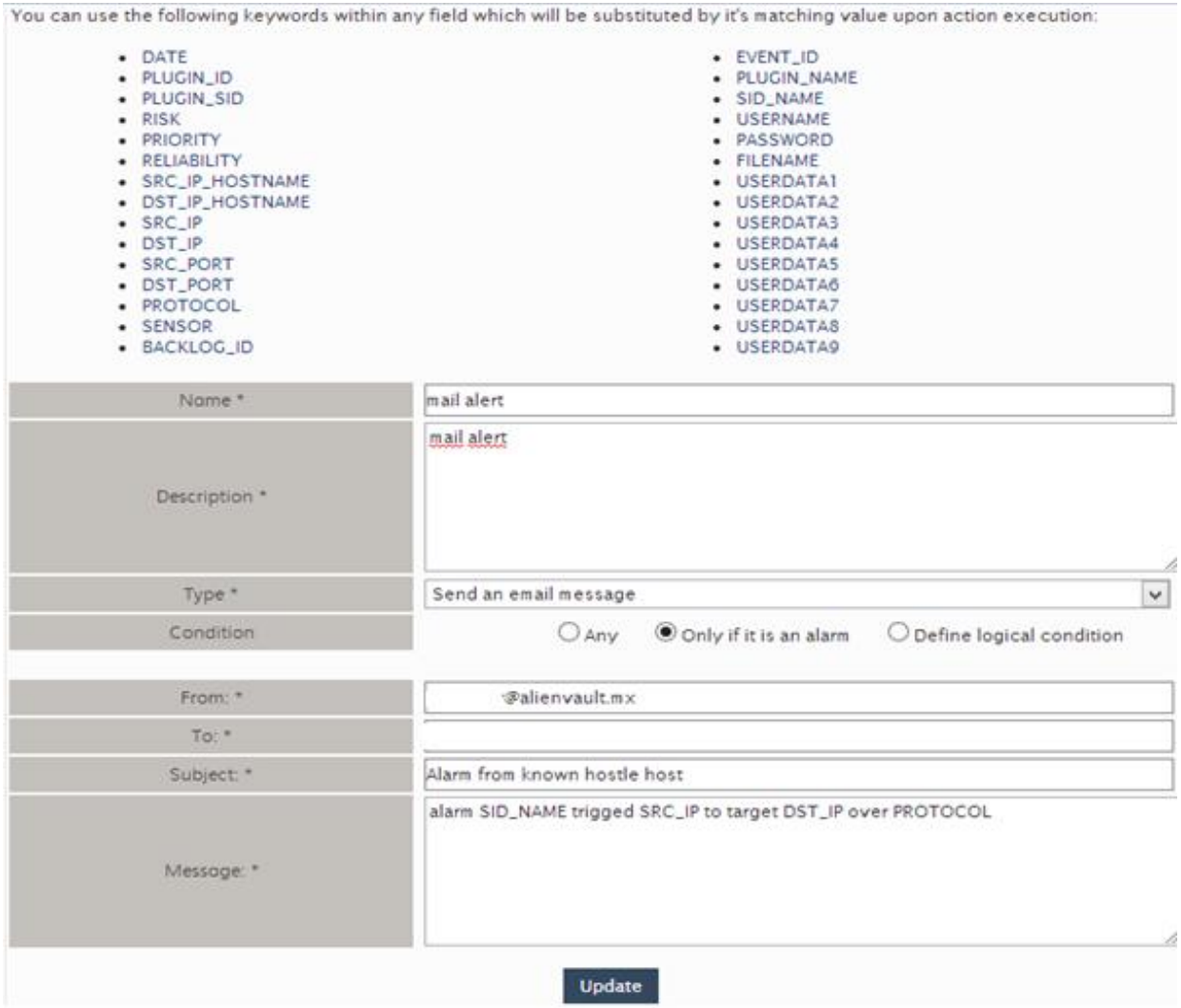
Rules Files | Rule Editor

zeus_rules.xml

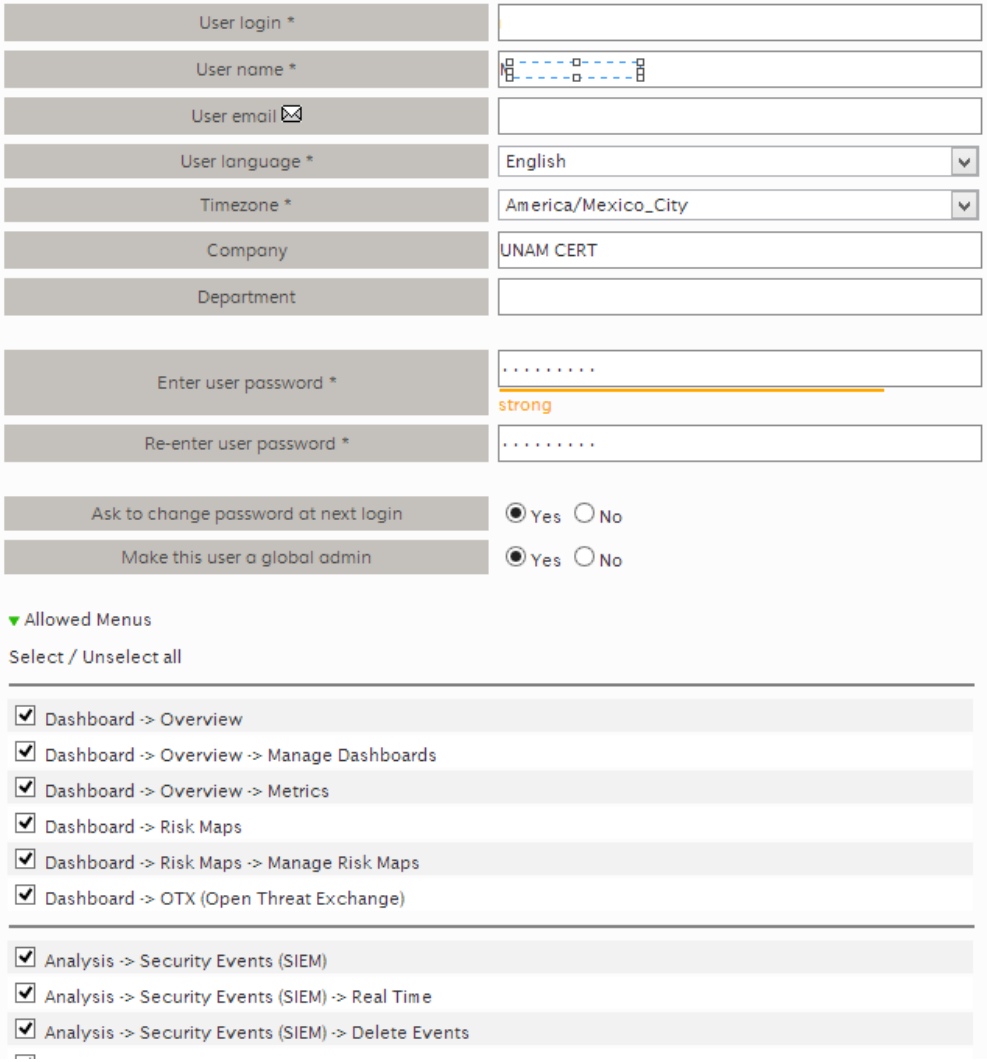
- zeus_rules.xml
  - group name="zeus"
    - Attributes
    - rule id="31200"
    - rule id="31201"
    - rule id="31202"
    - rule id="31203"
    - rule id="31204"
    - rule id="31205"
    - rule id="31206"
    - rule id="31251"

```
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



Administración AlienVault



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?