OSSIM技术研究

安全团队　靳晓飞

主要内容

- OSSIM简介
- OSSIM部署
- OSSIM应用
- OSSIM常见问题

OSSIM简介

- OSSIM是什么？
- OSSIM的主要功能和特点
- OSSIM系统架构

OSSIM是什么？

OSSIM是什么？

OSSIM	Unified Security Management
Open Source	Starts at $3900
Community-Supported Threat Intelligence	Weekly Updates from AlienVault Labs Threat Intelligence
Limited Log Collection & Log Retention Only for SIEM Events	Robust Log Management, Log Search & Long-Term Log Retention
3 High-Level Reporting Templates	150+ Customizable Reports, Including Compliance-Specific Report

OSSIM是什么？

设计思想：以资产为核心

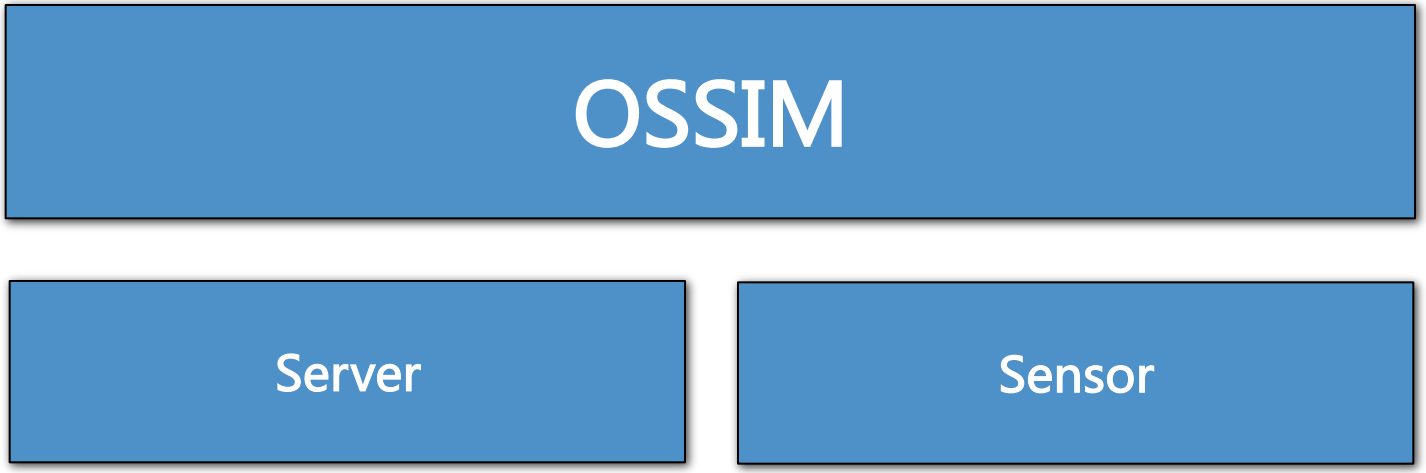
产品定位：集成解决方案，并非开发新的安全功能

OSSIM的主要功能和特点

OSSIM的主要功能和特点

- 集成了主流的开源安全工具/系统
- 提供友好、统一、可视化的管理界面
- 关联分析
- 以资产为核心
- 多种开发语言
- 部署速度快

OSSIM系统架构



主要内容

- OSSIM简介
- OSSIM部署
- OSSIM应用
- OSSIM常见问题

OSSIM部署

- 部署OSSIM后的安全收益
- OSSIM部署方式
- 部署前的准备工作
- OSSIM部署实战

部署OSSIM后的安全收益

- 可提供多种安全功能
- 部署速度快，成本低
- 方便管理
- 提升对恶意攻击的主动发现能力
- 提升对安全事件的应急响应能力

OSSIM部署方式

- 单机部署
- 分布式部署

部署前的准备工作

- OSSIM知识储备
- 硬件准备及IP地址规划
- 了解网络架构，确定部署方式和监控范围

OSSIM部署实战

- 背景介绍
- OSSIM部署实战

背景介绍

实验环境： 三台测试机

部署方式： 分布式部署

Server： 192.168.25.5

Sensor：192.168.25.6

Linux： 192.168.25.7

主要内容

- OSSIM简介
- OSSIM部署
- OSSIM应用
- OSSIM常见问题

OSSIM应用

- 资产管理
- 漏洞扫描
- 入侵检测
- 安全策略配置
- 威胁情报交换

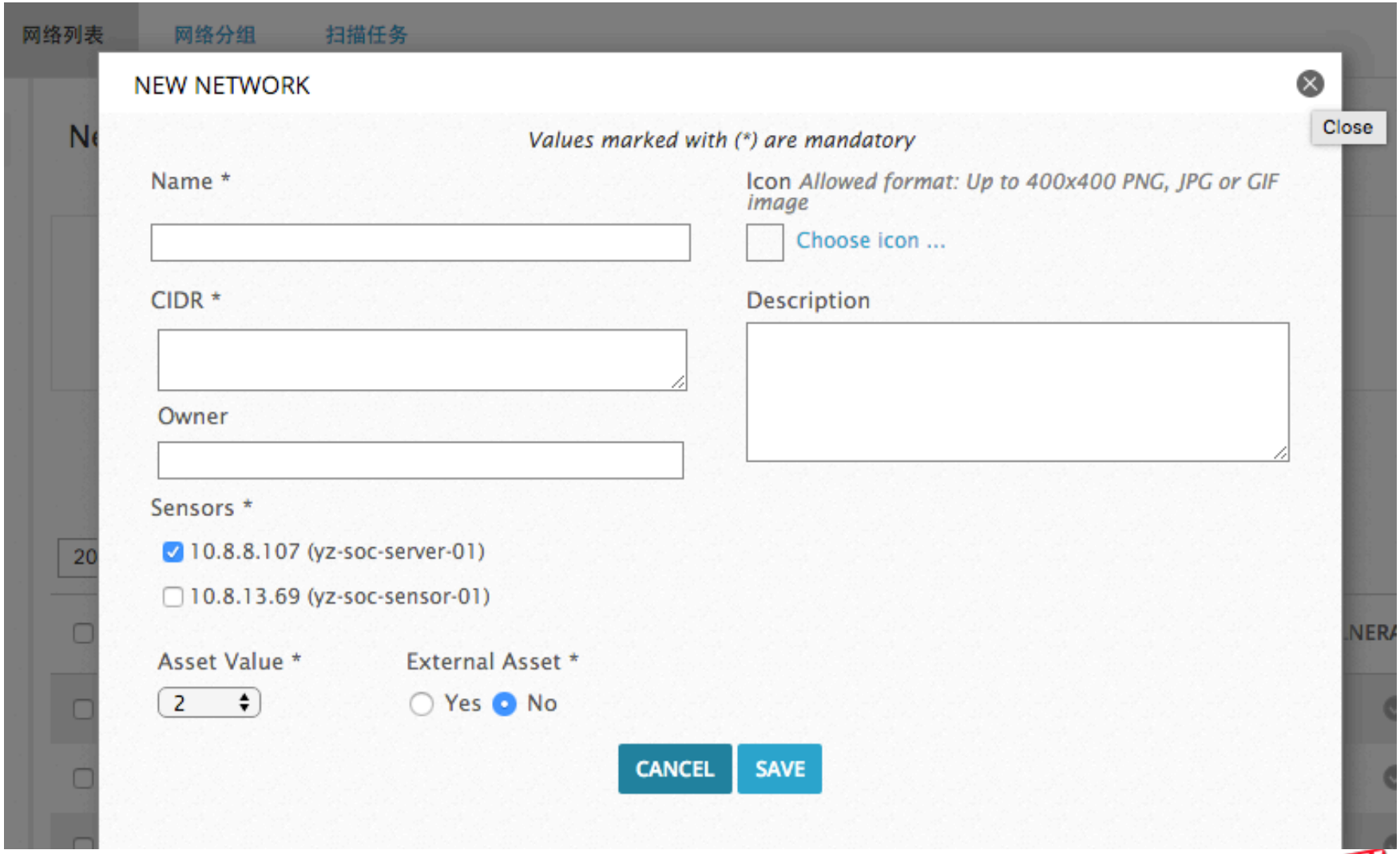
资产管理

添加网络

1. 手工添加

2. 从CSV文件导入

添加网络


网络列表
网络分组
扫描任务
NEW NETWORK
Close
Values marked with (*) are mandatory
Name *
Icon Allowed format: Up to 400x400 PNG, JPG or GIF image
Choose icon ...
CIDR *
Description
Owner
Sensors *
10.8.8.107 (yz-soc-server-01)
10.8.13.69 (yz-soc-sensor-01)
Asset Value *
2
External Asset *
Yes
No
CANCEL
SAVE

添加网络

IMPORT NETWORKS FROM CSV

Choose a CSV file:

选择文件 未选择任何文件

☐ Ignore invalid characters (Net names)

IMPORT

Formats allowed:

Version 4.x.x, 5.x.x:

Format: *"Netname";"CIDRs(CIDR1,CIDR2,...)";"Description";"Asset Value";"Net ID"*
Header: *"Netname";"CIDRs";"Description";"Asset Value";"Net ID"*
Example: *"Net-1";"192.168.10.0/24,192.168.9.0/24";"Short description";"2";"479D45C0BBF22B4458BD2F8EE09ECAC2"*

Version 3.x.x:

Format: *"Netname";"CIDRs(CIDR1,CIDR2,...)";"Description";"Asset Value";"Sensors(Sensor1,Sensor2,...)"*
Header: *"Netname";"CIDRs";"Description";"Asset Value";"Sensors"*
Example: *"Net-1";"192.168.10.0/24,192.168.9.0/24";"Short description";"2";"192.168.10.2,192.168.10.3"*

Notes:

- Characters allowed for net names: [A-Za-z0-9], '.' (dot), ':' (colon), '_' (underscore) and '-' (hyphen)
- Netname, CIDR and sensor fields cannot be empty

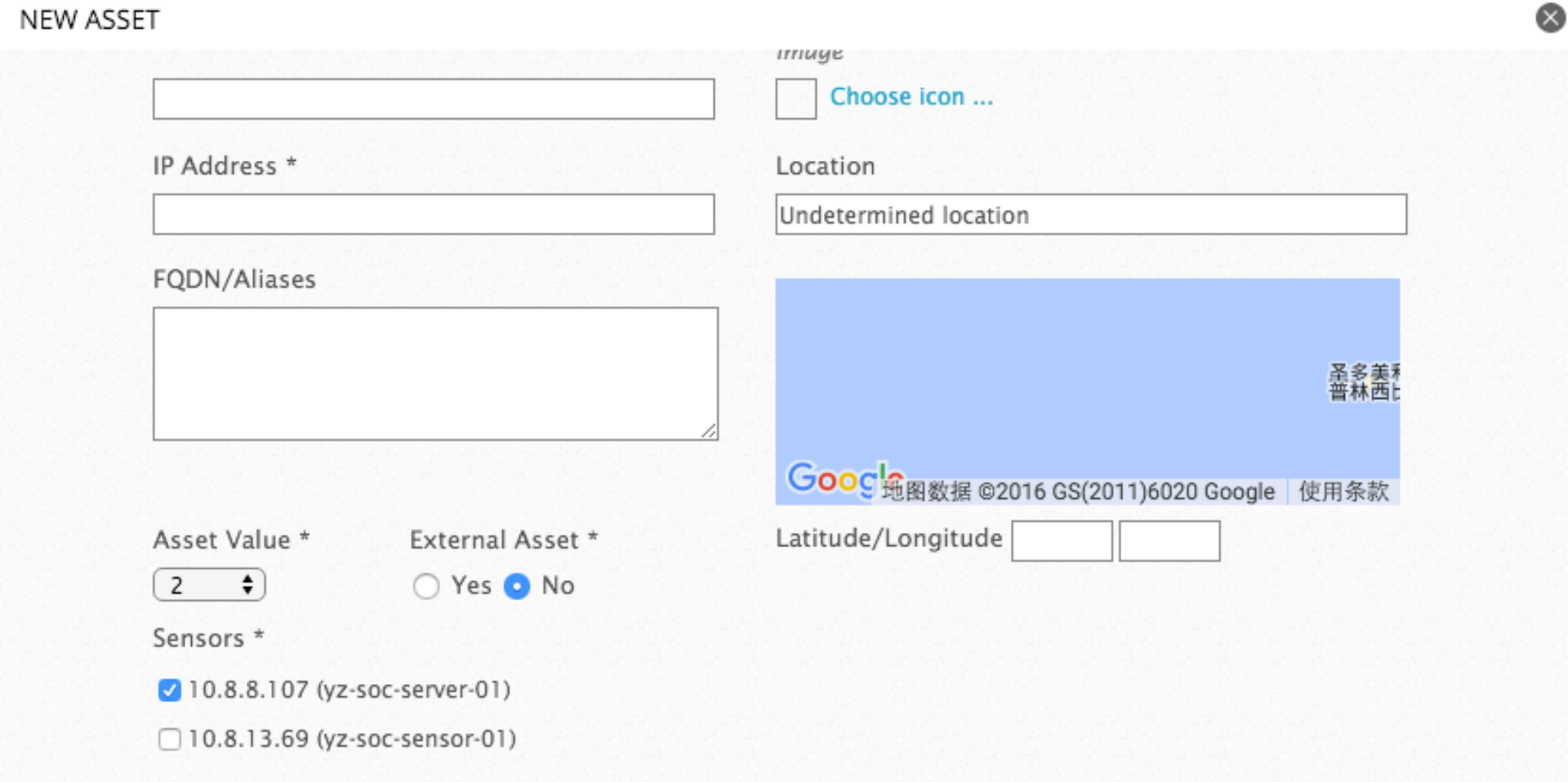
添加网络

NETWORK	CIDR	OWNER(S)	SENSORS	ALARMS	VULNERABILITIES	EVENTS
yz-idc-10.8.9.0	10.8.9.0/24	xiaofeijin	yz-soc-sensor-01	-	✓	-
yz-idc-10.8.8.0	10.8.8.0/24	xiaofeijin	yz-soc-server-01	✓	✓	✓
yz-idc-10.8.7.0	10.8.7.0/24	xiaofeijin	yz-soc-server-01	✓	✓	✓
yz-idc-10.8.6.0	10.8.6.0/24	xiaofeijin	yz-soc-server-01	✓	✓	✓
yz-idc-10.8.5.0	10.8.5.0/24	xiaofeijin	yz-soc-server-01	✓	✓	✓
yz-idc-10.8.4.0	10.8.4.0/24	xiaofeijin	yz-soc-server-01	✓	✓	✓
yz-idc-10.8.3.0	10.8.3.0/24	xiaofeijin	yz-soc-server-01	✓	✓	✓
yz-idc-10.8.248.0	10.8.248.0/24	xiaofeijin	yz-soc-sensor-01	-	-	-
yz-idc-10.8.2.0	10.8.2.0/24	xiaofeijin	yz-soc-server-01	✓	✓	✓
yz-idc-10.8.14.0	10.8.14.0/24	xiaofeijin	yz-soc-sensor-01	-	✓	-

发现资产

1. 手工添加
2. 从CSV文件导入
3. 从SIEM事件中导入
4. 通过扫描发现资产

发现资产


NEW ASSET
Image
Choose icon ...
IP Address *
Location
Undetermined location
FQDN/Aliases
Google
地图数据 ©2016 GS(2011)6020 Google
使用条款
Asset Value *
External Asset *
Latitude/Longitude
2
Yes
No
Sensors *
10.8.8.107 (yz-soc-server-01)
10.8.13.69 (yz-soc-sensor-01)

发现资产

IMPORT ASSETS FROM CSV

Choose a CSV file:

选择文件 未选择任何文件 Ignore invalid characters (Hostnames)

IMPORT

Formats allowed:

Version 4.x.x, 5.x.x:

Format: *"IPs(IP1,IP2,...)";"Hostname";"FQDNs(FQDN1,FQDN2,...)";"Description";"Asset Value";"Operating System";"Latitude";"Longitude";"Asset ID";"External Asset";"Device Types(Type1,Type2,...)"*

Header: *"IPs";"Hostname";"FQDNs";"Description";"Asset Value";"Operating System";"Latitude";"Longitude";"Asset ID";"External Asset";"Device Type"*

Example: *"192.168.10.3";"Host-1";"www.example-1.es,www.example-2.es";"Short description";"2";"Windows";"23.78";"121.45";"379D45C0BBF22B4458BD2F8EE09ECCC2";0;"Server:Mail Server"*

Version 3.x.x:

Format: *"IP";"Hostname";"FQDNs(FQDN1,FQDN2,...)";"Description";"Asset Value";"Sensors(Sensor1,Sensor2,...)";"Operating System";"Latitude";"Longitude"*

Header: *"IP";"Hostname";"FQDNs";"Description";"Asset Value";"Sensors";"Operating System";"Latitude";"Longitude"*

Example: *"192.168.10.3";"Host-1";"www.example-1.es,www.example-2.es";"Short description";"2";"192.168.10.2,192.168.10.3";"Windows";"23.78";"121.45"*

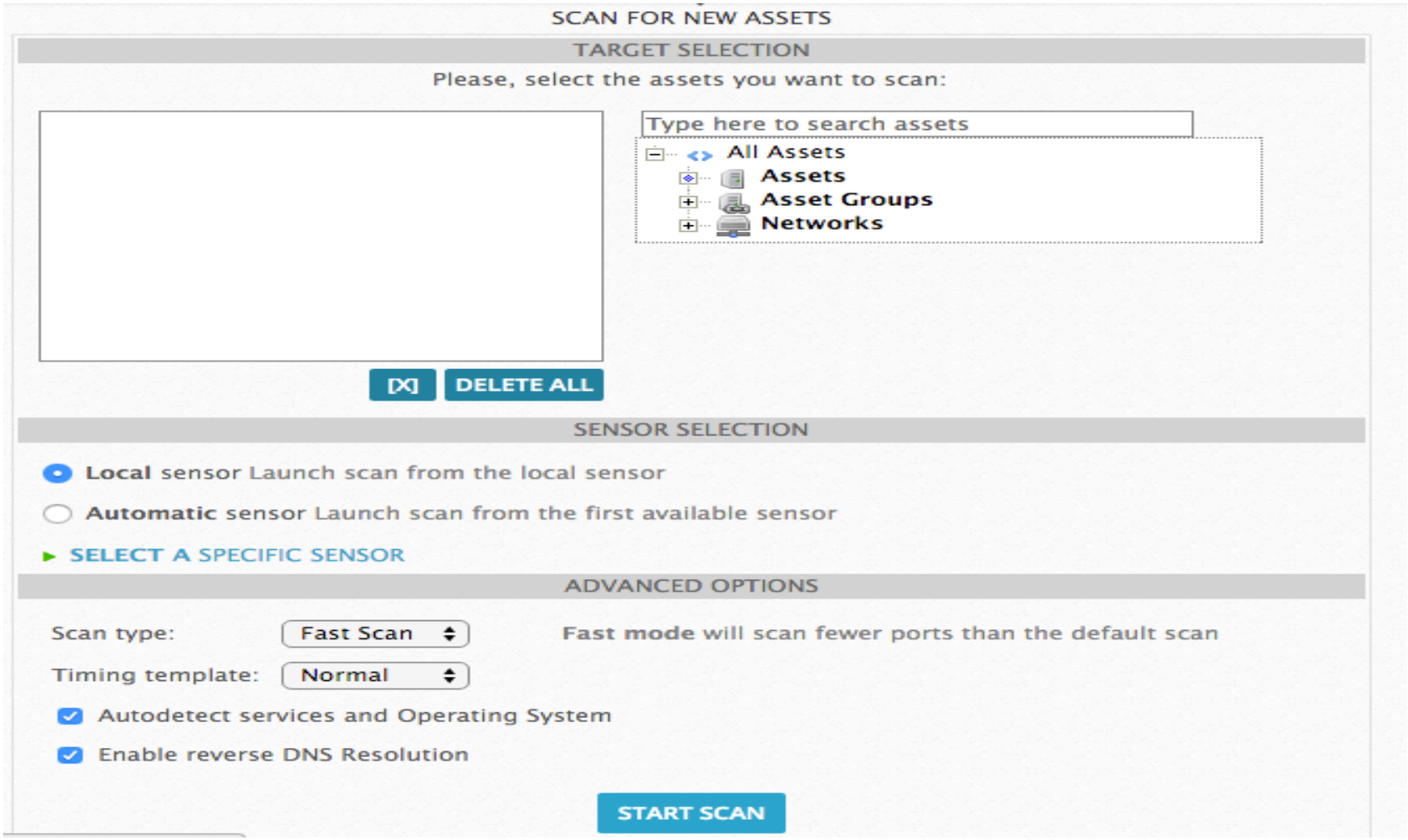
Notes:

- IP address and sensor fields cannot be empty
- Hostname syntax defined by RFC 1123
- FQDN syntax defined by RFC 1035, RFC 1123 and RFC 2181
- Valid Operating System values:
  Windows, Linux, FreeBSD, NetBSD, OpenBSD, MacOS, Solaris, Cisco, AIX,HP-UX, Tru64, IRIX, BSD/OS, SunOS, Plan9 or IPhone

发现资产


IMPORT ASSETS FROM SIEM EVENTS
Searching assets from network GZ-QXG
77%
CANCEL
IMPORT

发现资产


SCAN FOR NEW ASSETS
TARGET SELECTION
Please, select the assets you want to scan:
Type here to search assets
All Assets
Assets
Asset Groups
Networks
[X]
DELETE ALL
SENSOR SELECTION
Local sensor Launch scan from the local sensor
Automatic sensor Launch scan from the first available sensor
SELECT A SPECIFIC SENSOR
ADVANCED OPTIONS
Scan type:
Fast Scan
Fast mode will scan fewer ports than the default scan
Timing template:
Normal
Autodetect services and Operating System
Enable reverse DNS Resolution
START SCAN

发现资产

1,388
资产

清除所有

20 ASSETS

ACTIONS

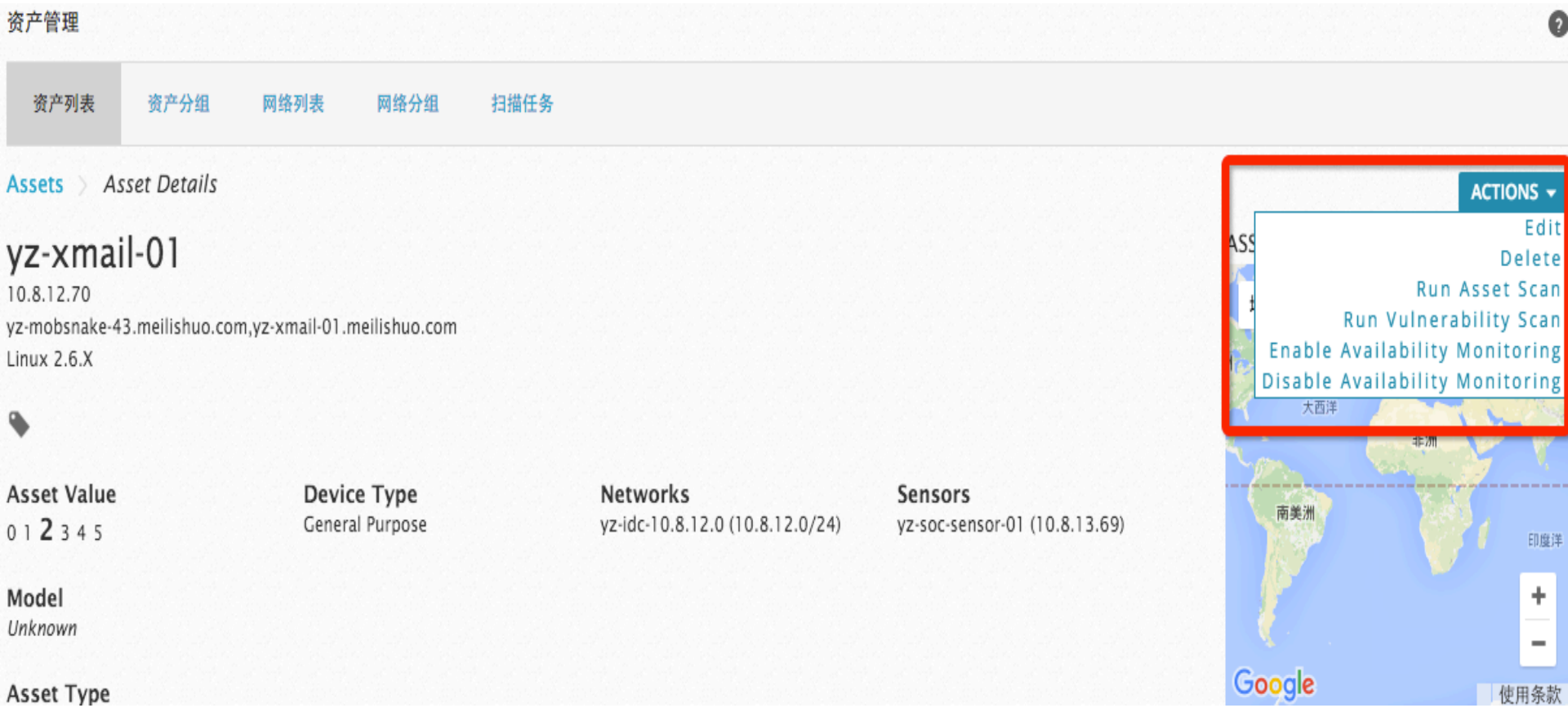
HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
yz-xmail-01	10.8.12.70	General Purpose	Linux 2.6.X	2	Yes	Not Deployed
yz-wwwop-01	10.8.12.62	General Purpose	Linux 2.6.X	2	Yes	Not Deployed
yz-wwwhb-09	10.8.12.44	General Purpose	Linux 2.6.X	2	Yes	Not Deployed
yz-wwwhb-08	10.8.9.55	General Purpose	Linux 2.6.X	2	Yes	Not Deployed
yz-wwwhb-07	10.8.9.54	General Purpose	Linux 2.6.X	2	Yes	Not Deployed
yz-wwwhb-06	10.8.9.53	General Purpose	Linux 2.6.X	2	Yes	Not Deployed

发现资产

自动发现资产

NAME	SENSOR	TARGETS	FREQUENCY	ENABLED
nmap-00	yz-soc-server-01	10.8.0.0/24	Hourly	Yes
nmap-01	yz-soc-server-01	10.8.1.0/24	Hourly	Yes
nmap-02	yz-soc-server-01	10.8.2.0/24	Hourly	Yes
nmap-03	yz-soc-server-01	10.8.3.0/24	Hourly	Yes
nmap-04	yz-soc-server-01	10.8.4.0/24	Hourly	Yes
nmap-05	yz-soc-server-01	10.8.5.0/24	Hourly	Yes
nmap-06	yz-soc-server-01	10.8.6.0/24	Hourly	Yes
nmap-07	yz-soc-server-01	10.8.7.0/24	Hourly	Yes

资产管理


资产管理
资产列表
资产分组
网络列表
网络分组
扫描任务
Assets
Asset Details
yz-xmail-01
10.8.12.70
yz-mobsnake-43.meilishuo.com,yz-xmail-01.meilishuo.com
Linux 2.6.X
Asset Value
0 1 2 3 4 5
Device Type
General Purpose
Networks
yz-idc-10.8.12.0 (10.8.12.0/24)
Sensors
yz-soc-sensor-01 (10.8.13.69)
Model
Unknown
Asset Type
ACTIONS
Edit
Delete
Run Asset Scan
Run Vulnerability Scan
Enable Availability Monitoring
Disable Availability Monitoring
大西洋
南美洲
印度洋
Google
使用条款

资产管理

Description
Unknown

VULNERABILITIES | ALARMS | EVENTS | SOFTWARE | SERVICES | PLUGINS | PROPERTIES | NETFLOW | GROUPS

EDIT SERVICES

10 SERVICES

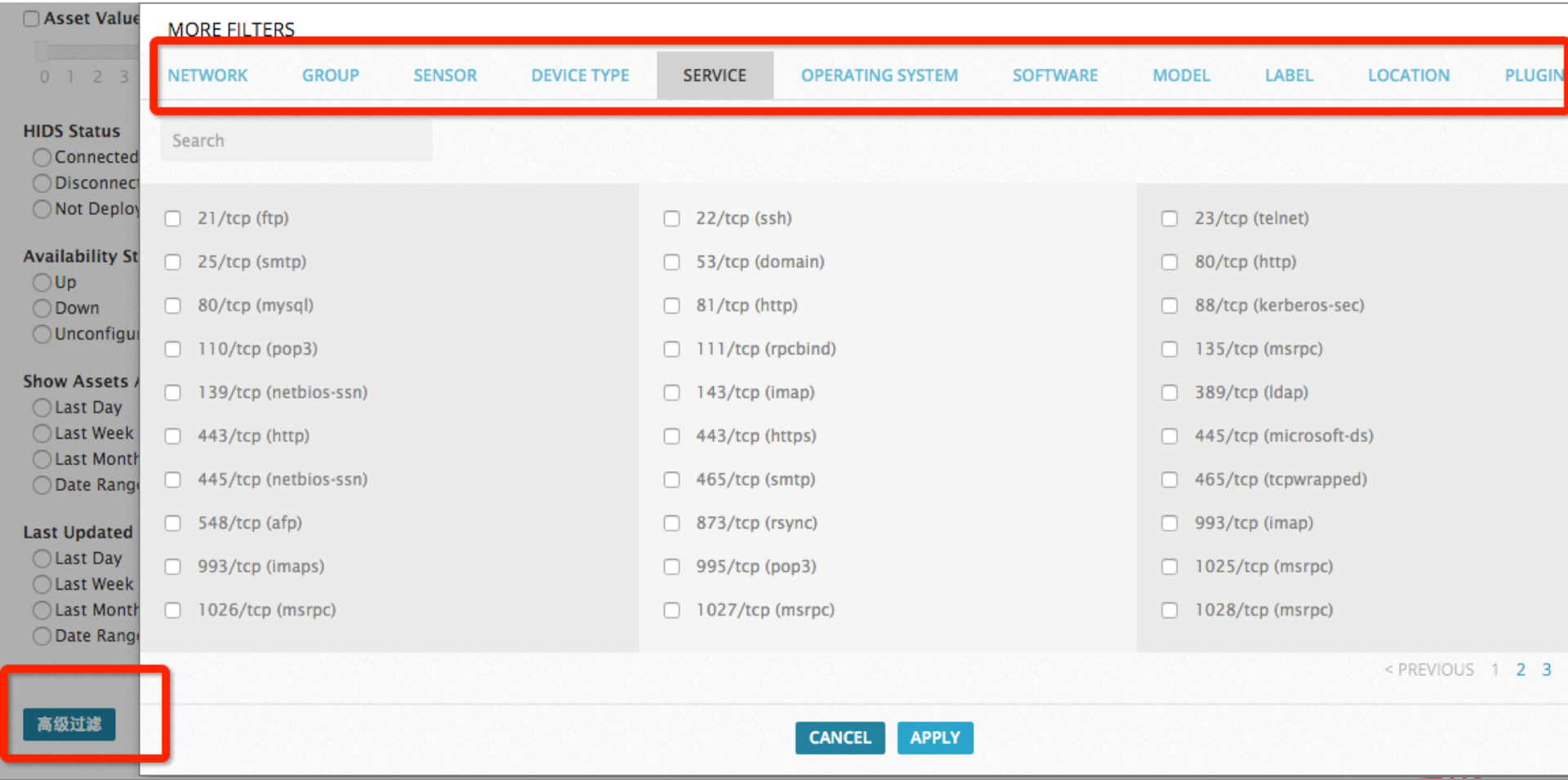
IP ADDRESS	PORT	PROTOCOL	NAME	STATUS	MONITORING
yz-xmail-01 (10.8.12.70)	22	tcp	ssh	-	No
yz-xmail-01 (10.8.12.70)	80	tcp	http	-	No
yz-xmail-01 (10.8.12.70)	9999	tcp	tcpwrapped	-	No

SHOWING 1 TO 3 OF 3 SERVICES

< PREVIOUS 1 NEXT >

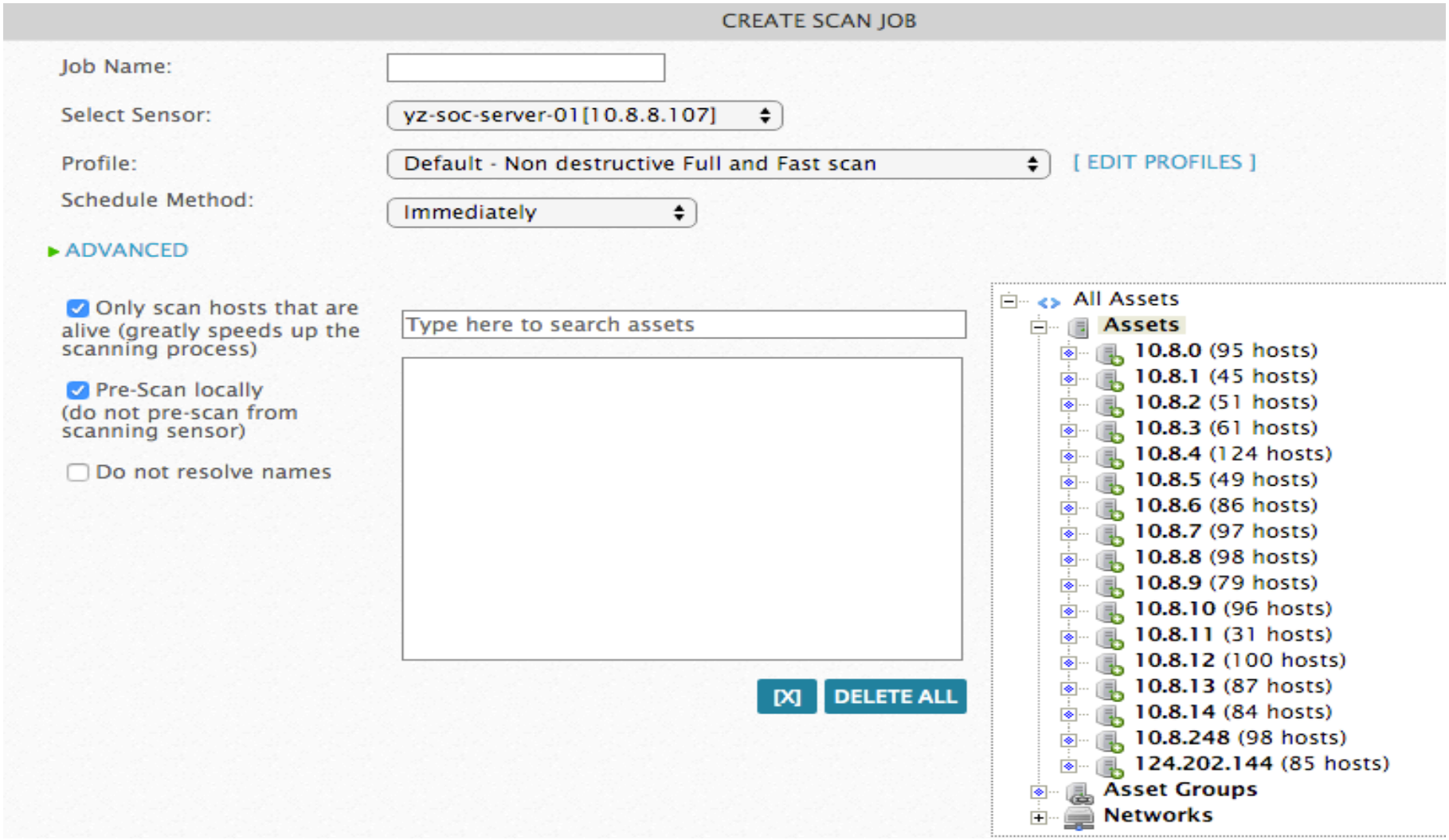
资产管理

快速查找资产


Asset Value
0 1 2 3
HIDS Status
Connected
Disconnec
Not Deplo
Availability St
Up
Down
Unconfigu
Show Assets
Last Day
Last Week
Last Month
Date Rang
Last Updated
Last Day
Last Week
Last Month
Date Rang
高级过滤
MORE FILTERS
NETWORK
GROUP
SENSOR
DEVICE TYPE
SERVICE
OPERATING SYSTEM
SOFTWARE
MODEL
LABEL
LOCATION
PLUGIN
Search
21/tcp (ftp)
25/tcp (smtp)
80/tcp (mysql)
110/tcp (pop3)
139/tcp (netbios-ssn)
443/tcp (http)
445/tcp (netbios-ssn)
548/tcp (afp)
993/tcp (imaps)
1026/tcp (msrpc)
22/tcp (ssh)
53/tcp (domain)
81/tcp (http)
111/tcp (rpcbind)
143/tcp (imap)
443/tcp (https)
465/tcp (smtp)
873/tcp (rsync)
995/tcp (pop3)
1027/tcp (msrpc)
23/tcp (telnet)
80/tcp (http)
88/tcp (kerberos-sec)
135/tcp (msrpc)
389/tcp (ldap)
445/tcp (microsoft-ds)
465/tcp (tcpwrapped)
993/tcp (imap)
1025/tcp (msrpc)
1028/tcp (msrpc)
< PREVIOUS 1 2 3
CANCEL
APPLY

漏洞扫描

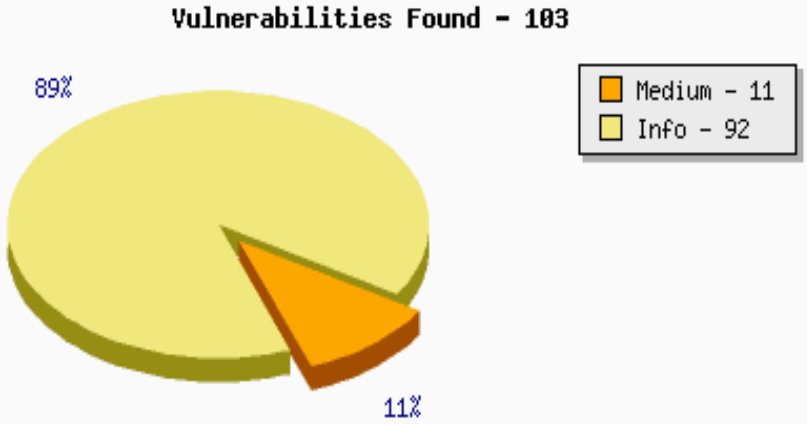
添加扫描任务


CREATE SCAN JOB
Job Name:
Select Sensor:
yz-soc-server-01[10.8.8.107]
Profile:
Default - Non destructive Full and Fast scan
[EDIT PROFILES]
Schedule Method:
Immediately
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
[X]
DELETE ALL
All Assets
Assets
10.8.0 (95 hosts)
10.8.1 (45 hosts)
10.8.2 (51 hosts)
10.8.3 (61 hosts)
10.8.4 (124 hosts)
10.8.5 (49 hosts)
10.8.6 (86 hosts)
10.8.7 (97 hosts)
10.8.8 (98 hosts)
10.8.9 (79 hosts)
10.8.10 (96 hosts)
10.8.11 (31 hosts)
10.8.12 (100 hosts)
10.8.13 (87 hosts)
10.8.14 (84 hosts)
10.8.248 (98 hosts)
124.202.144 (85 hosts)
Asset Groups
Networks

运行扫描任务

NAME	SCHEDULE TYPE	TIME	NEXT SCAN	STATUS	ACTION
yz-idc-10-8-4	Monthly	03:00:00	2016-02-04 03:00:00	Enabled	
yz-idc-10-8-14	Monthly	03:00:00	2016-01-14 03:00:00	Enabled	
yz-idc-10-8-13	Monthly	03:00:00	2016-02-13 03:00:00	Enabled	
yz-idc-10-8-12	Monthly	03:00:00	2016-02-12 03:00:00	Enabled	
yz-idc-10-8-11	Monthly	03:00:00	2016-02-11 03:00:00	Enabled	
yz-idc-10-8-10	Monthly	03:00:00	2016-02-10 03:00:00	Enabled	
yz-idc-10-8-9	Monthly	03:00:00	2016-02-09 03:00:00	Enabled	
yz-idc-10-8-8	Monthly	03:00:00	2016-02-08 03:00:00	Enabled	
yz-idc-10-8-7	Monthly	03:00:00	2016-02-07 03:00:00	Enabled	

查看扫描结果



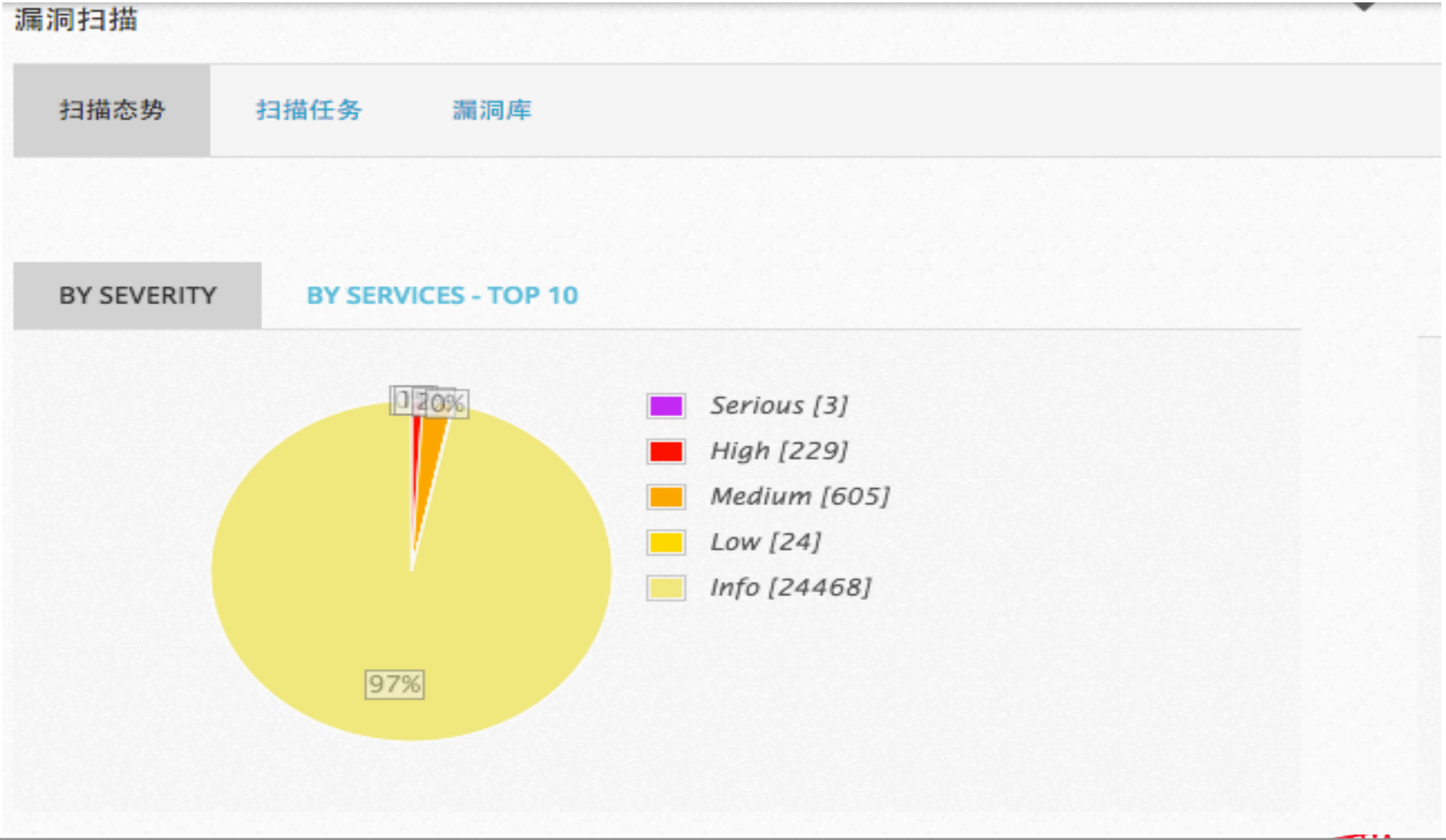
SUMMARY OF SCANNED HOSTS

HOST	HOSTNAME	Serious	High	Medium	Low	Info
10.8.1.45	yz-it-mail-01	-	-	11	-	92

View false positives

- True result - False positive result - Additional information is available

查看扫描结果


漏洞扫描
扫描态势
扫描任务
漏洞库
BY SEVERITY
BY SERVICES - TOP 10
1%
2%
97%
Serious [3]
High [229]
Medium [605]
Low [24]
Info [24468]

入侵检测

IDS(入侵检测系统)

基于主机的IDS(OSSEC)

基于网络的IDS(Suricate)

基于主机的IDS(OSSEC)

OSSEC是一个开源的基于主机的入侵检测系统，可运行在Windows/Linux/Mac等多个平台

主要功能：日志分析、完整性检查、rootkit检测、基于时间的警报和主动响应

官网：http://ossec.github.io/

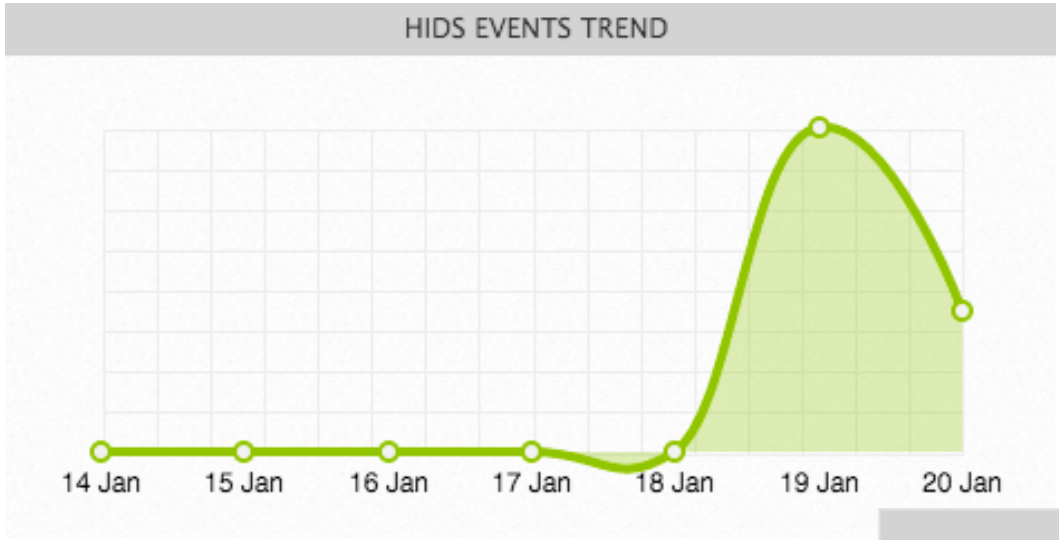
基于主机的IDS(OSSEC)

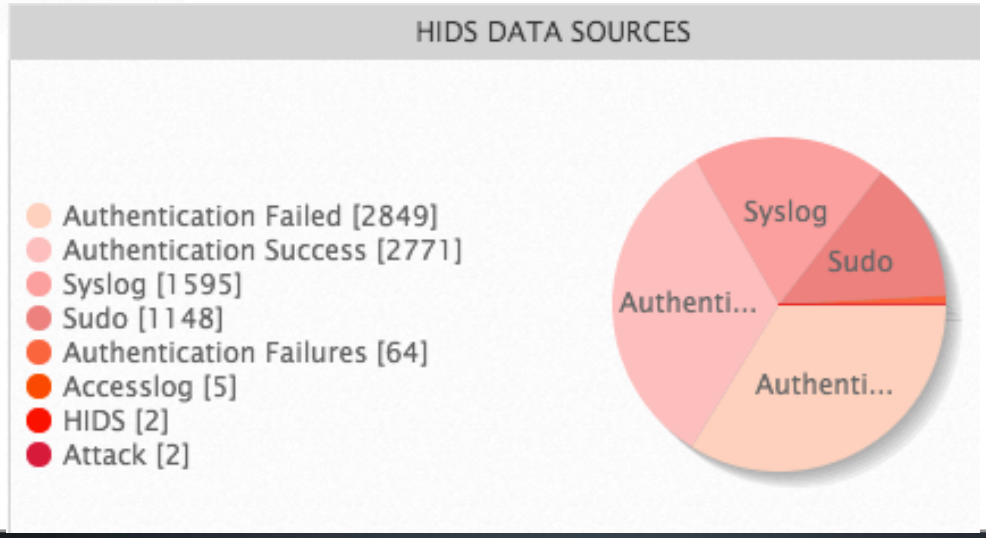
OSSIM中OSSEC配置文件路径：/var/ossec/etc/ossec.conf

日志保存路径：/var/ossec/logs/

```
yz-soc-server-01:/usr/share/ossim# ls /var/ossec/logs/
alerts    firewall   ossec.log.1     ossec.log.3.gz  ossec.log.5.gz  ossec.log.7.gz
archives  ossec.log  ossec.log.2.gz  ossec.log.4.gz  ossec.log.6.gz
```

基于主机的IDS(OSSEC)





基于主机的IDS(OSSEC)

利用OSSEC对系统日志进行安全分析过程：

基于主机的IDS(OSSEC)

编辑客户端机器的rsyslog配置文件，将日志发送至rsyslog服务器

配置文件路径：/etc/rsyslog.conf

基于主机的IDS(OSSEC)

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog
```

```
#$ActionResumeRetryCount -1    # infinite retries
# remote host is: name/ip:port, e.g. 192.168.0.1
authpriv.* @10.8.8.107:514
# ### end of the forwarding rule ###
```

基于主机的IDS(OSSEC)

编辑服务器端ossec.conf，配置syslog相关选项

```
<!-- 配置syslog -->
<syslog_output>
  <server>10.8.8.107</server>
  <port>514</port>
</syslog_output>
<!--<remote>
  <connection>secure</connection>
</remote>-->
<remote>
  <connection>syslog</connection>
  <allowed-ips>10.8.0.0/16</allowed-ips>
</remote>
```

```
udp        0      0 0.0.0.0:514             0.0.0.0:*
```

基于主机的IDS(OSSEC)

```
[xiao[redacted]-01] $ ssh secsky@yz-sec-01
secsky@yz-sec-01's password:
Permission denied, please try again.
```

```
Jan 20 14:39:12 yz-sec-01 sshd[8930]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.12.85  user=
secsky
Jan 20 14:39:14 yz-sec-01 sshd[8930]: Failed password for secsky from 172.16.12.85 port 46834 ssh2
```

```
AV - Alert - "1453271949" --> RID: "5503"; RL: "5"; RG: "pam,syslog,authentication_failed,"; RC: "User login failed."; USER: "None"; SRCIP: "172.
16.12.85"; HOSTNAME: "yz-sec-01"; LOCATION: "10.8.4.36"; EVENT: "[INIT]Jan 20 14:39:12 yz-sec-01 sshd[8930]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.12.85  user=secsky[END]";
AV - Alert - "1453271951" --> RID: "5716"; RL: "5"; RG: "syslog,sshd,authentication_failed,"; RC: "SSHD authentication failed."; USER: "None"; SR
CIP: "172.16.12.85"; HOSTNAME: "yz-sec-01"; LOCATION: "10.8.4.36"; EVENT: "[INIT]Jan 20 14:39:14 yz-sec-01 sshd[8930]: Failed password for secsky
 from 172.16.12.85 port 46834 ssh2[END]";
```

SIGNATURE	DATE GMT+8:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK
AlienVault HIDS: SSHD authentication failed.	2016-01-20 14:39:11	yz-soc-server-01	N/A	172.16.12.85:46834	0.0.0.0	2->0	0
AlienVault HIDS: User login failed.	2016-01-20 14:39:09	yz-soc-server-01	N/A	172.16.12.85	0.0.0.0	2->0	0

USERNAME	USERDATA1	USERDATA2	USERDATA3	USERDATA4
secsky	10.8.4.36	172.16.12.85	SSHD authentication failed.	syslog,sshd,authentication_failed,

RAW LOG

```
AV - Alert - "1453271951" --> RID: "5716"; RL: "5"; RG: "syslog,sshd,authentication_failed,"; RC: "SSHD authentication failed.";
USER: "None";
SRCIP: "172.16.12.85"; HOSTNAME: "yz-sec-01"; LOCATION: "10.8.4.36"; EVENT: "[INIT]Jan 20 14:39:14 yz-sec-01 sshd[8930]: Failed
password for
secsky from 172.16.12.85 port 46834 ssh2[END]";
```

基于网络的IDS(Suricate)

Suricate是一个开源的基于网络的入侵检测系统（NIDS）

特点：多线程，高性能，支持多个平台

官网：http://suricata-ids.org/

基于网络的IDS(Suricate)

配置文件路径：/etc/suricata

```
yz-soc-sensor-01:/etc/suricata# ll
total 128
-rw-r--r-- 1 root root   169 Dec 25 18:06 afpacket_f.yaml
-rw-r--r-- 1 root root  1763 Dec 21 10:33 alienvault.conf
-rw-r--r-- 1 root root  2638 Dec 21 10:33 classification.config
-rw-r--r-- 1 root root  1378 Sep 17 23:16 reference.config
-rw-r--r-- 1 root root  1167 Oct 29 11:43 rule-files.yaml
drwxr-xr-x 2 root root  4096 Nov 16 17:06 rules
-rw-r--r-- 1 root root 49739 Aug 19 21:50 suricata-debian.yaml
-rw-r--r-- 1 root root 47557 Nov 18 17:44 suricata.yaml
```

基于网络的IDS(Suricate)

规则配置文件路径：/etc/suricata/rules

```
yz-soc-sensor-01:/etc/suricata/rules# ls
BSD-License.txt                 emerging-mobile_malware.rules       emerging_pro-current_events.rules   emerging_pro-smtp.rules
LICENSE                         emerging-netbios.rules              emerging_pro-decoder-events.rules   emerging_pro-snmp.rules
alienvault.rules                emerging-p2p.rules                  emerging_pro-deleted.rules          emerging_pro-sql.rules
botcc.portgrouped.rules         emerging-policy.rules               emerging_pro-dns.rules              emerging_pro-stream-events.rules
botcc.rules                     emerging-pop3.rules                 emerging_pro-dos.rules              emerging_pro-telnet.rules
ciarmy.rules                    emerging-rbn-malvertisers.rules     emerging_pro-drop.rules             emerging_pro-tftp.rules
compromised.rules               emerging-rbn.rules                  emerging_pro-dshield.rules          emerging_pro-tls-events.rules
decoder-events.rules            emerging-rpc.rules                  emerging_pro-exploit.rules          emerging_pro-tor.rules
drop.rules                      emerging-scada.rules                emerging_pro-files.rules            emerging_pro-trojan.rules
dshield.rules                   emerging-scan.rules                 emerging_pro-ftp.rules              emerging_pro-user_agents.rules
emerging-activex.rules          emerging-shellcode.rules            emerging_pro-games.rules            emerging_pro-voip.rules
emerging-attack_response.rules  emerging-smtp.rules                 emerging_pro-http-events.rules      emerging_pro-web_client.rules
emerging-botcc.rules            emerging-snmp.rules                 emerging_pro-icmp.rules             emerging_pro-web_server.rules
emerging-chat.rules             emerging-sql.rules                  emerging_pro-icmp_info.rules        emerging_pro-web_specific_apps.rules
emerging-ciarmy.rules           emerging-telnet.rules               emerging_pro-imap.rules             emerging_pro-worm.rules
emerging-compromised.rules      emerging-tftp.rules                 emerging_pro-inappropriate.rules    files.rules
emerging-current_events.rules   emerging-tor.rules                  emerging_pro-info.rules             gpl-2.0.txt
emerging-deleted.rules          emerging-trojan.rules               emerging_pro-malware.rules          http-events.rules
emerging-dns.rules              emerging-user_agents.rules          emerging_pro-misc.rules             local.rules
emerging-dos.rules              emerging-virus.rules                emerging_pro-mobile_malware.rules   rbn-malvertisers.rules
emerging-drop.rules             emerging-voip.rules                 emerging_pro-netbios.rules          rbn.rules
emerging-dshield.rules          emerging-web_client.rules           emerging_pro-p2p.rules              smtp-events.rules
emerging-exploit.rules          emerging-web_server.rules           emerging_pro-policy.rules           stream-events.rules
emerging-ftp.rules              emerging-web_specific_apps.rules    emerging_pro-pop3.rules             suricata-decoder-events.rules
emerging-games.rules            emerging-worm.rules                 emerging_pro-rbn-malvertisers.rules suricata-files.rules
emerging-icmp.rules             emerging_pro-activex.rules          emerging_pro-rbn.rules              suricata-http-events.rules
emerging-icmp_info.rules        emerging_pro-attack_response.rules  emerging_pro-rpc.rules              suricata-smtp-events.rules
emerging-imap.rules             emerging_pro-botcc.portgrouped.rules emerging_pro-scada.rules           suricata-stream-events.rules
emerging-inappropriate.rules    emerging_pro-botcc.rules            emerging_pro-scada_special.rules    tls-events.rules
emerging-info.rules             emerging_pro-chat.rules             emerging_pro-scan.rules             tor.rules
emerging-malware.rules          emerging_pro-ciarmy.rules           emerging_pro-shellcode.rules
emerging-misc.rules             emerging_pro-compromised.rules      emerging_pro-smtp-events.rules
```

基于网络的IDS(Suricate)

日志文件路径：/var/log/suricata

```
yz-soc-sensor-01:/var/log/suricata# ls
eve.json            unified2.alert.1446090386  unified2.alert.1447967793
eve.json.1.gz       unified2.alert.1446098946  unified2.alert.1448005122
eve.json.2.gz       unified2.alert.1446099709  unified2.alert.1448655999
eve.json.3.gz       unified2.alert.1446100010  unified2.alert.1448911882
eve.json.4.gz       unified2.alert.1446100018  unified2.alert.1449085963
eve.json.5.gz       unified2.alert.1447776366  unified2.alert.1449171766
stats.log           unified2.alert.1447839853  unified2.alert.1449181382
suricata-start.log  unified2.alert.1447840060  unified2.alert.1449257627
suricata.log        unified2.alert.1447964072  unified2.alert.1449343518
```

基于网络的IDS(Suricate)

SIGNATURE	DATE GMT+8:00	SENSOR	OTX	SOURCE	DESTINATION
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:27:16	yz-soc-sensor-01	N/A	76.127.119.148:30	115.[redacted]2.202.1:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:27:16	yz-soc-sensor-01	N/A	76.127.119.148:30	1[redacted]2.242.1:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:27:16	yz-soc-sensor-01	N/A	76.127.119.148:30	2[redacted]0.74:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:26:16	yz-soc-sensor-01	N/A	76.127.119.148:30	115[redacted]2.202.1:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:26:16	yz-soc-sensor-01	N/A	76.127.119.148:30	115[redacted].242.1:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:26:16	yz-soc-sensor-01	N/A	76.127.119.148:30	210[redacted]74:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:20:04	yz-soc-sensor-01	N/A	76.127.119.148:80	115[redacted]202.1:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:20:04	yz-soc-sensor-01	N/A	76.127.119.148:80	115[redacted].242.1:123
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"	2016-01-20 15:20:04	yz-soc-sensor-01	N/A	76.127.119.148:80	210.74[redacted]0.74:123

基于网络的IDS(Suricate)

Security Events > *AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"*

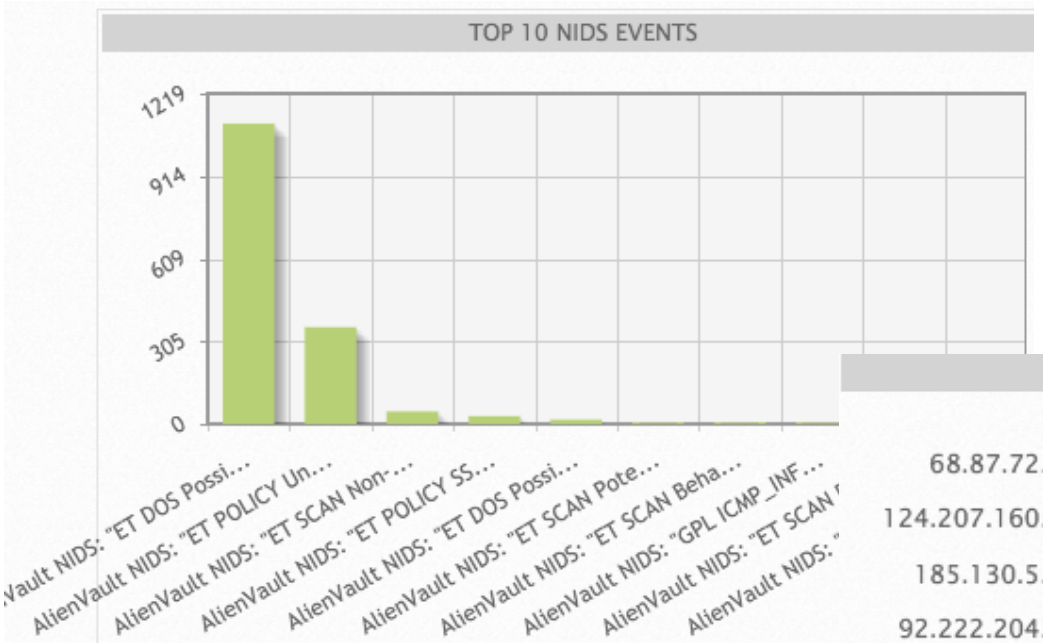
AlienVault NIDS: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"

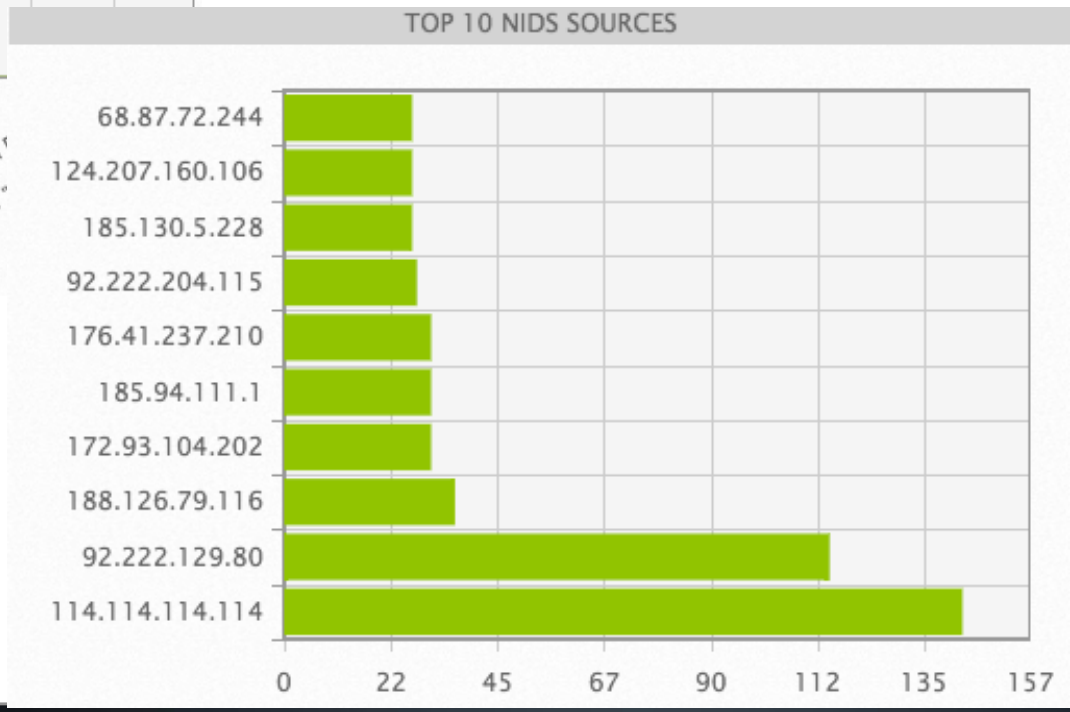
DATE	2016-01-20 15:27:16 GMT+8:00	CATEGORY	Exploit
ALIENVAULT SENSOR	yz-soc-sensor-01 [10.8.13.69]	SUB-CATEGORY	Denial Of Service
DEVICE IP	10.8.13.69 [eth1]	DATA SOURCE NAME	AlienVault NIDS
EVENT TYPE ID	2017919	DATA SOURCE ID	1001
UNIQUE EVENT ID#	bf4711e5-ad66-000c-29d5-abe23b7755a0	PRODUCT TYPE	Intrusion Detection
			URL

Rule Detection

File: emerging-dos.rules
Rule: alert udp any any -> any 123
msg: "ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03"
content: "|00 03 2A|"
offset: 1
depth: 3
byte_test: 1,!&,128,0
byte_test: 1,&,4,0
byte_test: 1,&,2,0
byte_test: 1,&,1,0
threshold: type both,track by_dst,count 2,seconds 60
reference: url,www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks
classtype: attempted-dos
sid: 2017919
rev: 2

基于网络的IDS(Suricate)





安全策略/规则配置

- 过滤无效告警日志
- SSH异常登录自动邮件告警

过滤无效告警日志

无效告警日志：

SIGNATURE	DATE GMT+8:00	SENSOR	OTX	SOURCE	DESTINATION
AlienVault HIDS: Login session closed [avapi].	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01	yz-soc-sensor-01
AlienVault HIDS: Login session closed.	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01	yz-soc-sensor-01
AlienVault HIDS: Login session opened.	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01	yz-soc-sensor-01
AlienVault HIDS: Successful sudo to ROOT executed [avapi]	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01	yz-soc-sensor-01
AlienVault HIDS: Login session opened [avapi].	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01	yz-soc-sensor-01
AlienVault HIDS: SSHD authentication success [avapi].	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01:60173	yz-soc-sensor-01
AlienVault HIDS: Login session closed [avapi].	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01	yz-soc-sensor-01
AlienVault HIDS: Login session opened [avapi].	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01	yz-soc-sensor-01
AlienVault HIDS: SSHD authentication success [avapi].	2016-01-19 11:06:26	yz-soc-sensor-01	N/A	yz-soc-sensor-01:60170	yz-soc-sensor-01

过滤无效告警日志

无效告警日志：

☐	sudo: Command executed [avapi]	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: Login session closed [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: Login session closed.	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: Login session opened.	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: Successful sudo to ROOT executed [avapi]	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: Login session opened [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: SSHD authentication success [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01:47025	yz-soc-server-01
☐	AlienVault HIDS: Login session closed [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: Login session opened [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: SSHD authentication success [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01:47024	yz-soc-server-01
☐	AlienVault HIDS: Login session closed [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01
☐	AlienVault HIDS: Login session opened [avapi].	2016-01-19 11:10:46	yz-soc-server-01	N/A	yz-soc-server-01	yz-soc-server-01

过滤无效告警日志

无效告警日志：

EVENT NAME	RISK	GENERATOR	SENSOR	OTX	SOURCE IP	DEST IP
Syslog: syslog entry	0	syslog	yz-soc-sensor-01	N/A	yz-soc-sensor-01	0.0.0.0
SSHd: Received disconnect	0	ssh	yz-soc-sensor-01	N/A	yz-soc-server-01	yz-soc-sensor-01:22
SSHd: Login sucessful, Accepted publickey [USERNAME]	0	ssh	yz-soc-sensor-01	N/A	yz-soc-server-01:41669	yz-soc-sensor-01:22
SSHd: Received disconnect	0	ssh	yz-soc-sensor-01	N/A	yz-soc-server-01	yz-soc-sensor-01:22
SSHd: Login sucessful, Accepted publickey [USERNAME]	0	ssh	yz-soc-sensor-01	N/A	yz-soc-server-01:41668	yz-soc-sensor-01:22
SSHd: Received disconnect	0	ssh	yz-soc-sensor-01	N/A	yz-soc-server-01	yz-soc-sensor-01:22
SSHd: Login sucessful, Accepted publickey [USERNAME]	0	ssh	yz-soc-sensor-01	N/A	yz-soc-server-01:41667	yz-soc-sensor-01:22

过滤无效告警日志

策略由CONDITIONS和CONSEQUENCES两部分组成

IF:

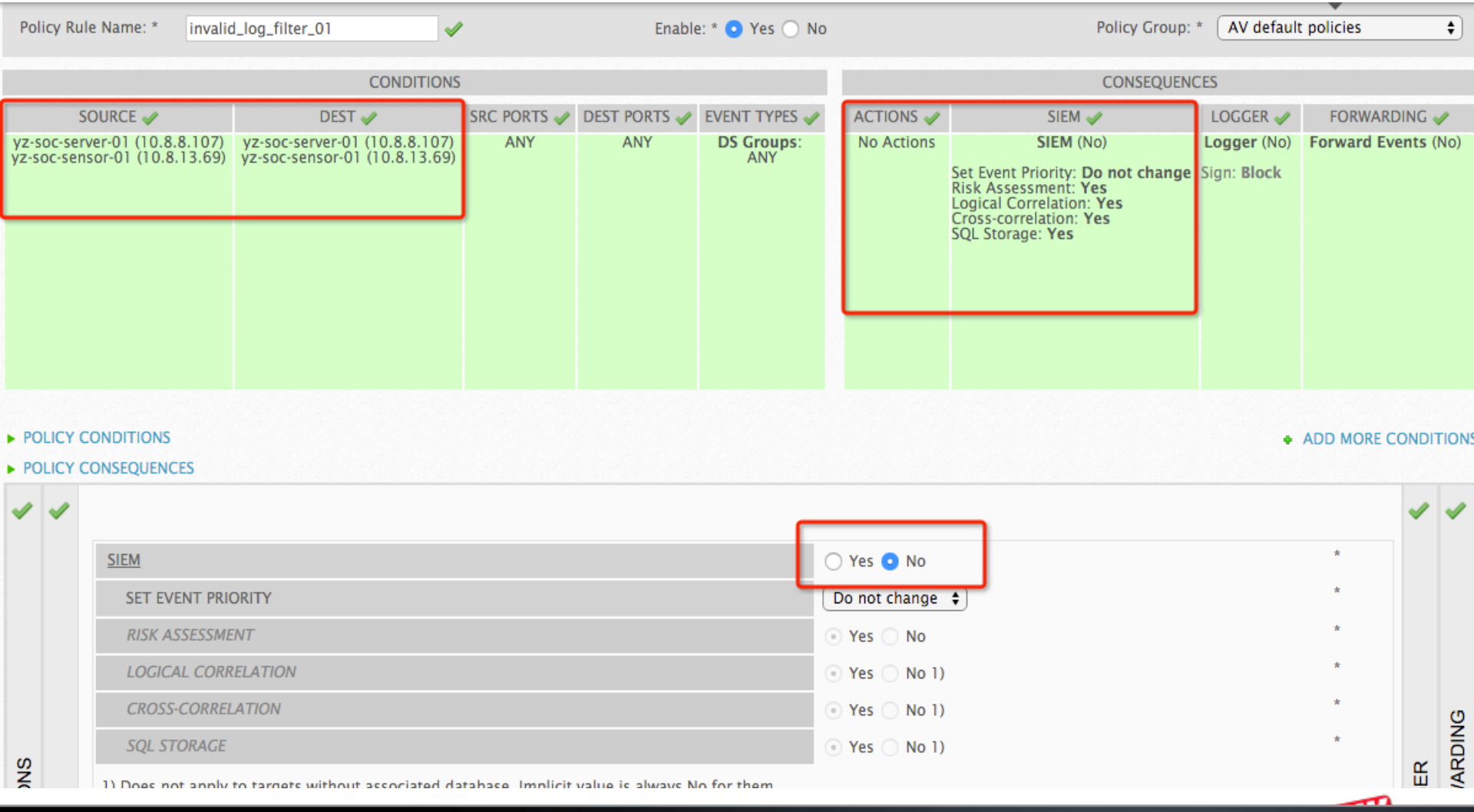
CONDITIONS

THEN:

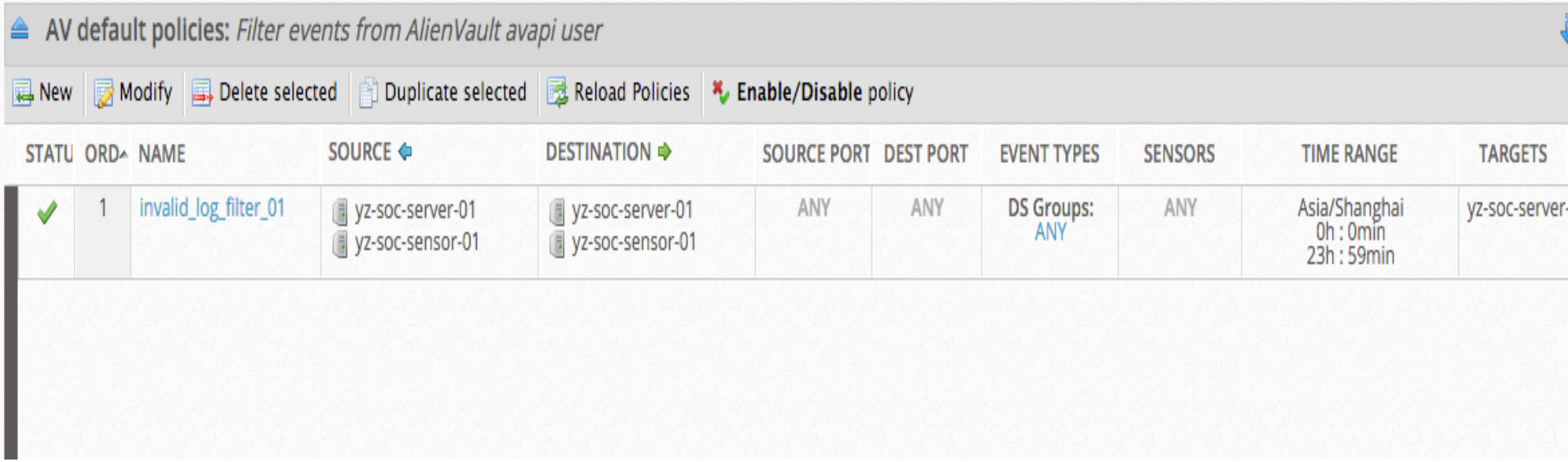
CONSEQUENCES

说明：新建或修改策略后需要reload使策略生效

过滤无效告警日志


Policy Rule Name: * invalid_log_filter_01
Enable: * Yes No
Policy Group: * AV default policies
CONDITIONS
CONSEQUENCES
SOURCE
DEST
SRC PORTS
DEST PORTS
EVENT TYPES
ACTIONS
SIEM
LOGGER
FORWARDING
yz-soc-server-01 (10.8.8.107)
yz-soc-sensor-01 (10.8.13.69)
yz-soc-server-01 (10.8.8.107)
yz-soc-sensor-01 (10.8.13.69)
ANY
ANY
DS Groups: ANY
No Actions
SIEM (No)
Set Event Priority: Do not change
Risk Assessment: Yes
Logical Correlation: Yes
Cross-correlation: Yes
SQL Storage: Yes
Logger (No)
Sign: Block
Forward Events (No)
POLICY CONDITIONS
ADD MORE CONDITIONS
POLICY CONSEQUENCES
SIEM
Yes No
SET EVENT PRIORITY
Do not change
RISK ASSESSMENT
LOGICAL CORRELATION
CROSS-CORRELATION
SQL STORAGE
Yes No
Yes No 1)
1) Does not apply to targets without associated database. Implicit value is always No for them

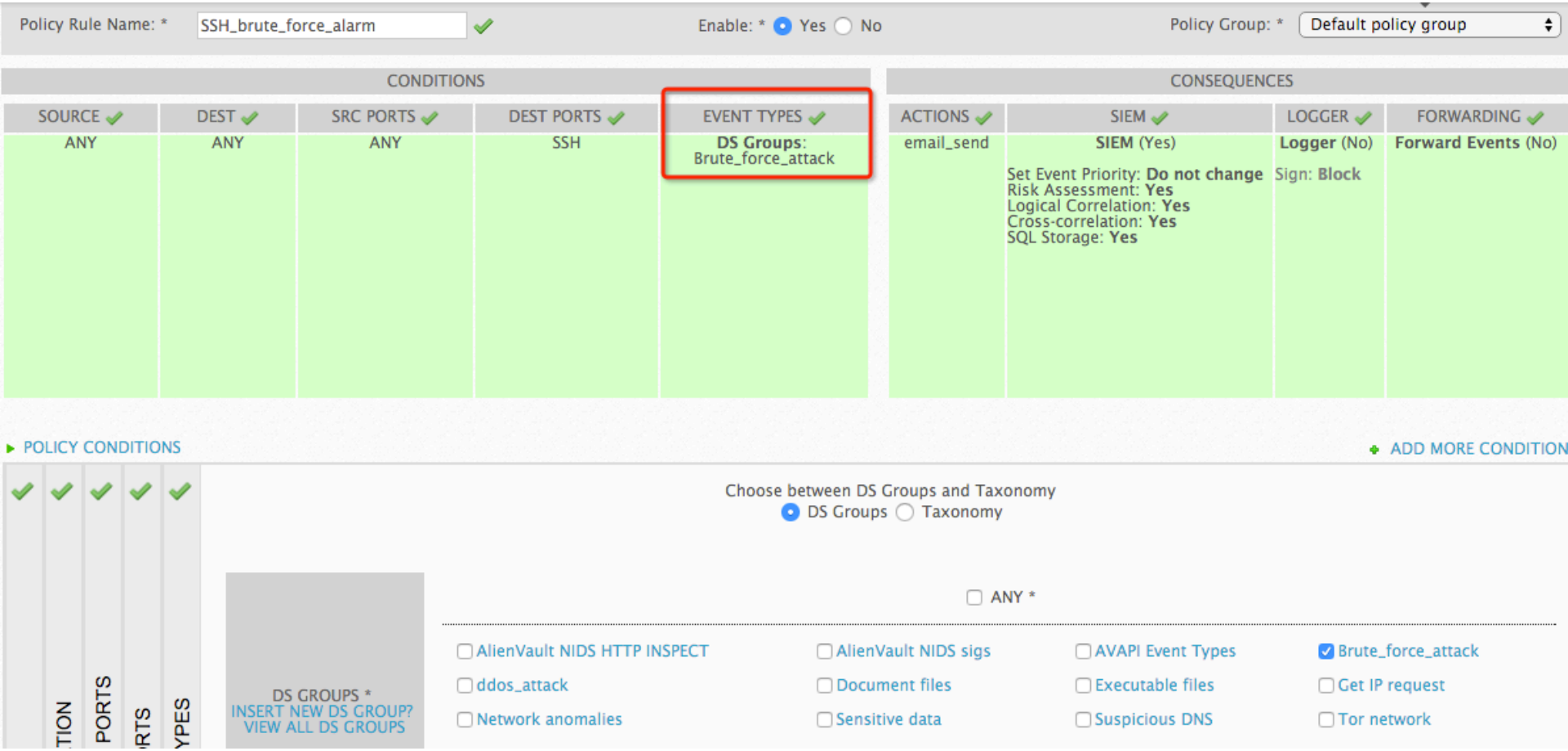
过滤无效告警日志


AV default policies: Filter events from AlienVault avapi user
New
Modify
Delete selected
Duplicate selected
Reload Policies
Enable/Disable policy
STATU
ORD
NAME
SOURCE
DESTINATION
SOURCE PORT
DEST PORT
EVENT TYPES
SENSORS
TIME RANGE
TARGETS
1
invalid_log_filter_01
yz-soc-server-01
yz-soc-sensor-01
yz-soc-server-01
yz-soc-sensor-01
ANY
ANY
DS Groups:
ANY
ANY
Asia/Shanghai
0h : 0min
23h : 59min
yz-soc-server-

SSH异常登录自动邮件告警

NAME *	email_send
DESCRIPTION *	恶意攻击行为自动邮件告警
TYPE *	Send an email message
CONDITION	Any　Only if it is an alarm　Define logical condition
FROM: *	xiaofeijin@[redacted]
TO: *	xiaofeijin@[redacted]
SUBJECT: *	恶意攻击行为自动告警---来自统一安全管理平台
MESSAGE: *	该邮件由统一安全管理平台自动发出，请勿回复!

SSH异常登录自动邮件告警



SSH异常登录自动邮件告警

Brute_force_attack

暴力破解攻击

Add events to the DS Group

ADD BY DATA SOURCE * ADD BY EVENT TYPE *

DATA SOURCE	DATA SOURCE NAME	DATA SOURCE DESCRIPTION / EVENT TYPES	
4003	ssh	SSHd: Secure Shell daemon	ssh events type selected: 2
7010	AlienVault HIDS-authentication_failed	authentication_failed	AlienVault HIDS-authentication_failed events type selected: 4

Default policy group: *Default group policy objects*

New | Modify | Delete selected | Duplicate selected | Reload Policies | **Enable/Disable** policy

STATU	ORD	NAME	SOURCE	DESTINATION	SOURCE PORT	DEST PORT	EVENT TYPES	SENSORS	TIME RANGE	TARGETS
✓	1	SSH_brute_force_alarm	ANY	ANY	ANY	SSH	DS Groups: Brute_force_atta	ANY	Asia/Shanghai 0h : 0min 23h : 59min	yz-soc-server

SSH异常登录自动邮件告警

```
root@secsky:~# medusa -h 10.8.13.69 -U users.txt -P password.txt -M ssh
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test1 (1 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test2 (2 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test3 (3 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test4 (4 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test5 (5 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test6 (6 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test7 (7 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test8 (8 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test9 (9 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky1 (1 of 21, 0 complete) Password: test10 (10 of 10 complet
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test1 (1 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test2 (2 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test3 (3 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test4 (4 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test5 (5 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test6 (6 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test7 (7 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test8 (8 of 10 complete)
ACCOUNT CHECK: [ssh] Host: 10.8.13.69 (1 of 1, 0 complete) User: secsky2 (2 of 21, 1 complete) Password: test9 (9 of 10 complete)
```

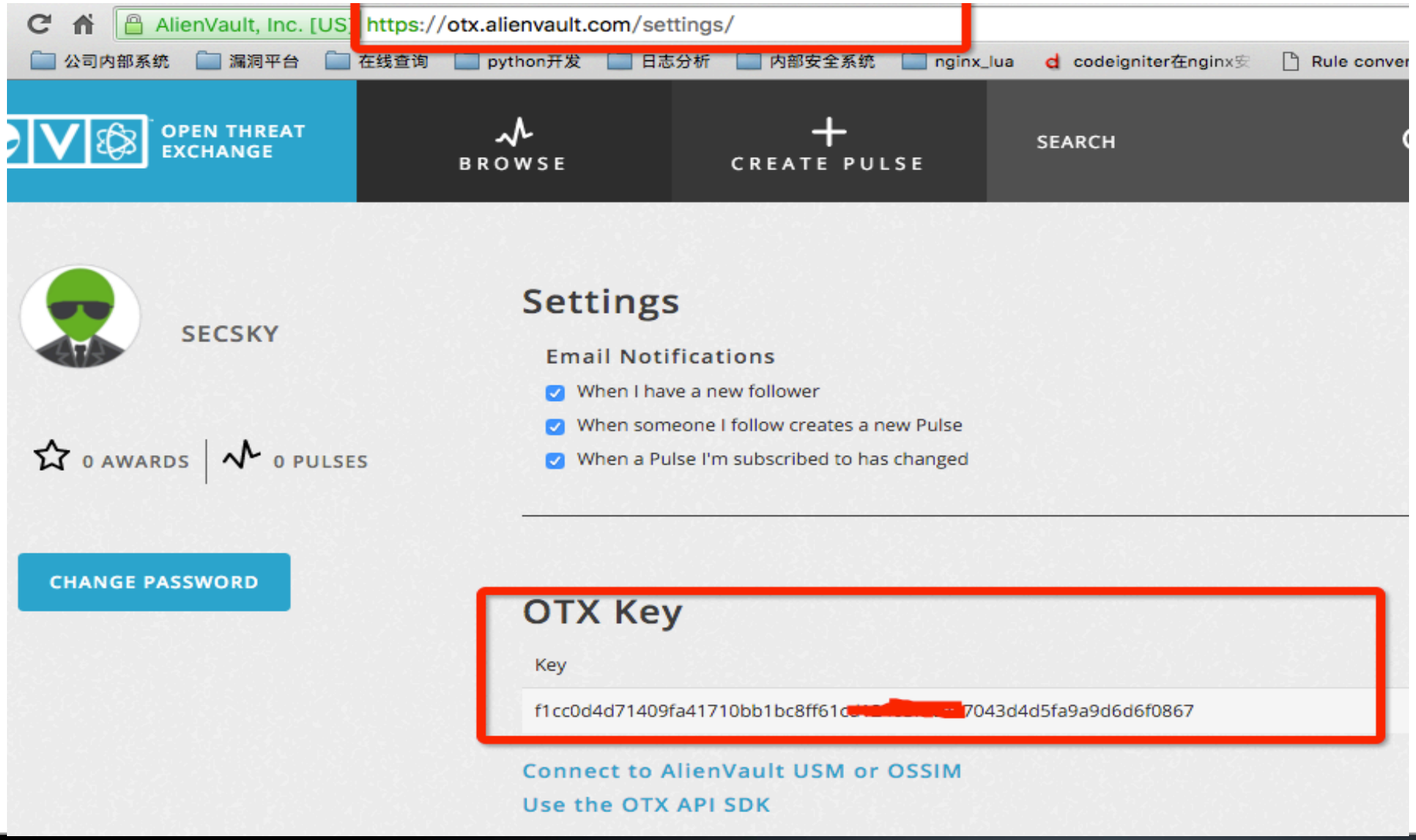
SSH异常登录自动邮件告警

该邮件由统一安全管理平台自动发出，请勿回复!

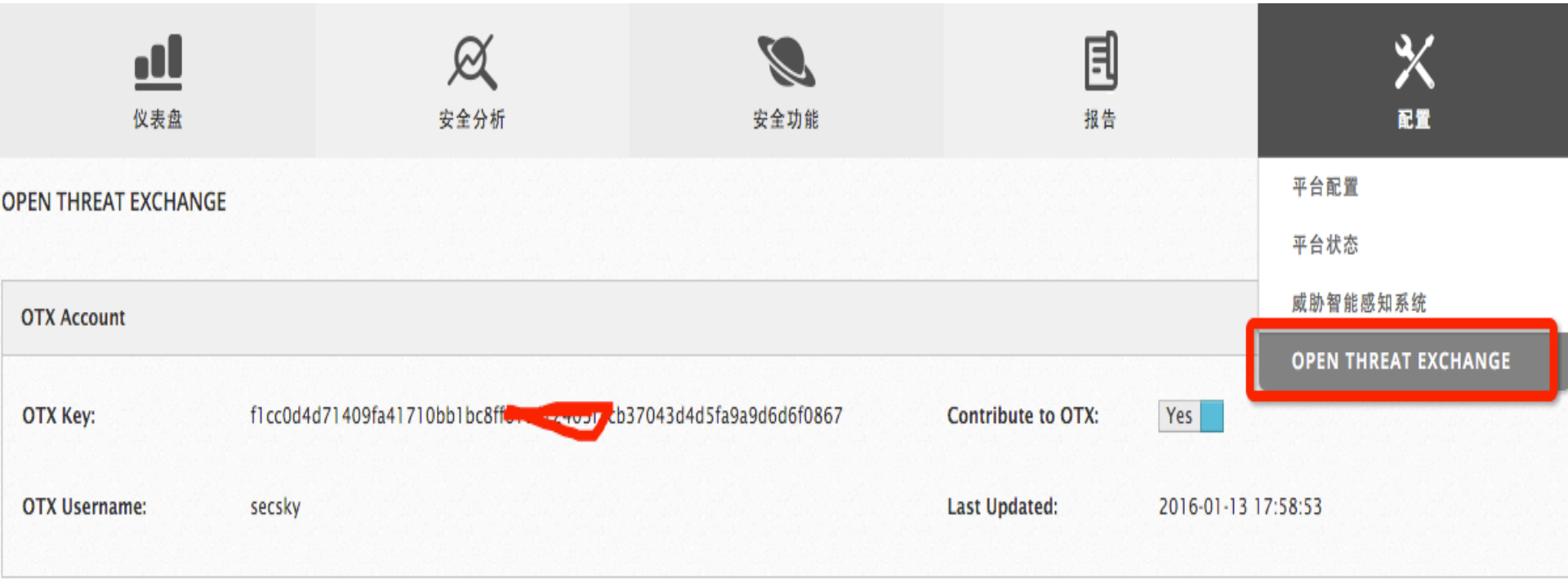
Alert detail:
* userdata2: yz-soc-sensor-01
* userdata1: invalid user
* protocol: tcp
* rep_rel_dst: 0
* context_id: c9819892-7d43-11e5-9878-eb0760cbdae4
* actions: 1
* reliability: 2
* plugin_sid: 1
* rep_prio_src: 0
* priority: 3
* src_port: 48291
* event_id: bf4b11e5-ae7f-000c-29d5-abe2278f2942
* src_ip: 172.17.69.199
* backlog_id: 29d7a32b-bf1f-11e5-962d-000c97b911e6
* plugin_id: 4003
* sensor: 10.8.13.69
* username: secsky2
* risk: 0
* rep_prio_dst: 0
* date: 2016-01-20 15:55:21
* type: event
* rep_rel_src: 0
* dst_port: 22
* dst_ip: 10.8.13.69
* policy_id: a6f9d906-6010-edac-8d67-d93a2f99bd0e

威胁情报交换

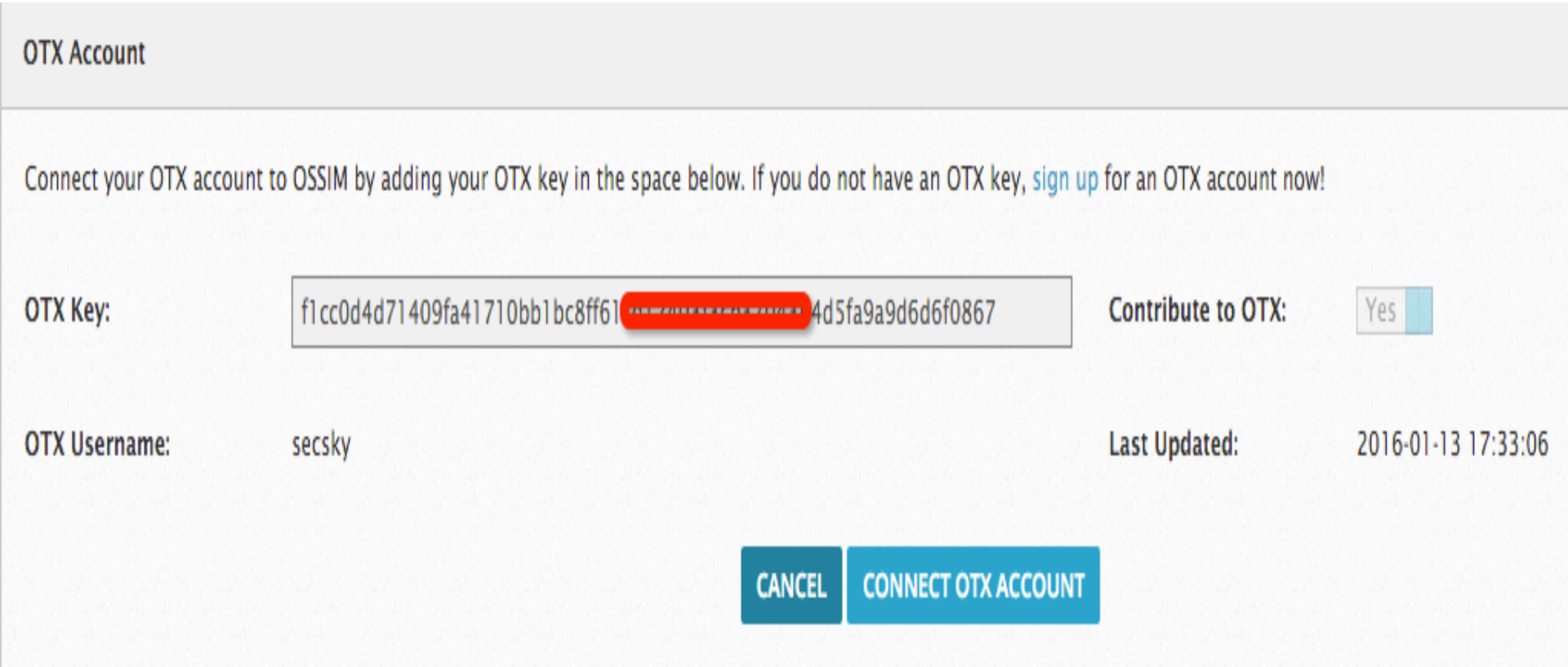
注册帐号


AlienVault, Inc. [US]
https://otx.alienvault.com/settings/
公司内部系统
漏洞平台
在线查询
python开发
日志分析
内部安全系统
nginx_lua
codeigniter在nginx安
Rule conver
OPEN THREAT EXCHANGE
BROWSE
CREATE PULSE
SEARCH
SECSKY
0 AWARDS
0 PULSES
Settings
Email Notifications
When I have a new follower
When someone I follow creates a new Pulse
When a Pulse I'm subscribed to has changed
CHANGE PASSWORD
OTX Key
Key
f1cc0d4d71409fa41710bb1bc8ff61c[redacted]7043d4d5fa9a9d6d6f0867
Connect to AlienVault USM or OSSIM
Use the OTX API SDK

配置OTX KEY


仪表盘
安全分析
安全功能
报告
配置
平台配置
平台状态
威胁智能感知系统
OPEN THREAT EXCHANGE
OPEN THREAT EXCHANGE
OTX Account
OTX Key:
f1cc0d4d71409fa41710bb1bc8ff
cb37043d4d5fa9a9d6d6f0867
Contribute to OTX:
Yes
OTX Username:
secsky
Last Updated:
2016-01-13 17:58:53

配置OTX KEY


OTX Account
Connect your OTX account to OSSIM by adding your OTX key in the space below. If you do not have an OTX key, sign up for an OTX account now!
OTX Key:
f1cc0d4d71409fa41710bb1bc8ff61
4d5fa9a9d6d6f0867
Contribute to OTX:
Yes
OTX Username:
secsky
Last Updated:
2016-01-13 17:33:06
CANCEL
CONNECT OTX ACCOUNT

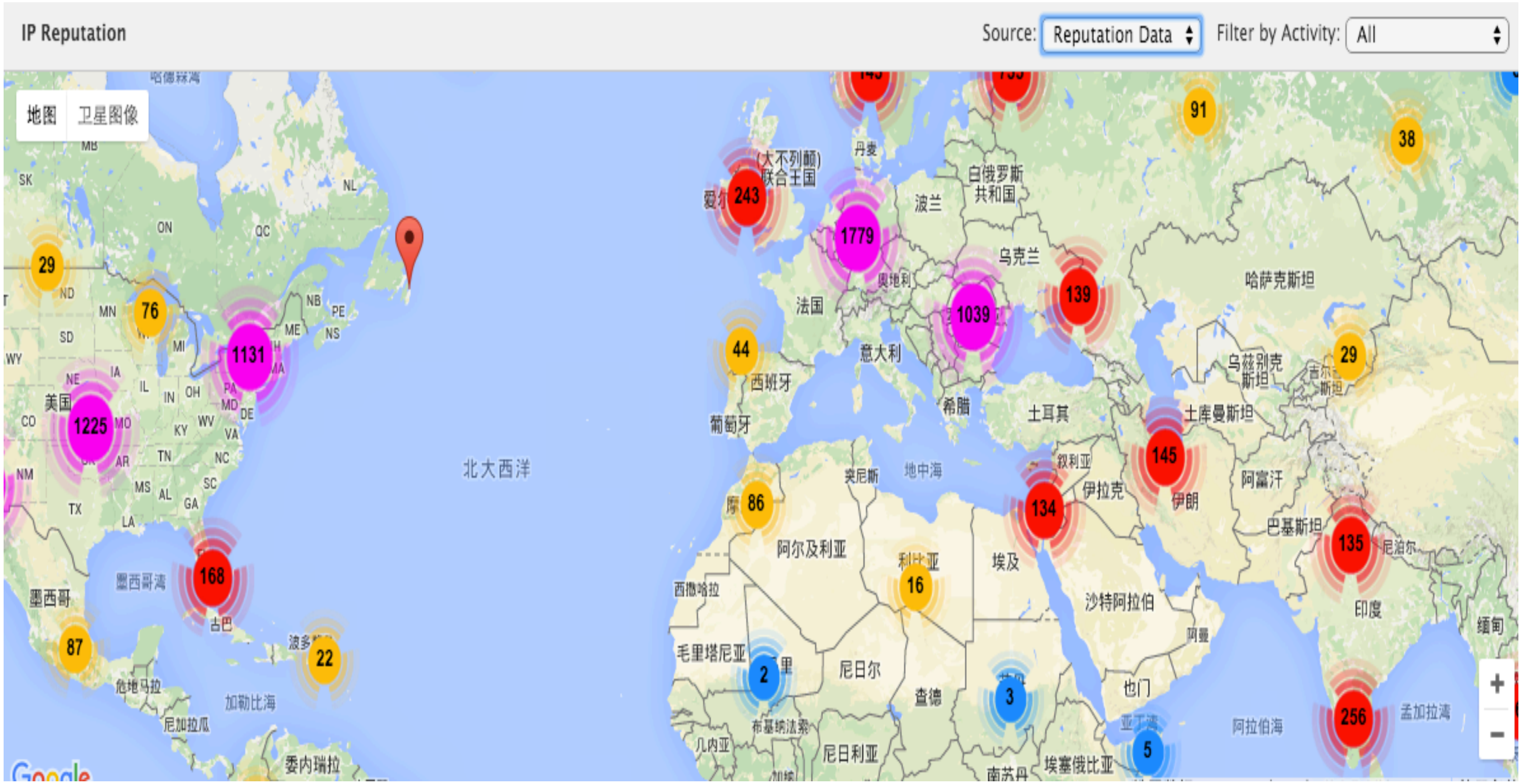
获取数据

说明：每小时更新一次

攻击态势

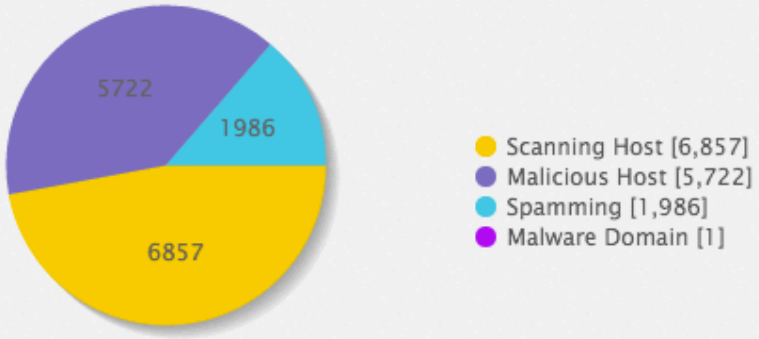
Pulses Subscribed	Indicators	Last Updated
393	18,478	2016-01-13 17:58:53

获取数据


IP Reputation
Source: Reputation Data
Filter by Activity: All
地图
卫星图像
北大西洋
1779
1225
1131
1039
256
243
168
145
139
135
134
91
87
86
76
44
38
29
29
22
16
5
3
2
美国
墨西哥
墨西哥湾
古巴
加勒比海
委内瑞拉
危地马拉
尼加拉瓜
法国
意大利
西班牙
葡萄牙
波兰
乌克兰
丹麦
希腊
土耳其
地中海
阿尔及利亚
埃及
沙特阿拉伯
伊拉克
伊朗
阿富汗
巴基斯坦
印度
哈萨克斯坦
土库曼斯坦
尼日尔
尼日利亚
乍得
毛里塔尼亚
西撒哈拉
也门
阿拉伯海
孟加拉湾
缅甸
埃塞俄比亚
南苏丹

获取数据

MALICIOUS IPS BY ACTIVITY



TOP 10 COUNTRIES

Country	Unique IPs
United States	3,438
China	2,357
Russian Federation	780
Germany	471
Ukraine	449
France	446
South Korea	387
Netherlands	360
Brazil	322
Viet Nam	293

主要内容

- OSSIM简介
- OSSIM部署
- OSSIM应用
- OSSIM常见问题

OSSIM常见问题

- 如何添加 Sensor
- 虚拟机如何接收镜像流量
- 邮件配置
- WEB管理后台汉化
- OSSIM学习资料

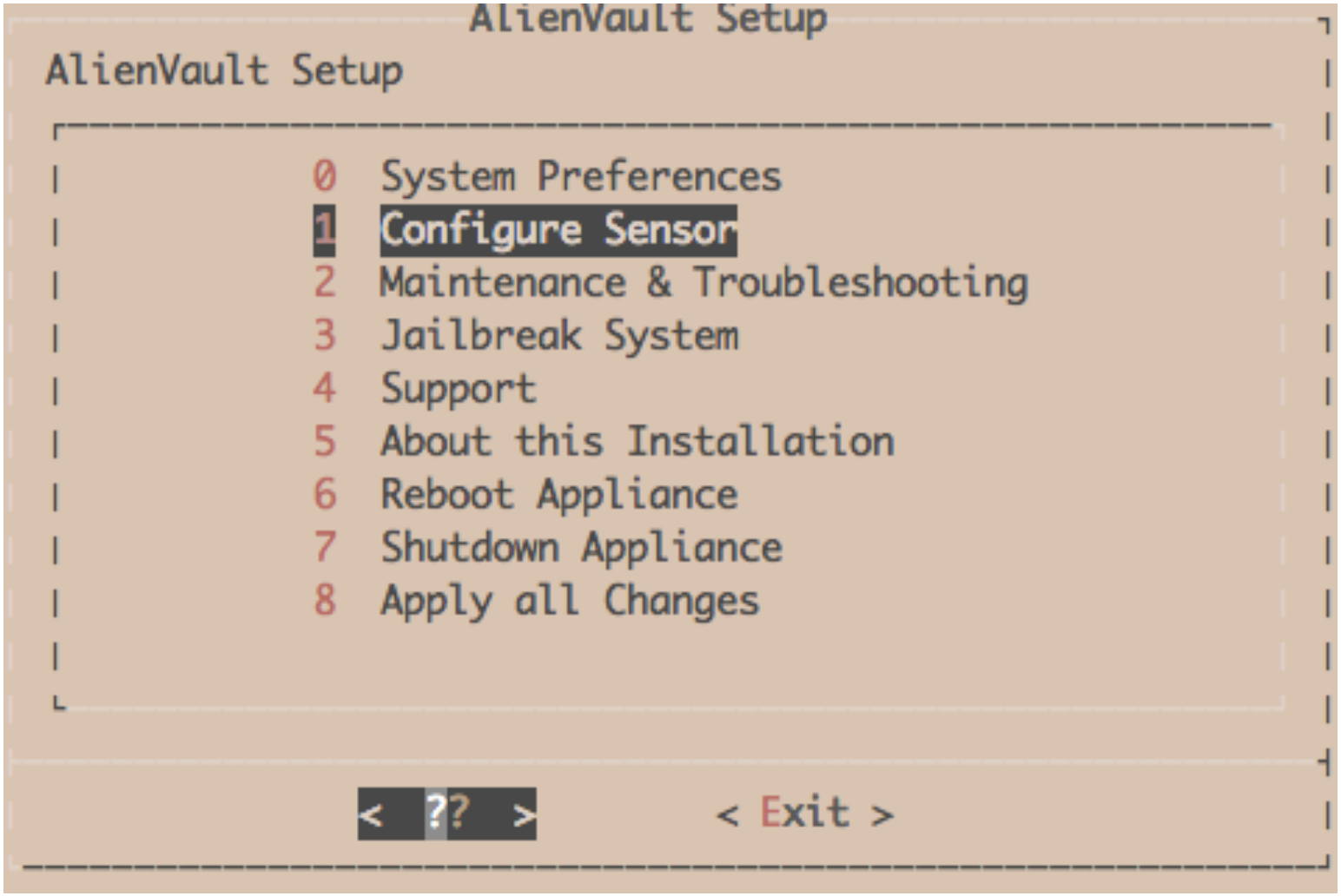
如何添加 Sensor

操作步骤：

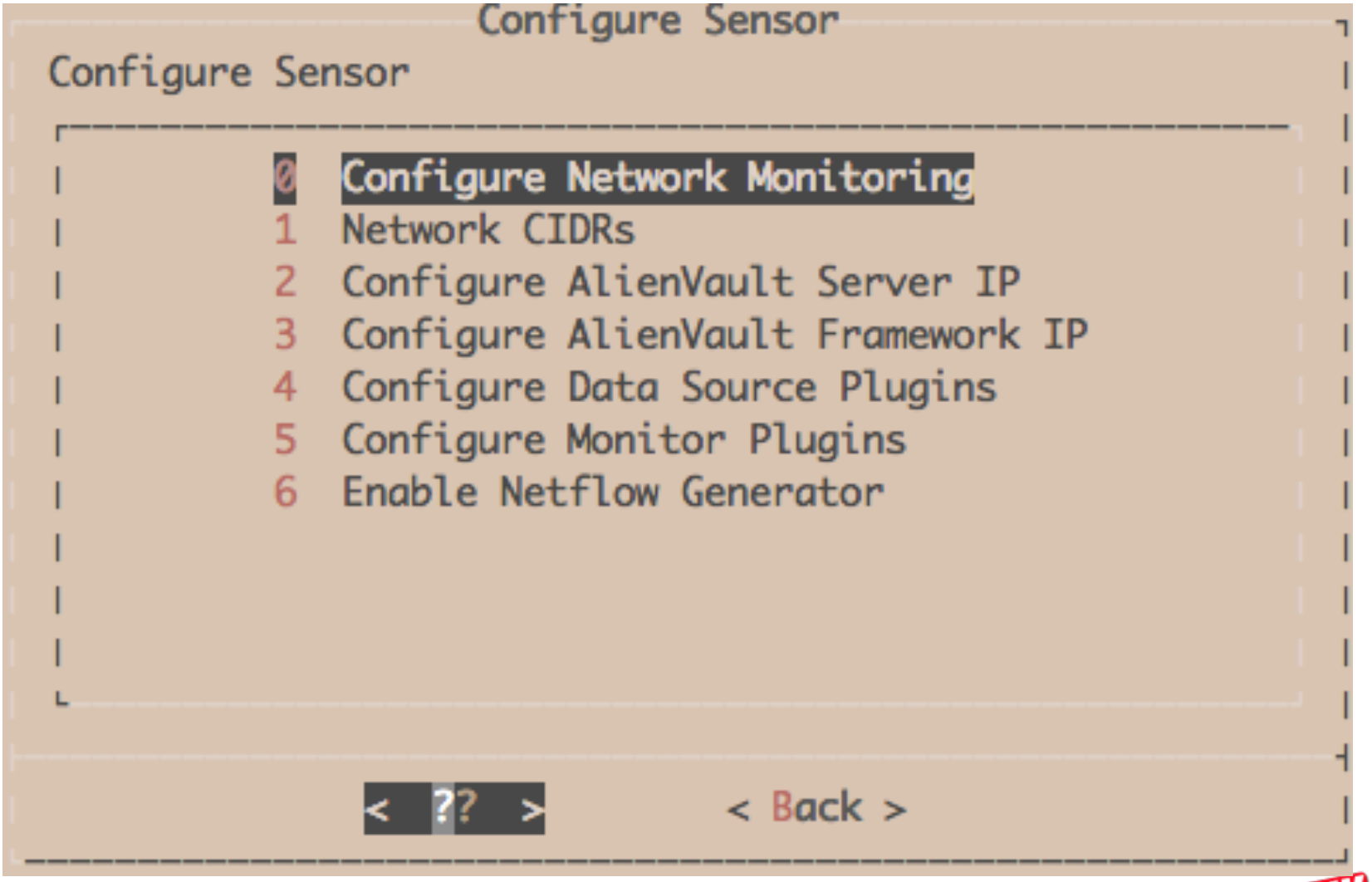
1. 通过SSH登录Sensor，配置相应信息并选择“应用改变”选项，使配置生效

2. 登录WEB管理后台，添加Sensor

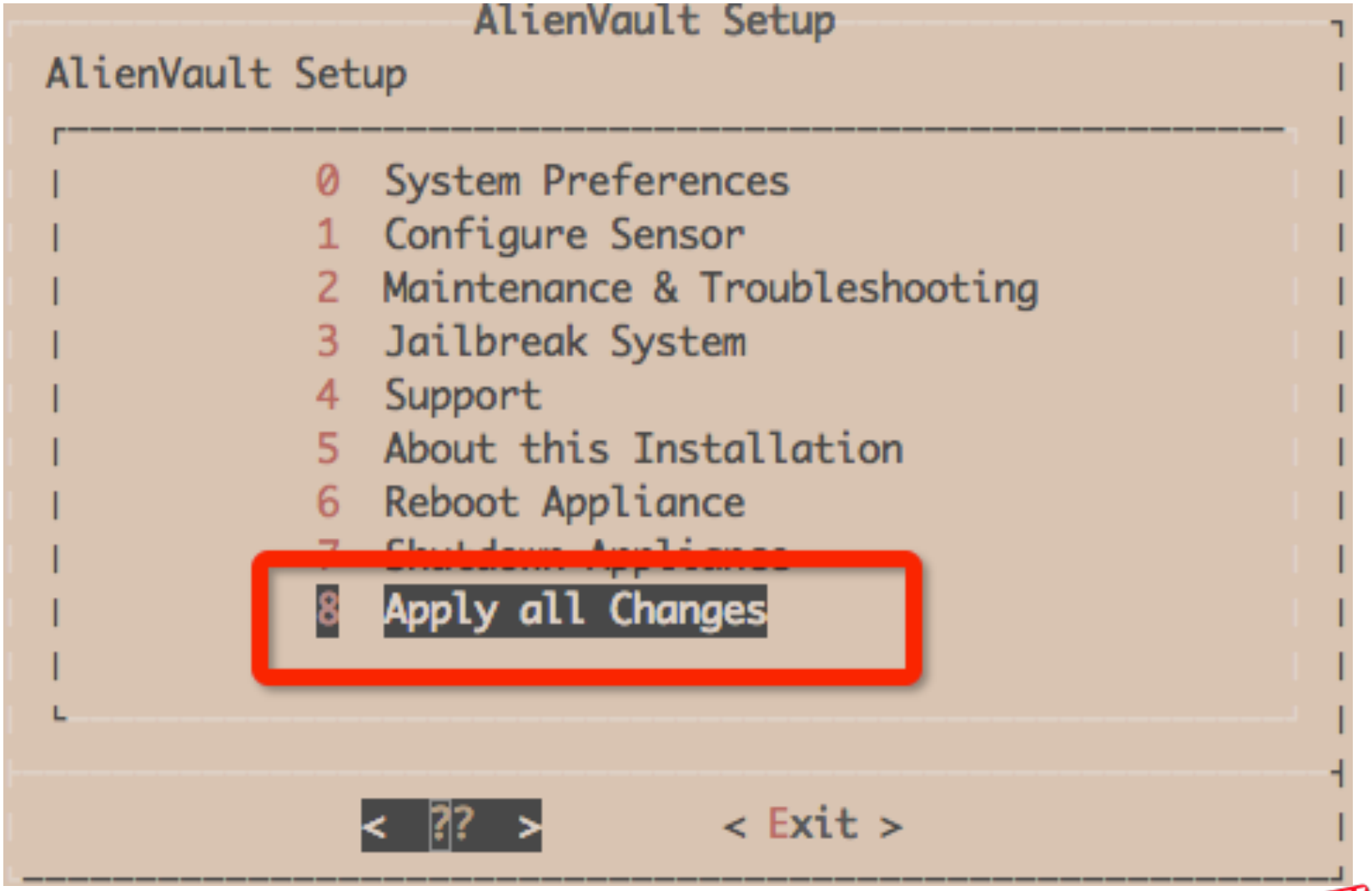
如何添加 Sensor


AlienVault Setup
AlienVault Setup
0 System Preferences
1 Configure Sensor
2 Maintenance & Troubleshooting
3 Jailbreak System
4 Support
5 About this Installation
6 Reboot Appliance
7 Shutdown Appliance
8 Apply all Changes
< ?? >
< Exit >

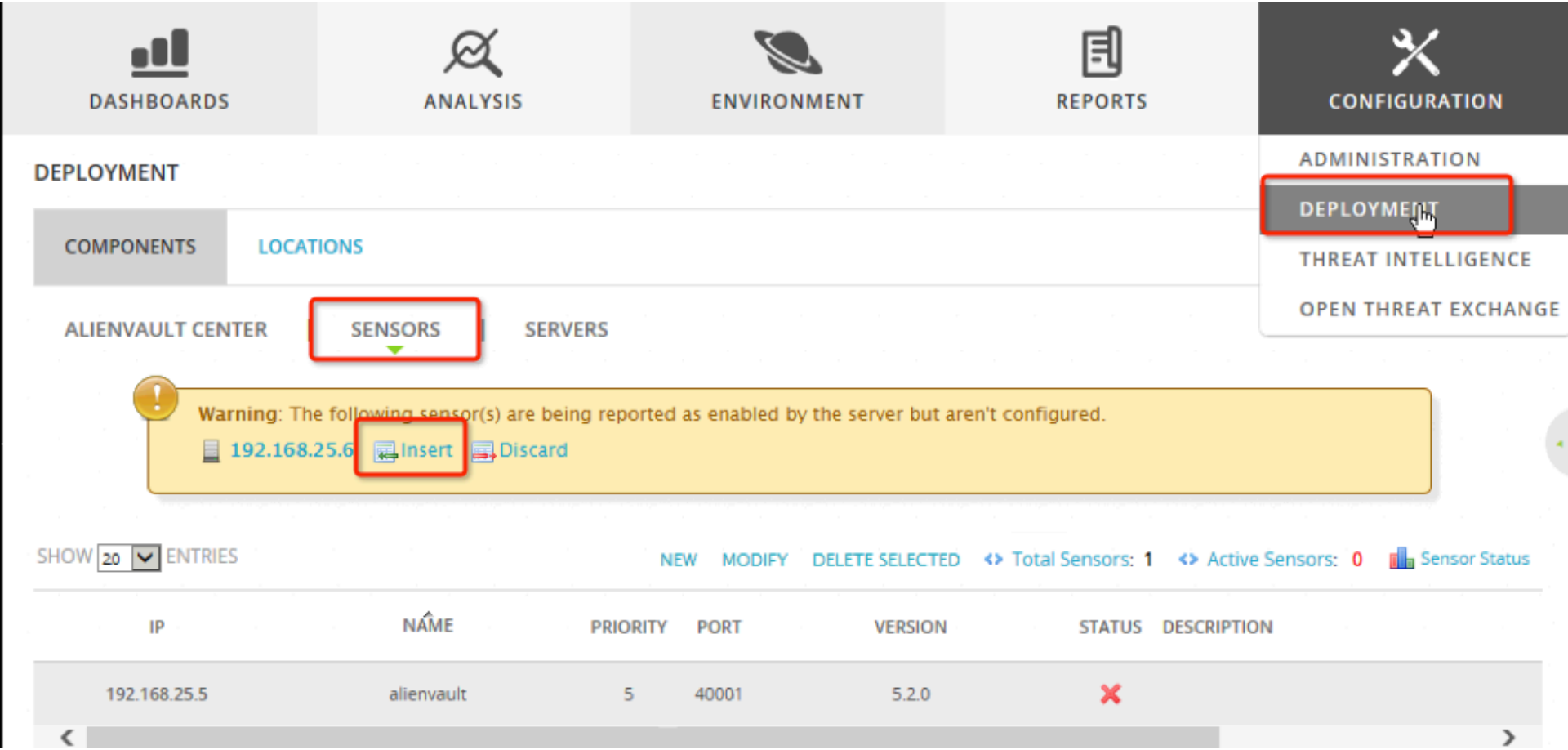
如何添加 Sensor


Configure Sensor
Configure Sensor
0 Configure Network Monitoring
1 Network CIDRs
2 Configure AlienVault Server IP
3 Configure AlienVault Framework IP
4 Configure Data Source Plugins
5 Configure Monitor Plugins
6 Enable Netflow Generator
< ?? >
< Back >

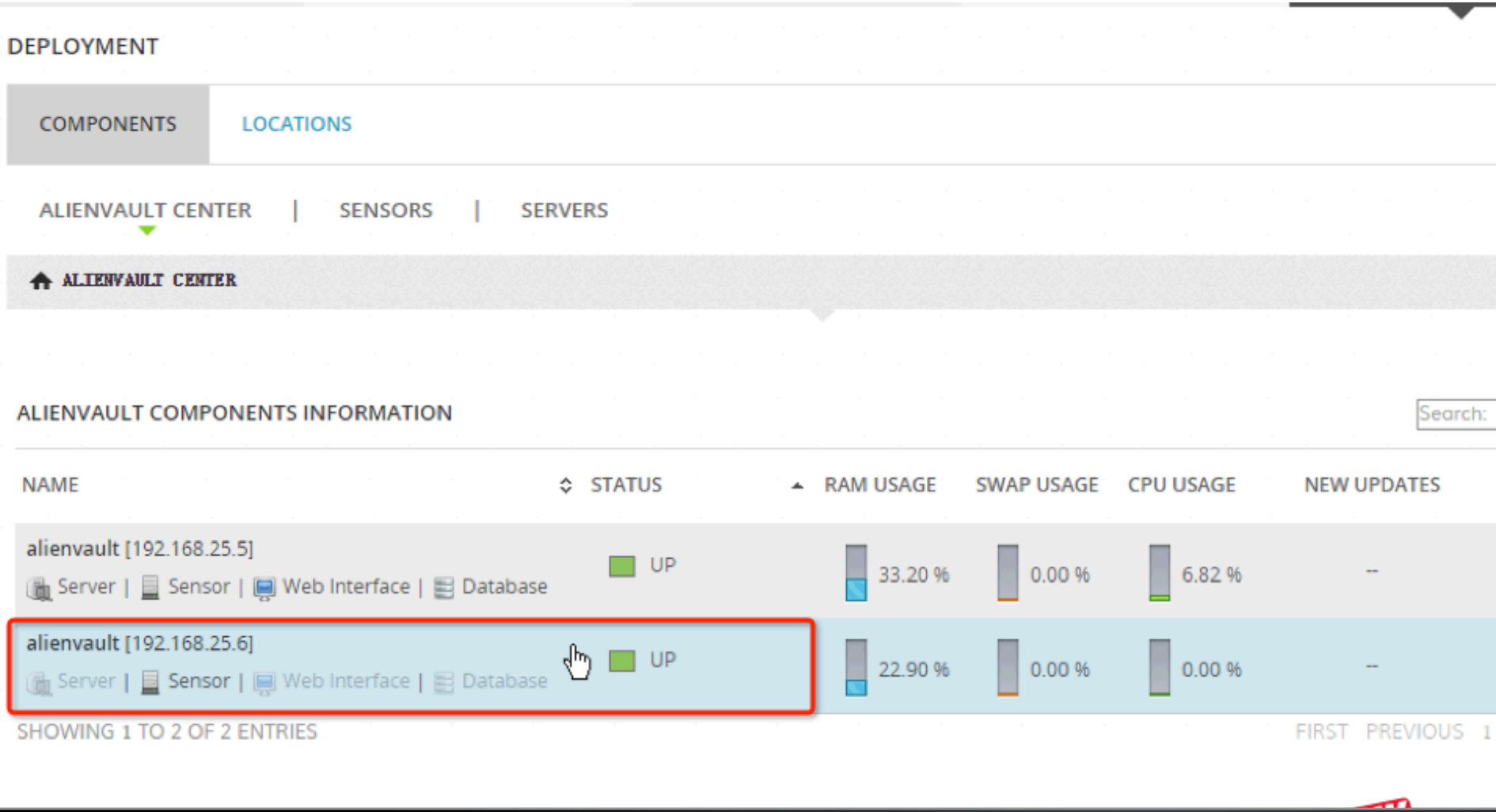
如何添加 Sensor


AlienVault Setup
AlienVault Setup
0 System Preferences
1 Configure Sensor
2 Maintenance & Troubleshooting
3 Jailbreak System
4 Support
5 About this Installation
6 Reboot Appliance
8 Apply all Changes
< ?? >
< Exit >

如何添加 Sensor


DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
ADMINISTRATION
DEPLOYMENT
THREAT INTELLIGENCE
OPEN THREAT EXCHANGE
DEPLOYMENT
COMPONENTS
LOCATIONS
ALIENVAULT CENTER
SENSORS
SERVERS
Warning: The following sensor(s) are being reported as enabled by the server but aren't configured.
192.168.25.6
Insert
Discard
SHOW 20 ENTRIES
NEW
MODIFY
DELETE SELECTED
Total Sensors: 1
Active Sensors: 0
Sensor Status
IP
NAME
PRIORITY
PORT
VERSION
STATUS
DESCRIPTION
192.168.25.5
alienvault
5
40001
5.2.0

如何添加 Sensor


DEPLOYMENT
COMPONENTS
LOCATIONS
ALIENVAULT CENTER | SENSORS | SERVERS
ALIENVAULT CENTER
ALIENVAULT COMPONENTS INFORMATION
Search:
NAME
STATUS
RAM USAGE
SWAP USAGE
CPU USAGE
NEW UPDATES
alienvault [192.168.25.5]
Server | Sensor | Web Interface | Database
UP
33.20 %
0.00 %
6.82 %
--
alienvault [192.168.25.6]
Server | Sensor | Web Interface | Database
UP
22.90 %
0.00 %
0.00 %
--
SHOWING 1 TO 2 OF 2 ENTRIES
FIRST PREVIOUS 1

虚拟机如何接收镜像流量

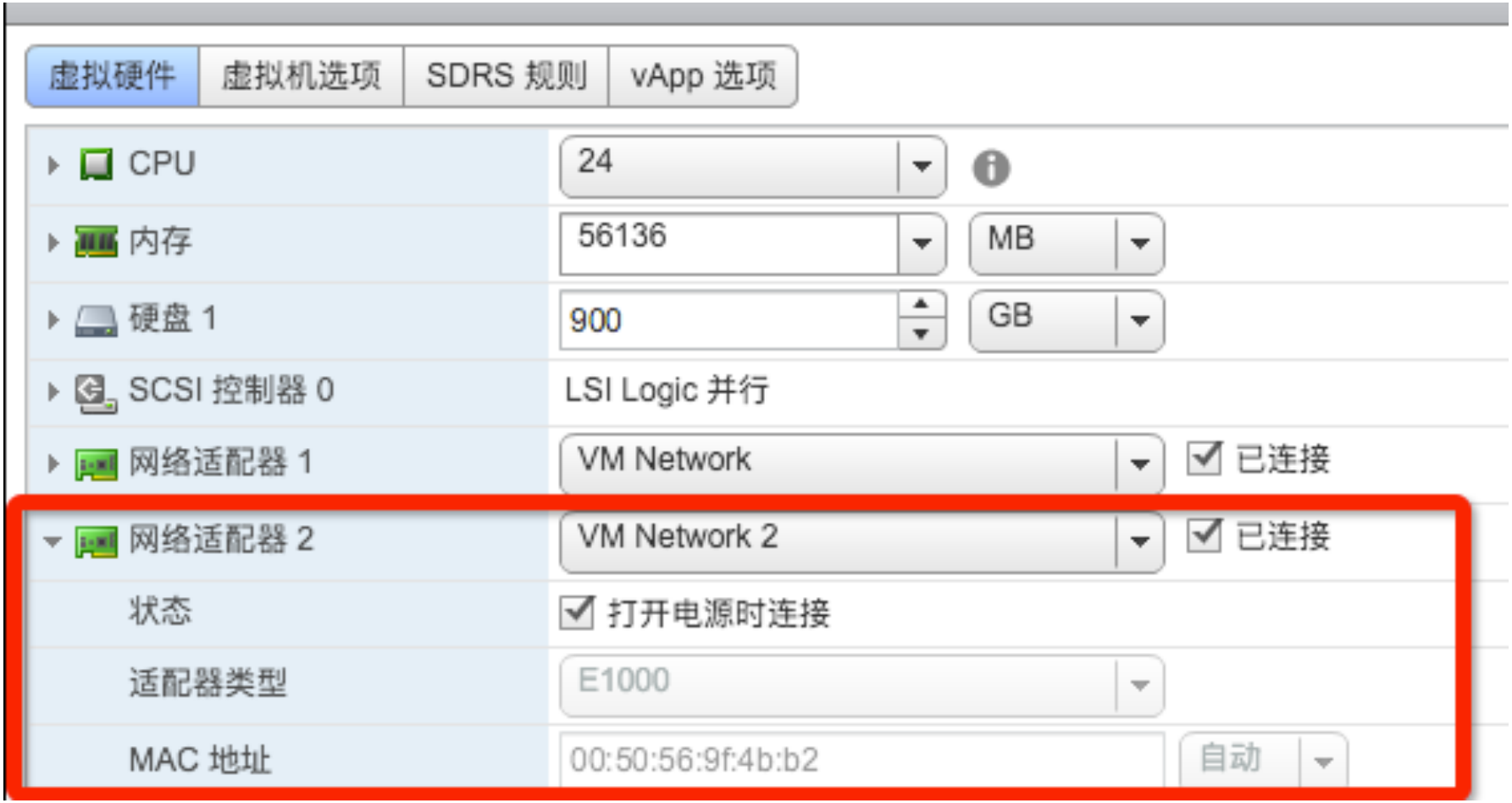
操作步骤：

1. 登录vmware vCenter，为接收镜像流量服务器（虚拟机）添加一块网卡，用来接收镜像流量；

说明：如果已添加网卡，则忽略此步骤

2. 选择虚拟机所在宿主机，增加一个虚拟交换机，将虚拟机新添加的网卡与宿主机接收镜像流量的网卡添加至该虚拟交换机即可

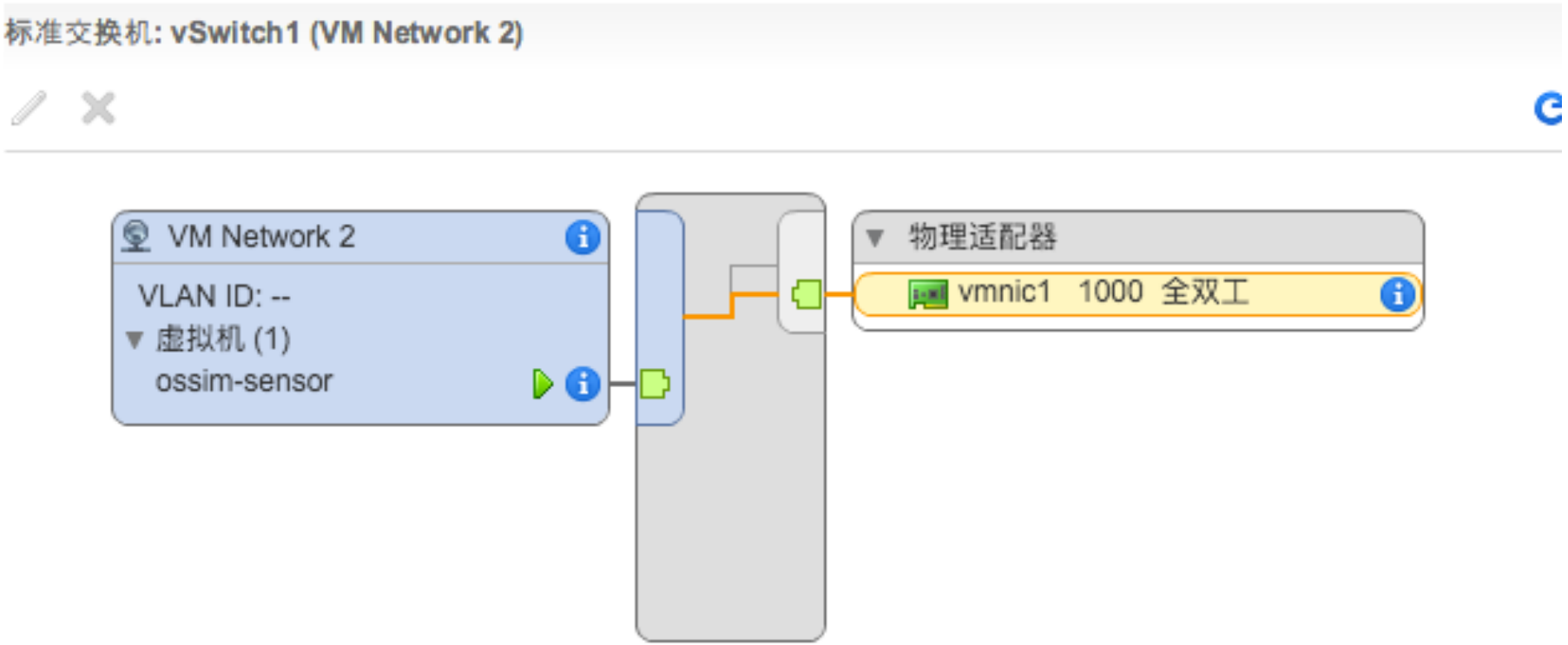
虚拟机如何接收镜像流量



虚拟机如何接收镜像流量


```
eth1      Link encap:Ethernet  HWaddr 00:50:56:9f:4b:b2
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:26197668993 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6598815334523 (6.0 TiB)  TX bytes:0 (0.0 B)
```

虚拟机如何接收镜像流量



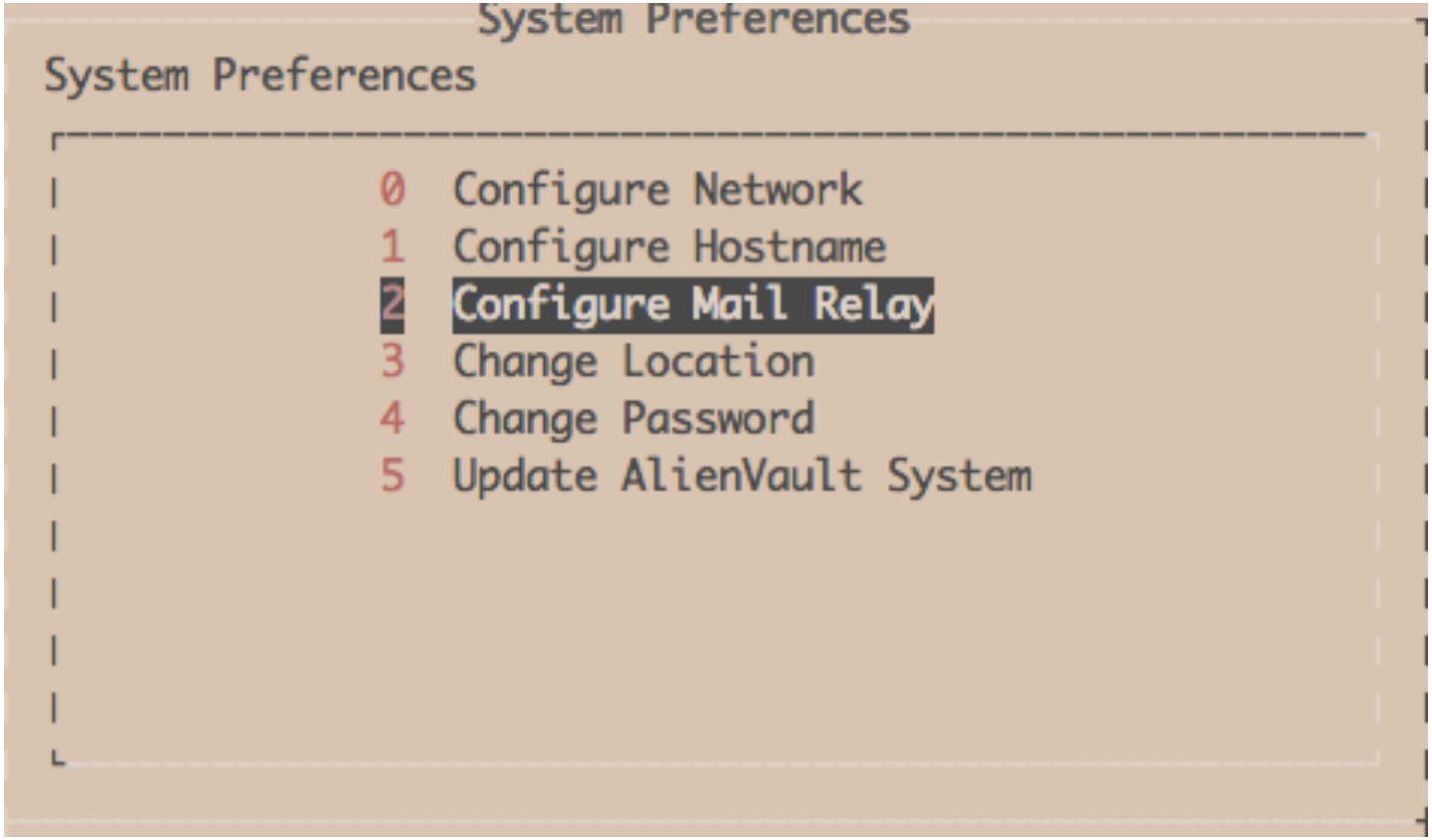
邮件配置

两种配置方式：

1. 控制台配置

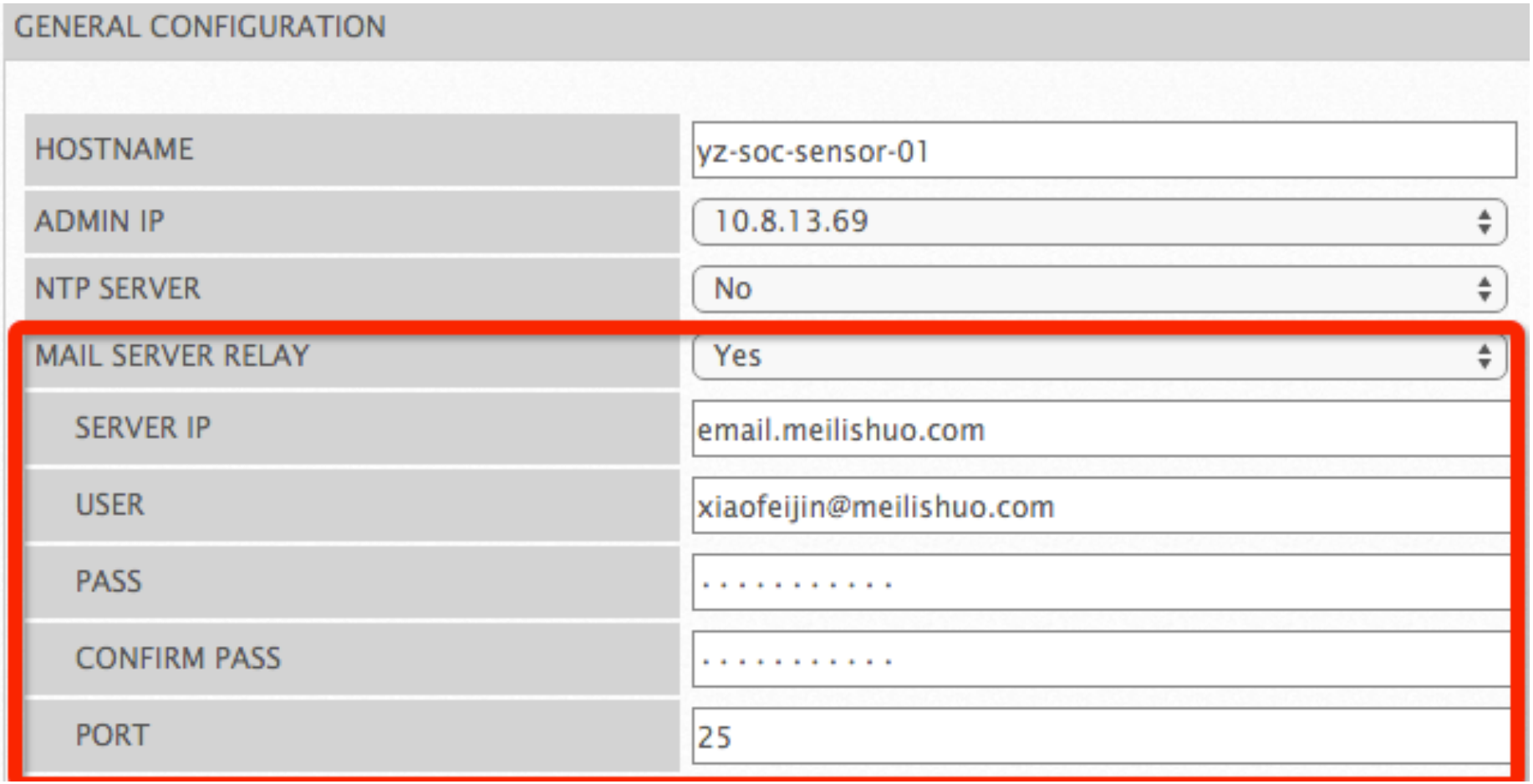
2. WEB管理界面配置

邮件配置



说明：配置完成后需要选择“应用改变”，使配置生效

邮件配置


GENERAL CONFIGURATION
HOSTNAME
yz-soc-sensor-01
ADMIN IP
10.8.13.69
NTP SERVER
No
MAIL SERVER RELAY
Yes
SERVER IP
email.meilishuo.com
USER
xiaofeijin@meilishuo.com
PASS
CONFIRM PASS
PORT
25

WEB管理后台汉化

原理：直接修改相应源码

建议：修改前一定要记得备份

WEB根目录：/usr/share/ossim/www

```
yz-soc-server-01:~# ls /usr/share/ossim/www
404.php             av_tree.php     doc                 incidents       nagios
action              backup          downloads           index.php       netgroup
alarm               compliance      favicon.ico         java            netscan
av_asset            conf            forensics           js              nfsen
av_backup           control_panel   graphs              legal           notes
av_center           dashboard       help                loading.php     ossec
av_routing.php      deployment      home                local_menu.php  ossem
av_schedule_scan    directives      host_report_menu.php message_center  otx
```

WEB管理后台汉化

汉化后效果预览：

WEB管理后台汉化

一、banner部分修改及汉化方法

如果想要修改默认banner信息和汉化这部分的导航，需要修改下面的文件：

文件保存位置：/usr/share/ossim/www/home/index.php

```
yz-soc-server-01:/usr/share/ossim/www/home# pwd
/usr/share/ossim/www/home
yz-soc-server-01:/usr/share/ossim/www/home# ls
controllers  index.php  index.php.bak  js  providers
yz-soc-server-01:/usr/share/ossim/www/home#
```

WEB管理后台汉化

打开index.php，找到如下代码，进行修改：

```
215                     <div id='header_logo'>
216                         <!--修改默认logo-->
217                         <!--<img src="<?php echo AV_PIXMAPS_DIR?>/logo/<?php echo ($pro) ?
    'av_contrast_logo' : 'ossim_contrast_logo' ?>.png"/>-->
218                         <h2>统一安全管理平台</h2>
219                     </div>
220
221
222                     <div id="header_options">
223                         <span id="welcome" title="<?php echo Session::get_session_user() ?>"
    class="tip">
224                             <?php echo _("Welcome") . " " . substr(Session::get_session_user(),
     0, 15) ?>
225                         </span>
226                         <span class="sep_ri">|</span>
227                         <div id="top_system_info"></div>
228
229                         <!-- Notification Center -->
230                         <a id="link_notification_center" href="javascript:void(0)">
231                             <img id='img_notif' alt="Notification Center"
    src='/ossim/pixmaps/statusbar/envelope.png' />
232                             <span id='notif_bubble'>0</span>
233                         </a>
234
235                         <a id="link_settings" href="javascript:void(0);"><?php echo
    _("用户设置") ?></a>
236                         <a id="link_support" href="javascript:void(0);"><?php echo
    _("技术支持") ?></a>
237                         <a href="<?php echo  AV_MAIN_PATH ?>/session/login
    .php?action=logout"><?php echo _("注销") ?></a>
238                     </div>
```

WEB管理后台汉化

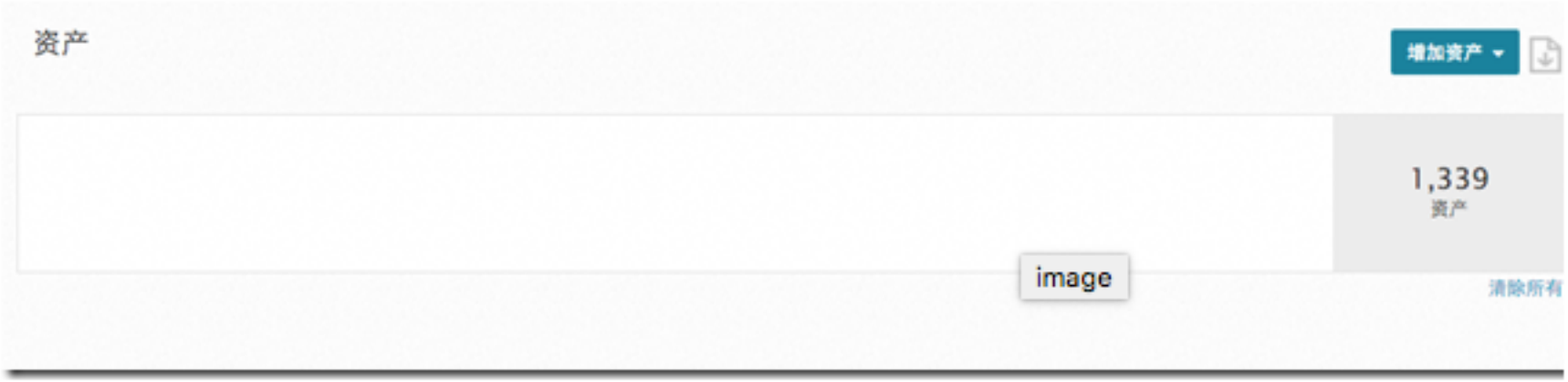
二、导航菜单汉化

导航菜单汉化需要修改menu.inc文件，该文件位于”/usr/share/ossim/include/classes”目录下，看下源码和页面导航的对应关系：

WEB管理后台汉化

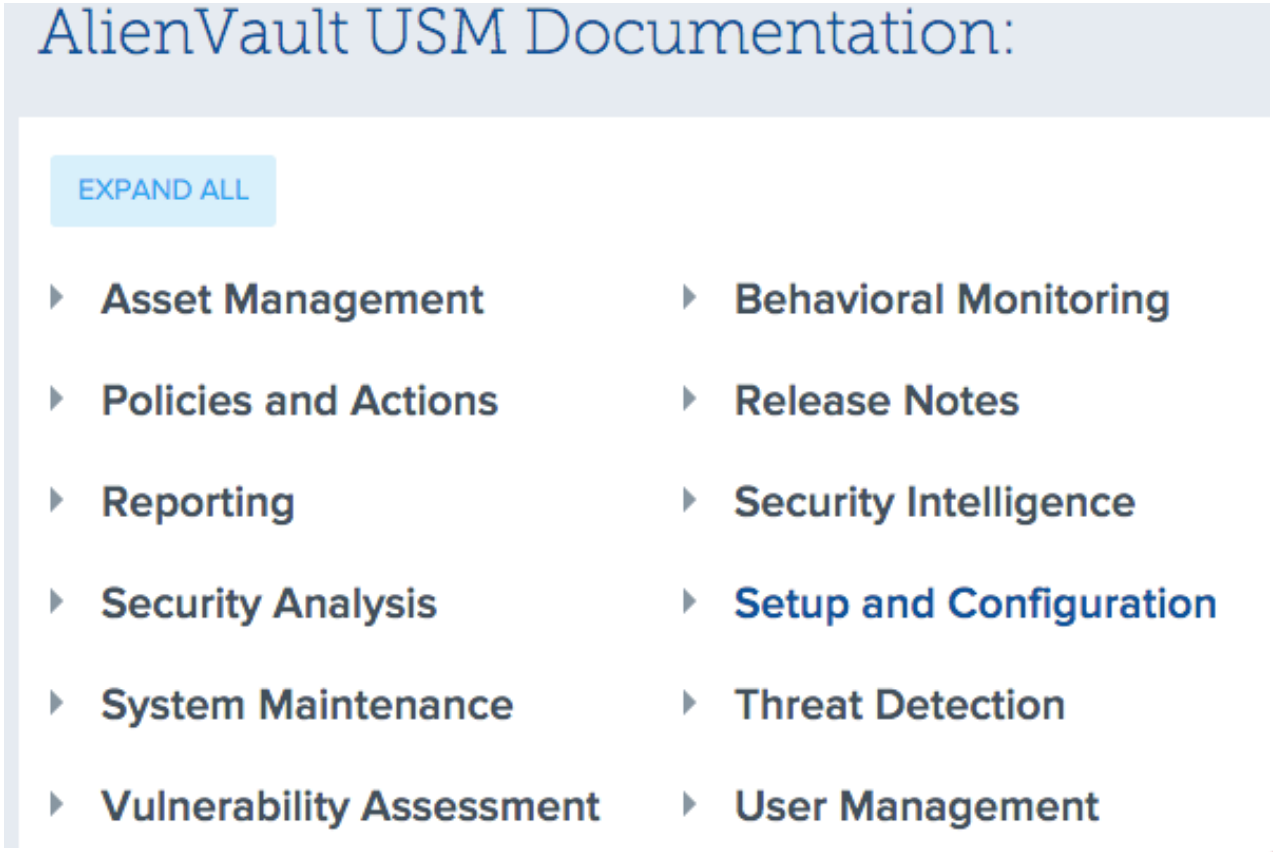
三、页面英文汉化方法

这部分比较麻烦，但难度不大，我这里并不建议大家对全部页面进行汉化，因为意义不大。如果非要这样话的样，可以找到相应的页面进行修改。这里以“资产管理”页面为例进行说明，该页面位于“usr/share/ossim/www/av_asset/asset/views “，文件名为list.php，找到相应内容进行修改。下面是修改后的效果：



OSSIM资料

https://www.alienvault.com/documentation/usm



感谢聆听