SACC

卓越 5周年 变迁

2013中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2013

大数据下的IT架构变迁

开源主机入侵检测系统

OSSEC

关于我

- 林鹏@当当网
- ID:Lion_00
- 安全爱好者
- CCIE(SECURITY)
- CISSP
- http://weibo.com/lion00
- QQ:69278183

安全“杯具”

什么是 

- Open Source SECurity
- Open Source Host-based Intrusion Detection System

优势

- 跨平台
- 支持无客户端模式
- 合规性需求
- Real-time and Configurable Alerts
- 集中管理
- ……

OSSEC 的主要功能

文件完整性检查

- 检查文件变化（包括内容，大小，属主等等）
- 实时变更报警
- 文件建立告警
- 注册表检查

```
Size changed from '2662' to '2736'
What changed:
29,30c29,32
<                 local maxn = table.maxn(temp_table);
<
---
>         local maxn = 0;
>         if "table" == type(temp_table) then
>             maxn = table.maxn(temp_table);
>         end
Old md5sum was: 'bec9cffc437440b63a28f816ae431d55'
New md5sum is : '04b41aa4466ea8ba4a19fabd01ff46bd'
Old sha1sum was: '4941e6cf265fb0df7959718e10a59a2cbb993f70'
New sha1sum is : '8eed26d0db88513fdbaa8d192d63e601b40ee216'
```

日志分析

- 丰富的rule规则
- 支持自定义rule
- 支持自定义decoder
- 支持自定义command
- 预检查规则

日志分析

```
[root@idc2-ossec-server rules]# cat testrule.xml
<group name="localte
  <rule id="16666"
    <match>lion_00</
    <description>lic
  </
   <rule id="18891" level="0">
    <match>session opened for user check
    <description>ignore checkos</descrip
   </rule>

/group>

root@idc2-ossec-server rules]#
root@idc2-ossec-server rules]#
root@idc2-ossec-server rules]#
root@idc2-ossec-server rules]# logger
ion_00
```

```
[root@idc2-ossec-server rules]# ../bin/ossec-logtest
2013/08/19 16:16:12 ossec-testrule: INFO: Reading local decoder file.
2013/08/19 16:16:12 ossec-testrule: INFO: Started (pid: 7348).
ossec-testrule: Type one log per line.
lion_00
```

收件人: sec
抄送:
主题: OSSEC Notification - idc2-ossec-server - Alert level 10

OSSEC HIDS Notification.
2013 Aug 19 16:20:52

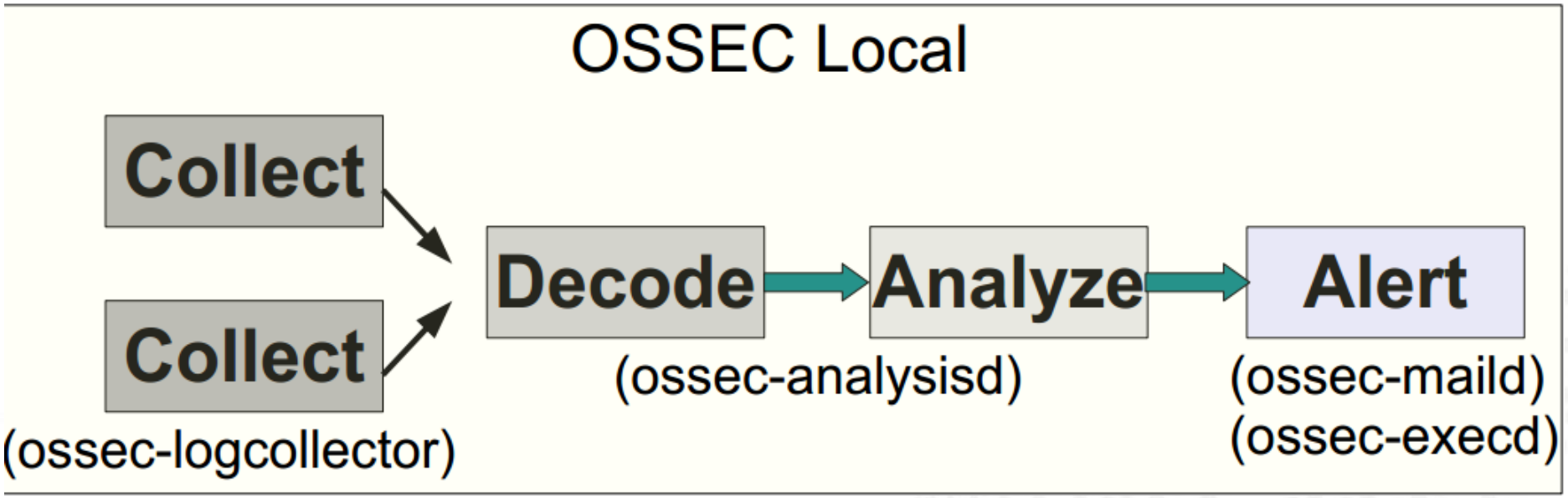
Received From: idc2-ossec-server->/var/log/messages
Rule: 16666 fired (level 10) -> "lion_00"
Portion of the log(s):

Aug 19 16:20:50 idc2-ossec-server root: lion_00

--END OF NOTIFICATION

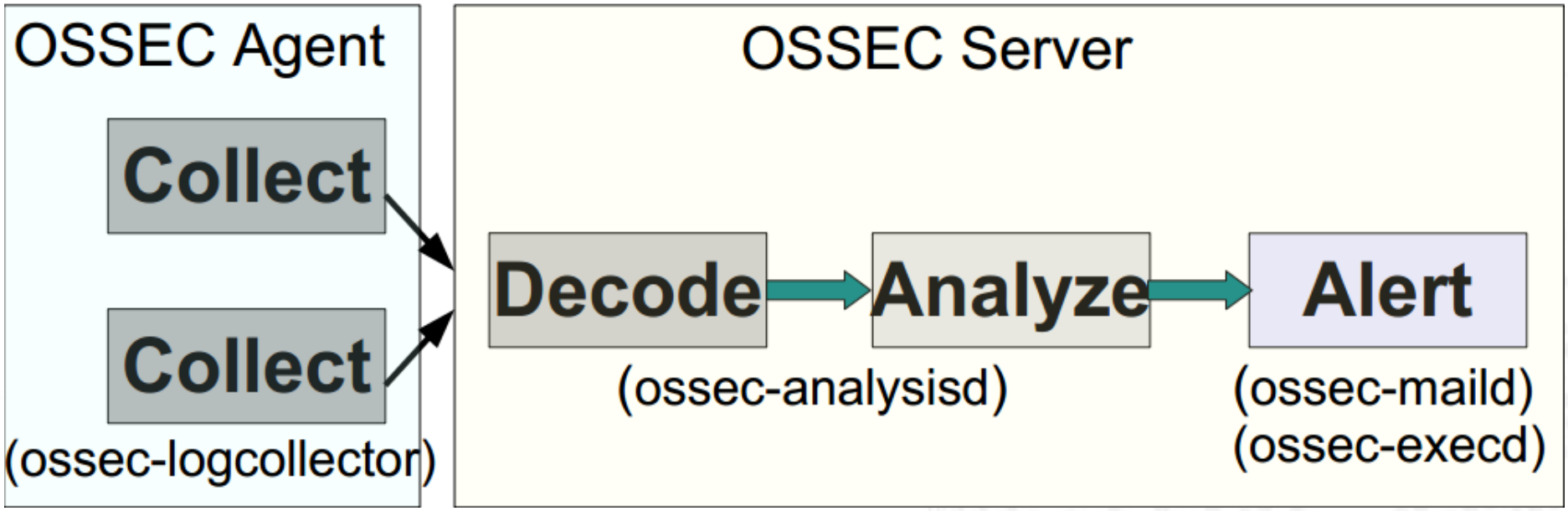
OSSEC LOG FLOW

Log flow (local)



OSSEC LOG FLOW

Log flow (agent/server)



Rootkit 检测

- Rootkit 检测
- 木马检测

```
Process '27256' hidden from /proc. Possible kernel level rootkit.
```

自动响应

- The Active Response feature within OSSEC can run applications on an agent or server in respo nse to certain triggers. These triggers can besp ecific alerts, alert levels, or rule groups.

OSSEC-AR1.wmv

部署架构


OSSEC
Server


OSSEC
Server


OSSEC
Server

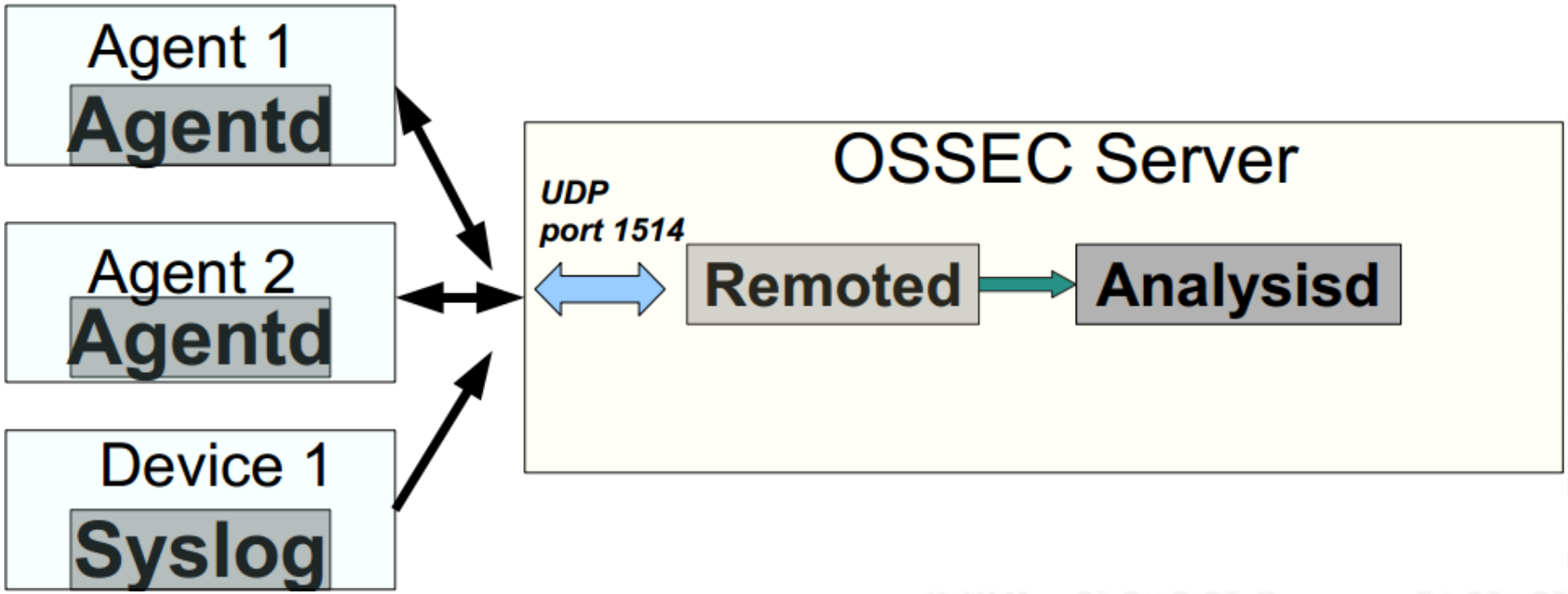

Agents
Microsoft
solaris
HP-ux
vmware


Agents
Microsoft
solaris
HP-ux
vmware


Agents
Microsoft
solaris
HP-ux
vmware

通信

Network communication



集中管理

- Ossec 支持集中管理
- 可以根据AGENT NAME， 操作系统类型下发策略
- 会覆盖与之冲突的策略

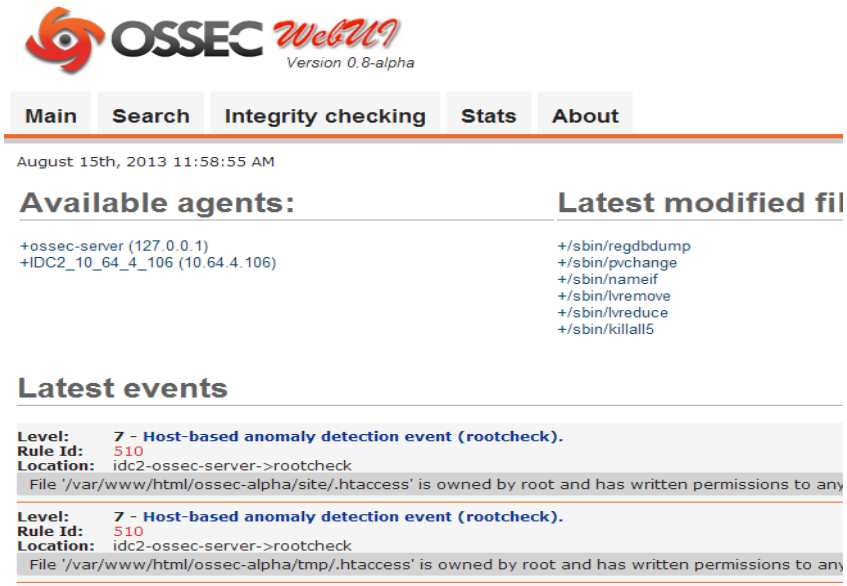
客户端自动注册

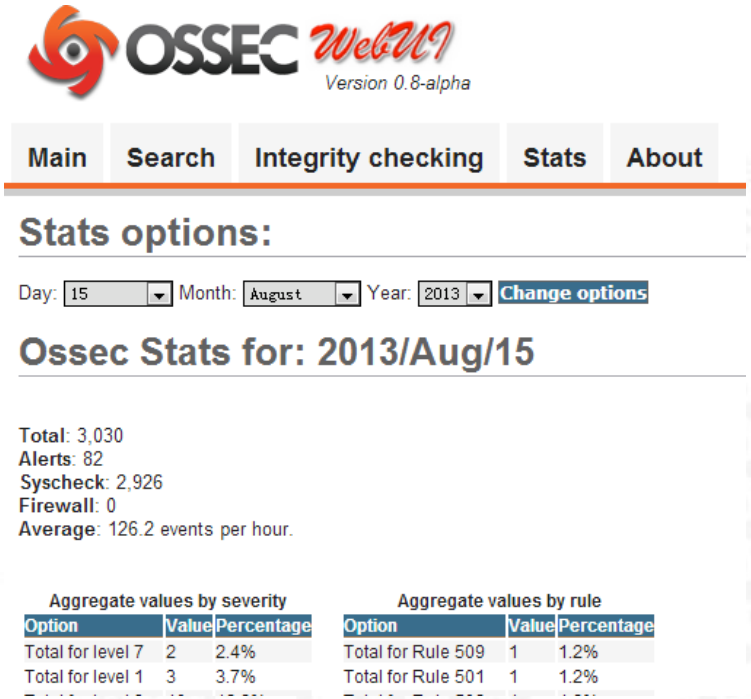
- 可以允许客户端自动注册
- 通过SSL

OSSEC 其他功能

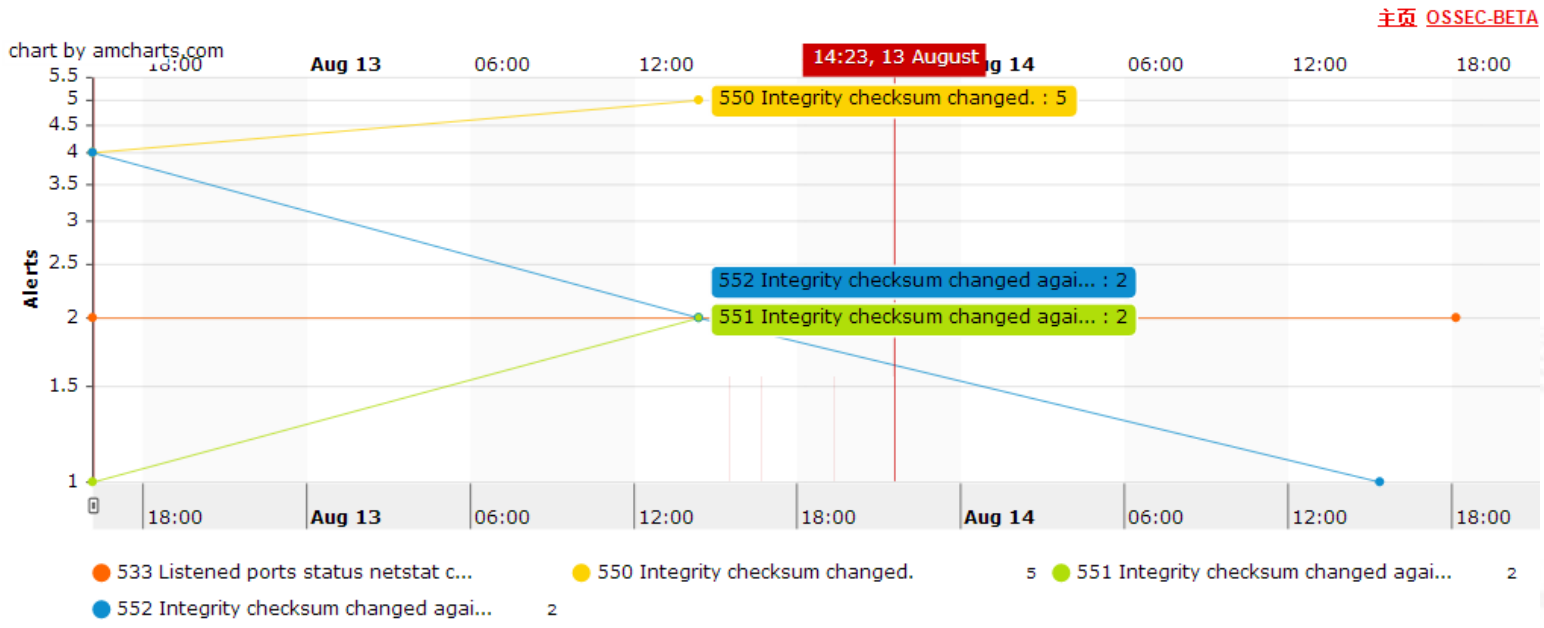
- 支持nmap 检查端口开放及变更情况
- 可以检测域名变化情况
- 检查磁盘空间及系统负载
- 检测主机端口变化
- ……

OSSEC WEBUI (官方版)





OSSEC WEBUI (1)



过滤器

级别 7+ 时长 72 统计图(分类) 主机 路径 级别 规则 类别 -- 确定

72 小时 (Level 7+)日志类型数量 TOP 10

9	Integrity Checksum Changed....
7	Integrity Checksum Changed Again (3rd ...
4	Listened Ports Status (Netstat) Change...
3	Integrity Checksum Changed Again (2nd ...

72 小时 (Level 7+)主机日志数量 Top 10

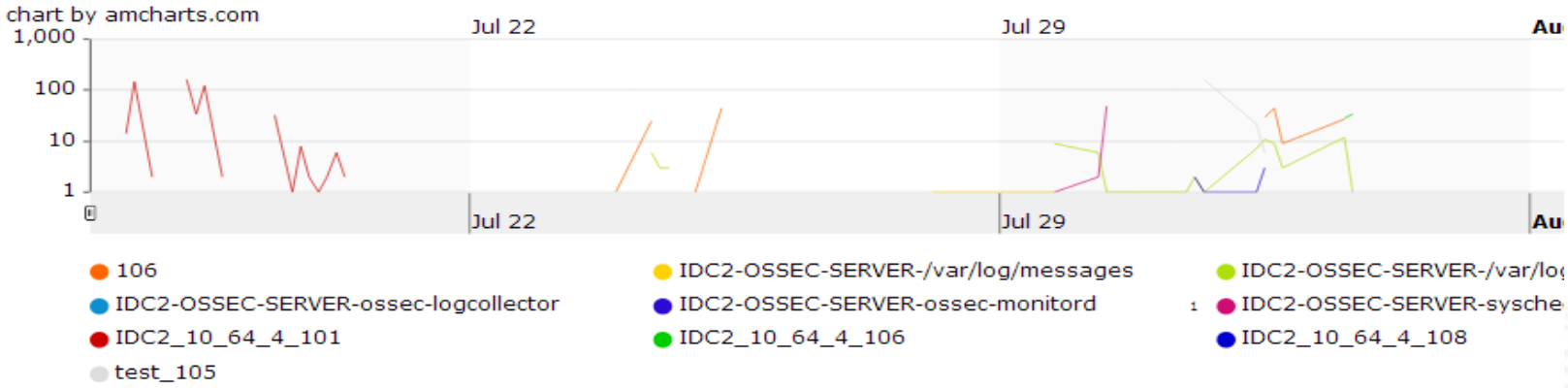
21	IDC4_10_4_12_21
2	IDC4_10_4_13_39

72 小时(Level 7+)

OSSEC WEBUI (2)

DangDang (M±M±Íø)

Index ossec-b



Filters

RuleID | Level Min: -- | From (HHMM DDMMYY): 1604 150713 | Source: -- | Data I

Category: -- | Level Max: -- | To (HHMM DDMMYY): | Path: -- | Data E

Common Patterns (Matching Our Regex)

Data

Search limited to latest 500 (of 1,428) results as per your global config. Please refine your search on increase the limit.

Download all 1,428 results as CSV

ID	Rule	Lvl	Timestamp	Location	IP	Data
2118	1006	5	2013/08/11 4:02:42	IDC2-OSSEC-SERVER->/var/log/messages		Aug 11 04:
2117	591	3	2013/08/11 4:02:42	IDC2-OSSEC-SERVER->ossec-logcollector		ossec: Fil
2116	591	3	2013/08/11 4:02:42	IDC2-OSSEC-SERVER->ossec-logcollector		ossec: Fil
2115	591	3	2013/08/11 4:02:42	IDC2-OSSEC-SERVER->ossec-logcollector		ossec: Fil
2114	5502	3	2013/08/08 4:38:48	IDC2-OSSEC-SERVER->/var/log/secure		Aug 8 16:3

OSSEC 坑

- 目录大小
- 端口连接数量

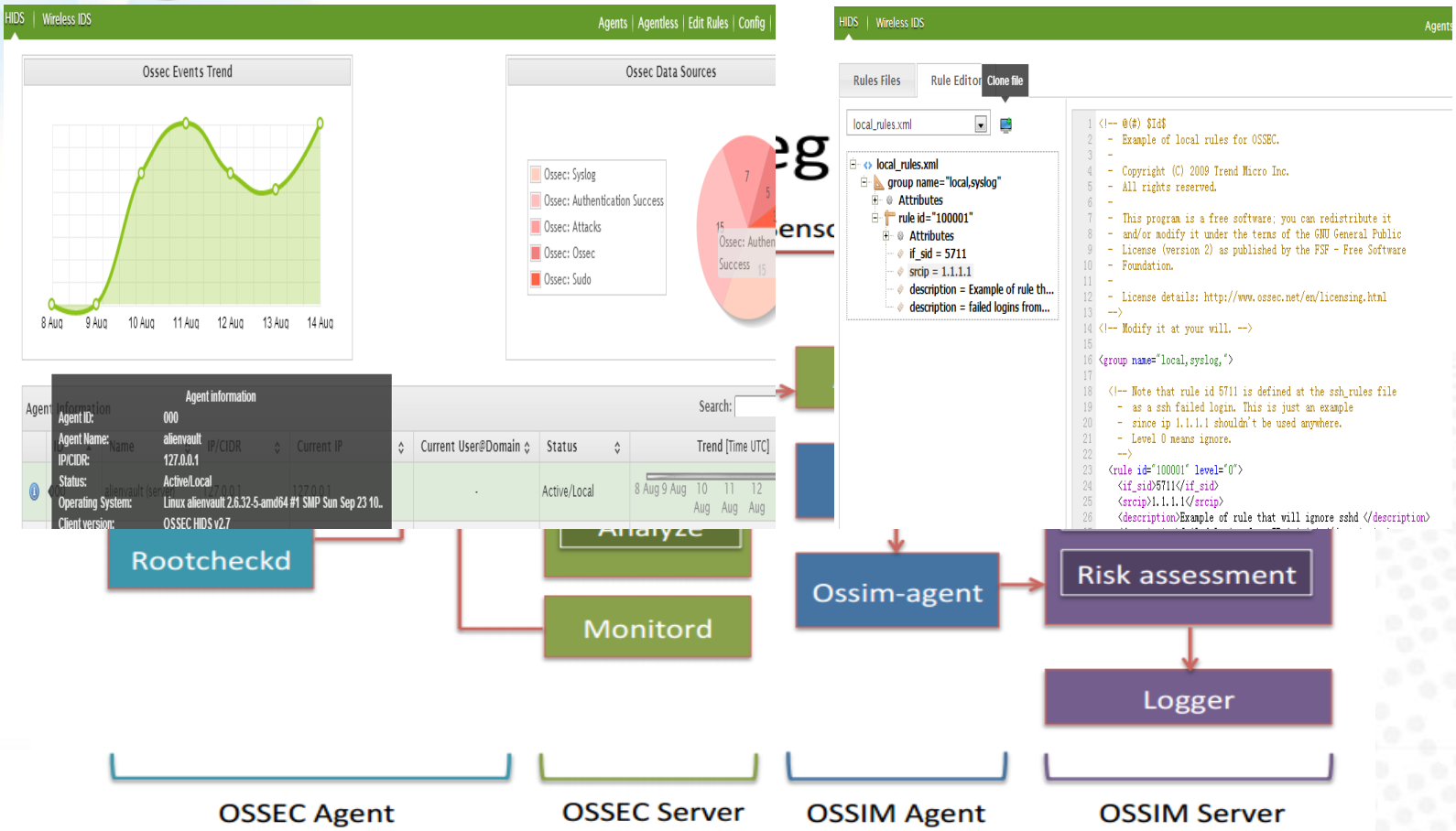
填坑

```
*/5 * * * * /var/ossec/safe_check.sh > /dev/null 2>&1
```

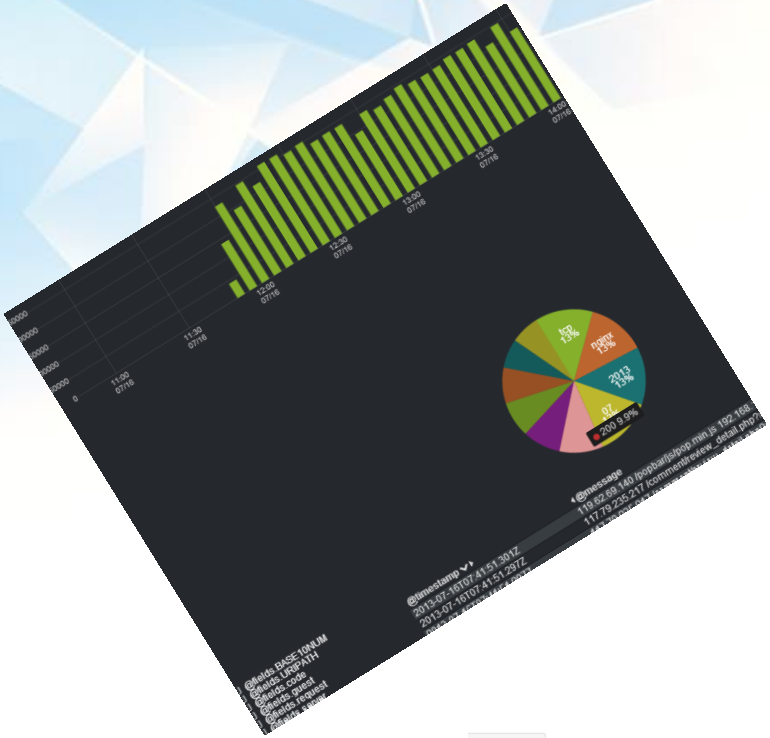
Agent_ID	IP地址		计算机名	文件Hash/最后修改时间(Windows)	连接时间	更新时间	目录大小	操作系统
0		8.31	JOB23831	no agent.conf [windows]	2013-08-08 14:37:41	2013-08-19 17:06:59	2M D:\\ossec\\ossec-agent\\	windows 2003
3			ossec-hids-agent	fd24b0fb97d89943f413c8cf5ffad3b0	2013-08-08 17:54:37	2013-08-19 17:04:58	4.8M /var/ossec/	Linux
6			localhost.localdomain	fd24b0fb97d89943f413c8cf5ffad3b0	2013-08-16 14:24:57	2013-08-19 17:04:57	2.8M /var/ossec/	Linux
8		192	readbo224192	no agent.conf	2013-08-08 17:54:49	2013-08-19 17:04:52	3.0M /var/ossec/	Linux
20		7.39	commu19239	no agent.conf	2013-08-08 16:36:08	2013-08-19 08:58:53	40M /ossec/	Linux
21		7.72	comm19272	no agent.conf	2013-08-08 16:36:09	2013-08-19 08:58:53	46M /ossec/	Linux

OSSEC SPLUNK

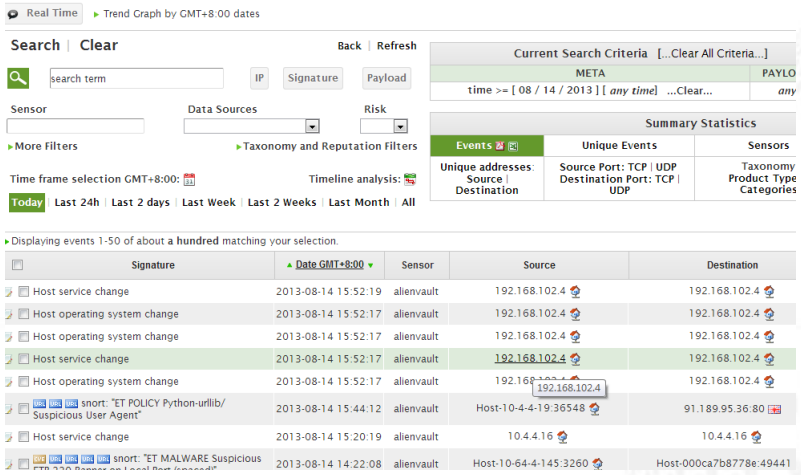
OSSEC OSSIM


HIDS | Wireless IDS
Agents | Agentless | Edit Rules | Config
Ossec Events Trend
8 Aug 9 Aug 10 Aug 11 Aug 12 Aug 13 Aug 14 Aug
Ossec Data Sources
Ossec: Syslog
Ossec: Authentication Success
Ossec: Attacks
Ossec: Ossec
Ossec: Sudo
Agent information
Agent ID: 000
Agent Name: alienvault
IP/CIDR: 127.0.0.1
Status: Active/Local
Operating System: Linux alienvault 2.6.32-5-amd64 #1 SMP Sun Sep 23 10..
Client version: OSSEC HIDS v2.7
Search:
Current IP
Current User@Domain
Status
Trend [Time UTC]
Active/Local
HIDS | Wireless IDS
Rules Files
Rule Editor
Clone file
local_rules.xml
local_rules.xml
group name="local,syslog"
Attributes
rule id="100001"
Attributes
if_sid = 5711
srcip = 1.1.1.1
description = Example of rule th...
description = failed logins from...
<!-- @(#) Id
- Example of local rules for OSSEC.
-
- Copyright (C) 2009 Trend Micro Inc.
- All rights reserved.
-
- This program is a free software; you can redistribute it
- and/or modify it under the terms of the GNU General Public
- License (version 2) as published by the FSF - Free Software
- Foundation.
-
- License details: http://www.ossec.net/en/licensing.html
-->
<!-- Modify it at your will. -->
<group name="local,syslog,">
<!-- Note that rule id 5711 is defined at the ssh_rules file
- as a ssh failed login. This is just an example
- since ip 1.1.1.1 shouldn't be used anywhere.
- Level 0 means ignore.
-->
<rule id="100001" level="0">
<if_sid>5711</if_sid>
<srcip>1.1.1.1</srcip>
<description>Example of rule that will ignore sshd </description>
Rootcheckd
Monitord
Ossim-agent
Risk assessment
Logger
OSSEC Agent
OSSEC Server
OSSIM Agent
OSSIM Server

安全“杯具”


@timestamp
@message
@fields.BASE10NUM
@fields.URIPATH
@fields.code
@fields.geoip
@fields.request
@fields.verb


特征
显示警告 1-14
[snort] SURICATA STREAM 3way handshake wrong seq wrong ack
[snort] ET POLICY Http Client Body contains passwd= in cleartext
[snort] SURICATA STREAM ESTABLISHED retransmission packet before last ack
[snort] SURICATA STREAM TIMEWAIT ACK with wrong seq
[snort] SURICATA HTTP response field missing colon
[url] [url] [snort] ET SCAN Non-Allowed Host Tried to Connect to MySQL Server
[snort] SURICATA STREAM 3way handshake with ack in wrong dir
[url] [snort] ET POLICY curl User-Agent Outbound
[snort] SURICATA STREAM Packet with invalid ack
[url] [snort] ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
[snort] SURICATA STREAM ESTABLISHED invalid ack
[url] [snort] ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package management
[snort] SURICATA STREAM ESTABLISHED packet out of window
[url] [snort] ET POLICY Python-urllib/ Suspicious User Agent
[snort] SURICATA STREAM ESTABLISHED packet out of window
动作


Real Time
Trend Graph by GMT+8:00 dates
Search | Clear
Back | Refresh
search term
IP
Signature
Payload
Sensor
Data Sources
Risk
More Filters
Taxonomy and Reputation Filters
Time frame selection GMT+8:00:
Timeline analysis:
Today | Last 24h | Last 2 days | Last Week | Last 2 Weeks | Last Month | All
Current Search Criteria [...Clear All Criteria...]
META
time >= [08 / 14 / 2013] [any time] ...Clear...
Summary Statistics
Events
Unique Events
Sensors
Unique addresses: Source | Destination
Source Port: TCP | UDP
Destination Port: TCP | UDP
Taxonomy Product Type Categories
Displaying events 1-50 of about a hundred matching your selection.
Signature
Date GMT+8:00
Sensor
Source
Destination
Host service change 2013-08-14 15:52:19 alienvault 192.168.102.4 192.168.102.4
Host operating system change 2013-08-14 15:52:17 alienvault 192.168.102.4 192.168.102.4
Host operating system change 2013-08-14 15:52:17 alienvault 192.168.102.4 192.168.102.4
Host service change 2013-08-14 15:52:17 alienvault 192.168.102.4 192.168.102.4
Host operating system change 2013-08-14 15:52:17 alienvault 192.168.102.4 192.168.102.4
snort: "ET POLICY Python-urllib/ Suspicious User Agent" 2013-08-14 15:44:12 alienvault Host-10-4-4-19:36548 91.189.95.36:80
Host service change 2013-08-14 15:20:19 alienvault 10.4.4.16 10.4.4.16
snort: "ET MALWARE Suspicious 2013-08-14 14:22:08 alienvault Host-10-64-4-145:3260 Host-000ca7b8778e:49441

Thanks!


SequeMedia
盛拓传媒
IT168.com
www.it168.com
ChinaUnix.net
ITPUB