DBAPPSecurity 安恒信息

WEB应用安全和数据库安全的领航者


# 基于云计算的大数据分析

演讲者：刘志乐

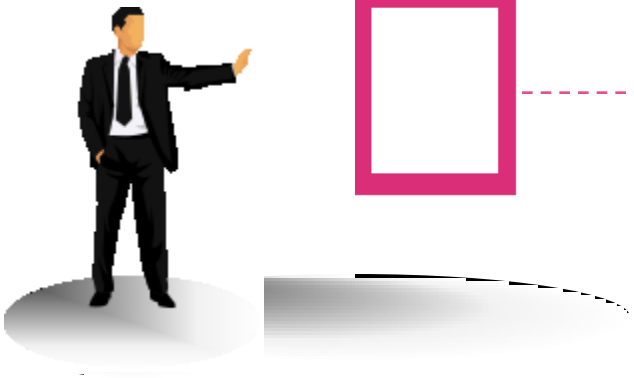
www.dbappsecurity.com.cn


杭州安恒信息技术有限公司
副总裁

- OWASP中国区委员
- OWASP中国杭州分会区域负责人
- 2011年中国计算机网络安全年会演讲嘉宾
- 2011年OWASP亚洲峰会演讲嘉宾
- 2011年ISF上海演讲嘉宾
- 2012年第四届中国云计算大会演讲嘉宾
- 2012年计算机网络安全年会演讲嘉宾
- 2012年OWASP AppSec Asia悉尼峰会演讲嘉宾
- 2013年第二届等级保护技术大会演讲嘉宾
- 2013年中国互联网安全大会演讲嘉宾
- 2014通信行业网络安全年会演讲嘉宾

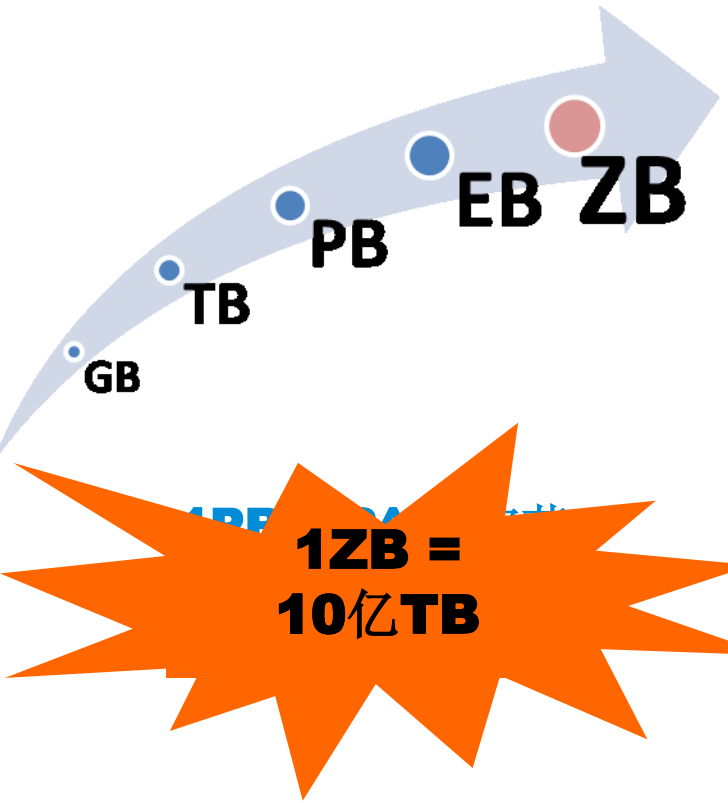
# 内容提要

1. 传统安全分析的困境
2. 基于云计算的分析构架
3. 基于大数据的分析方法

# 1 传统安全分析的困境

# 大数据的爆炸性增长




## 地球上至今总共的数据量：

- 2006年，个人用户刚迈进TB时代，全球就有约180EB的数据 ；
- 2012年，达到了1.8ZB；
- 2020年，预测将达到35.2ZB ！

**数据总量将会增长44倍**

# 近年攻击事件频发

当前位置：WooYun >> 搜索结果

搜索关键字： struts (共 1767 条记录) 将未公开漏洞纳入搜索结果

中国铁道科学研究院某系统命令执行（可内网）

每天撸一发，坚持 中国铁道科学研究院某系统命令执行...struts2命令执行 地址： http://tdm.rails.com.cn/login/logi

，192.168.200.42等等 ...服务器信息 内网信息 ...蛋疼的struts2，还是别用了吧

提交日期：2014-05-05 作者：Mody

方正宽带ICP备案管理系统拒绝服务攻击漏洞

...http://59.108.229.254:8088/user/gotoLoginPage.action ...Struts到新版本，开启相应IDS、IPS防护吧。

提交日期：2014-04-25 作者：神奇=路人甲

蒙特某分站命令执行漏洞导致内网渗透

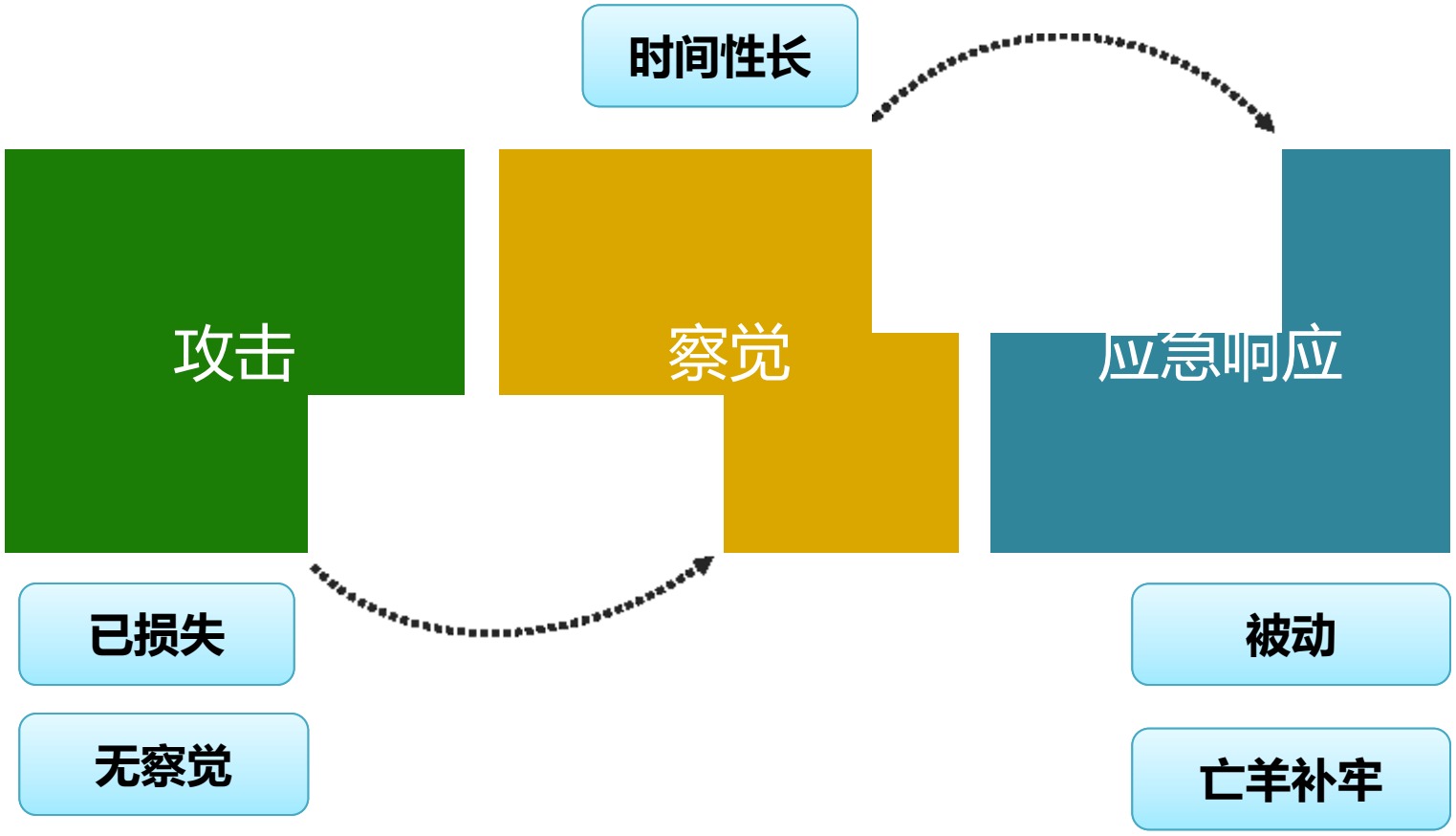
关注蒙特安全~...http://zjec.mountor.cn/ http://zjec.mount...Struts漏洞，直接上传马，system权限。 内网，可以继

.cn/license!getExpireDateOfDays.action Struts漏洞，直接上传马，system权限。 内网，可以继续渗透。 成功连

提交日期：2014-04-06 作者：Summer

从蹭网到爱普宽带核心系统沦陷

# 传统的应急响应



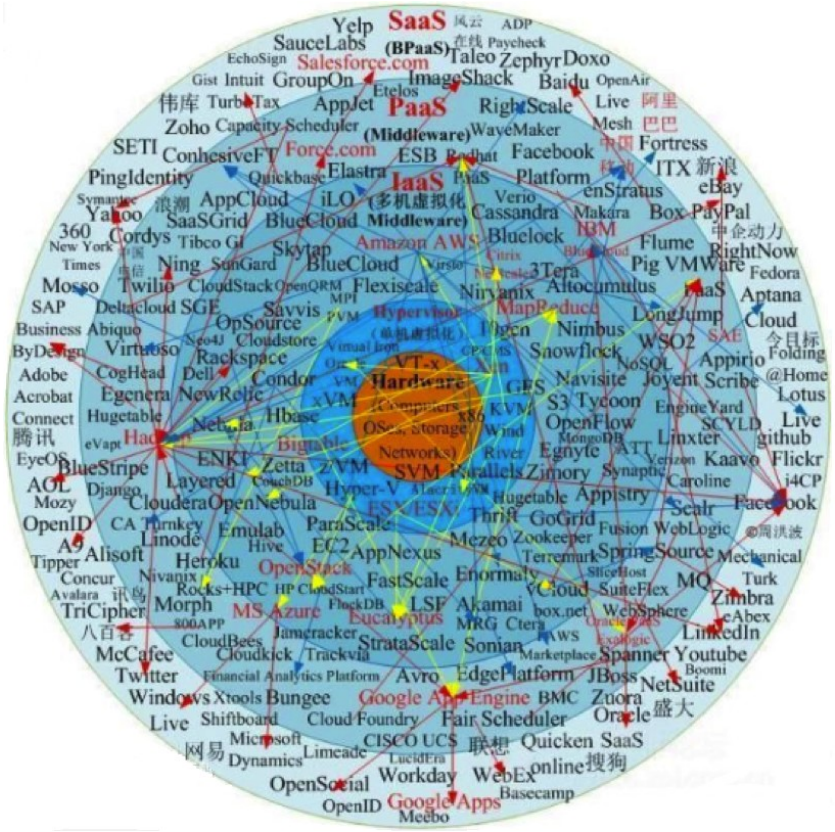
# Question


网站存在安全漏洞 — 如何及早发现网站安全漏洞？

内网被APT攻击 — 如何找出攻击来源、被入侵目标？
如何消除植入的木马及可疑程序？

突发的入侵事件 — 如何及时发现被入侵的目标，进行补救？

无有效的安全监管手段 — 如何利用现有资源产生最大价值？

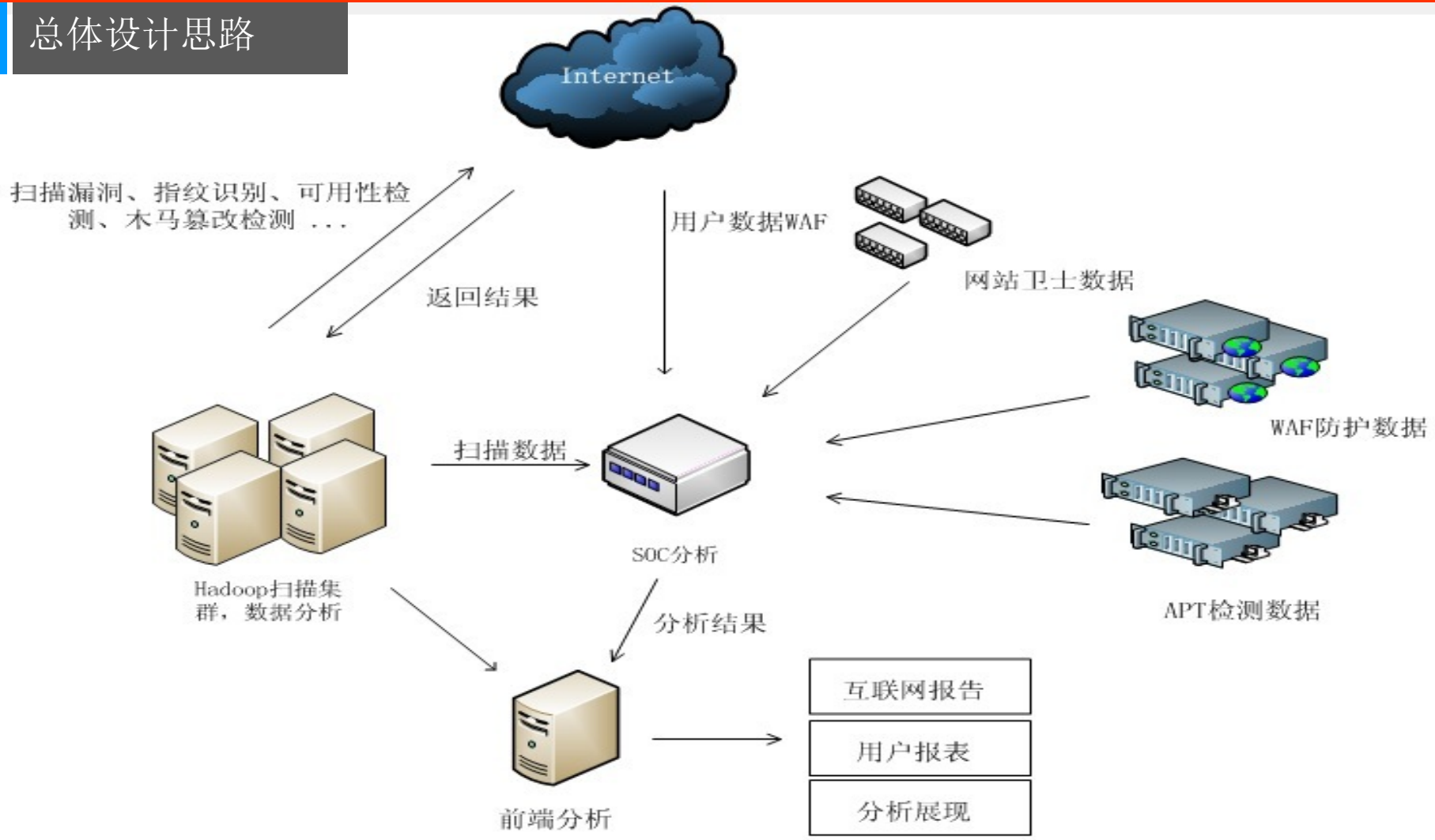



# 云计算
# 大数据
# ？
# 更先进的安全管理

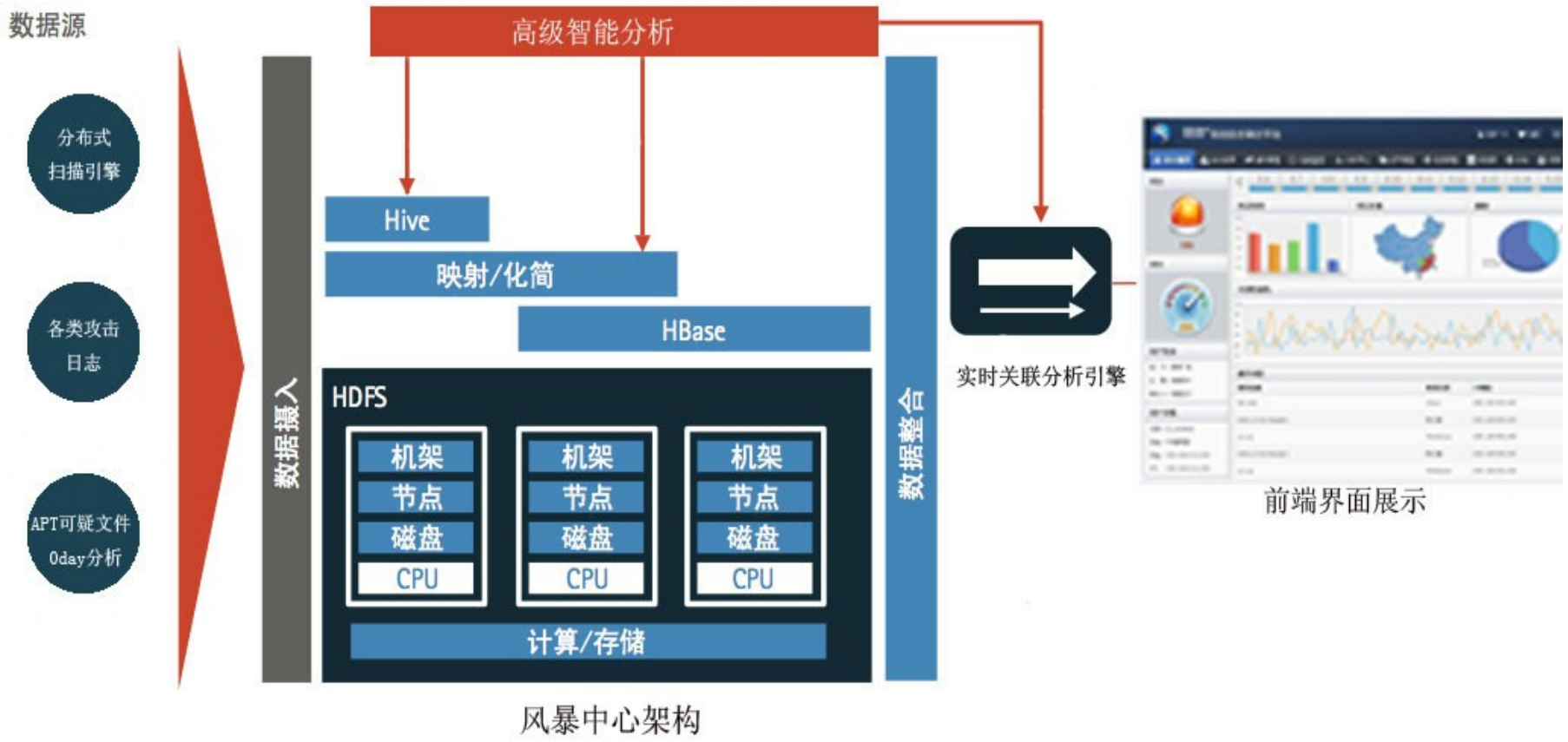
# 2 基于云计算的分析构架

# 基于云计算的大数据安全分析

## 总体设计思路



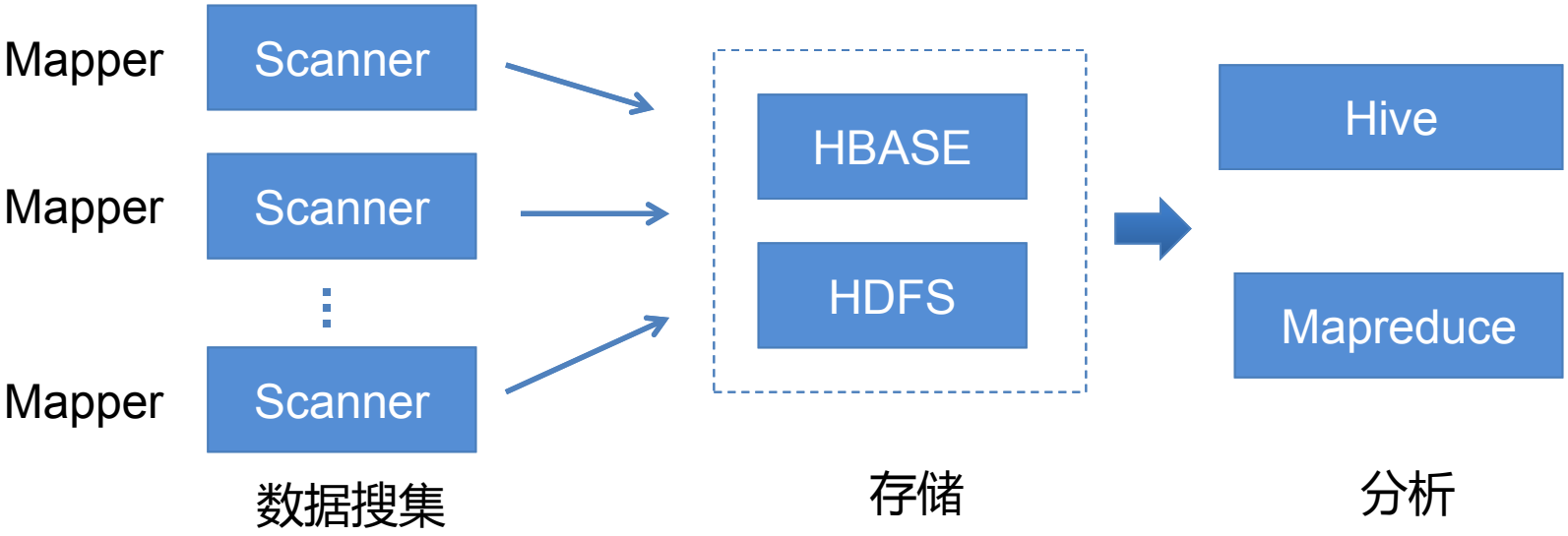
# 云计算架构




风暴中心架构

# 分布式扫描引擎

- 基于 Hadoop 的分布式扫描引擎
- 通过 Mapreduce 分解任务
- 每天产生超过20G的有效数据



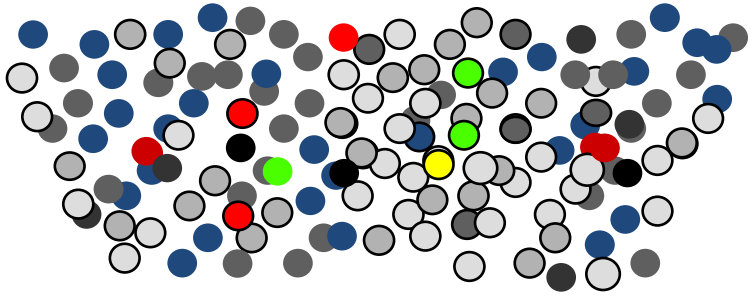
# WEB漏洞获取

# 攻击日志收集


支付业务会话
业务会话层
SNMP
Syslog
文件
流量镜像
应用层
SNMP
Syslog
文件
Agent
支付应用服务器
安全应用前置机
HTTP
网络层
SNMP
Syslog
OPSec
负载均衡
支付请求
数据链路层
SNMP
Syslog
xFlow
网络交换机

# 攻击日志收集

日志数据




过滤*

归并*

标准化

SmartSensor

带宽管理

集中更新

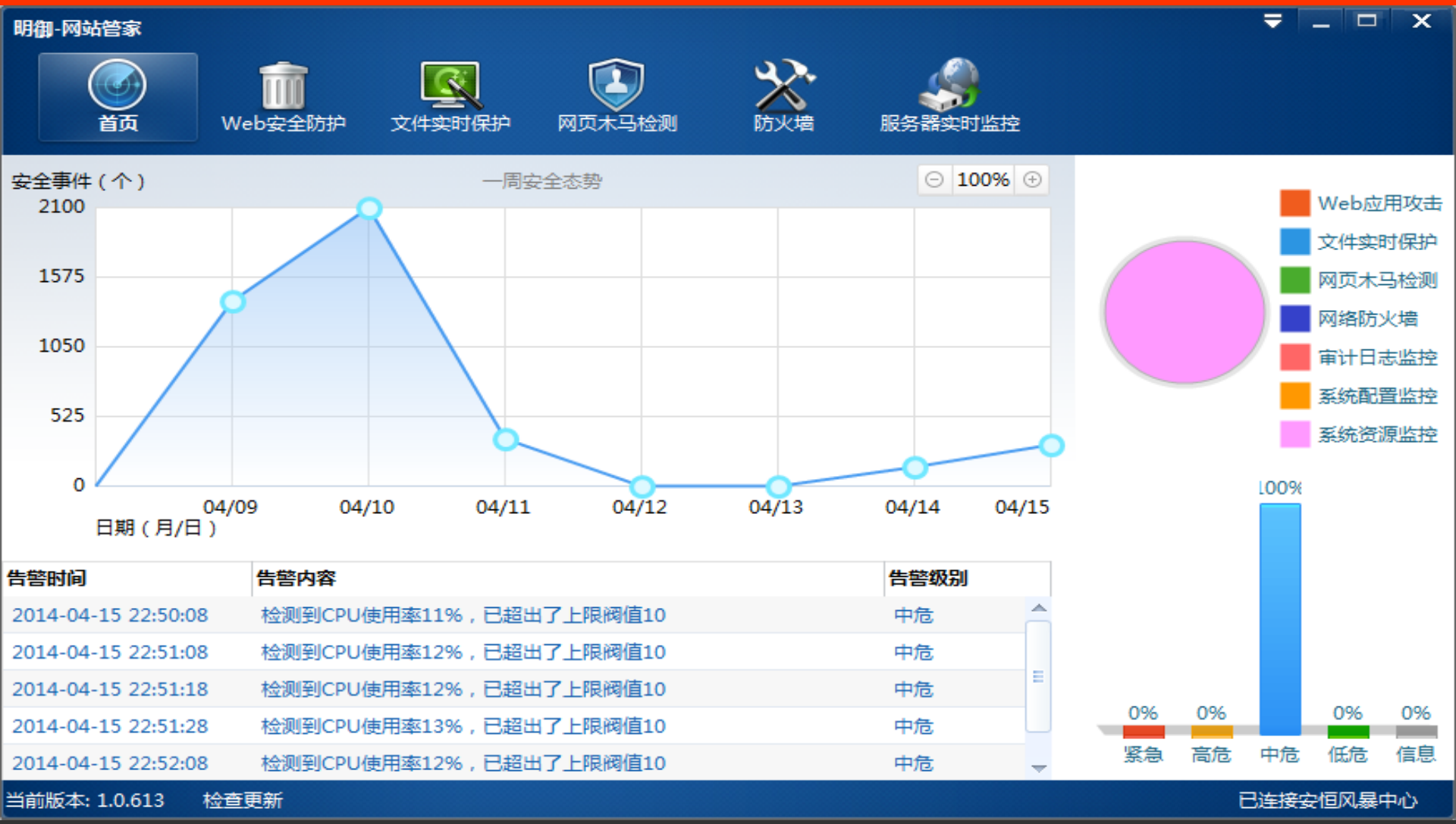
SSL

经过压缩的
日志数据


云端分析

*符合NIST 800-92日志归并要求

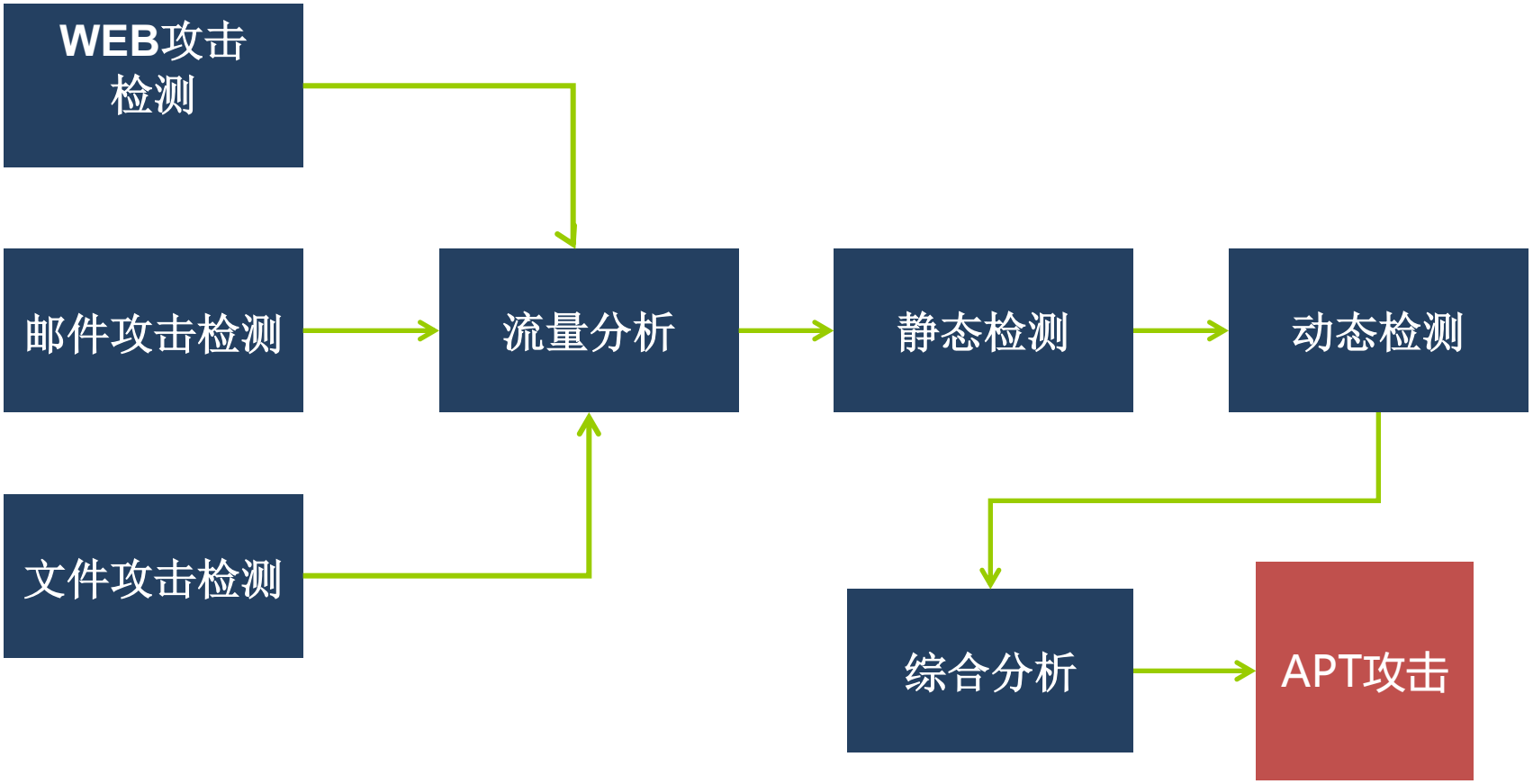
# 客户端防护日志收集

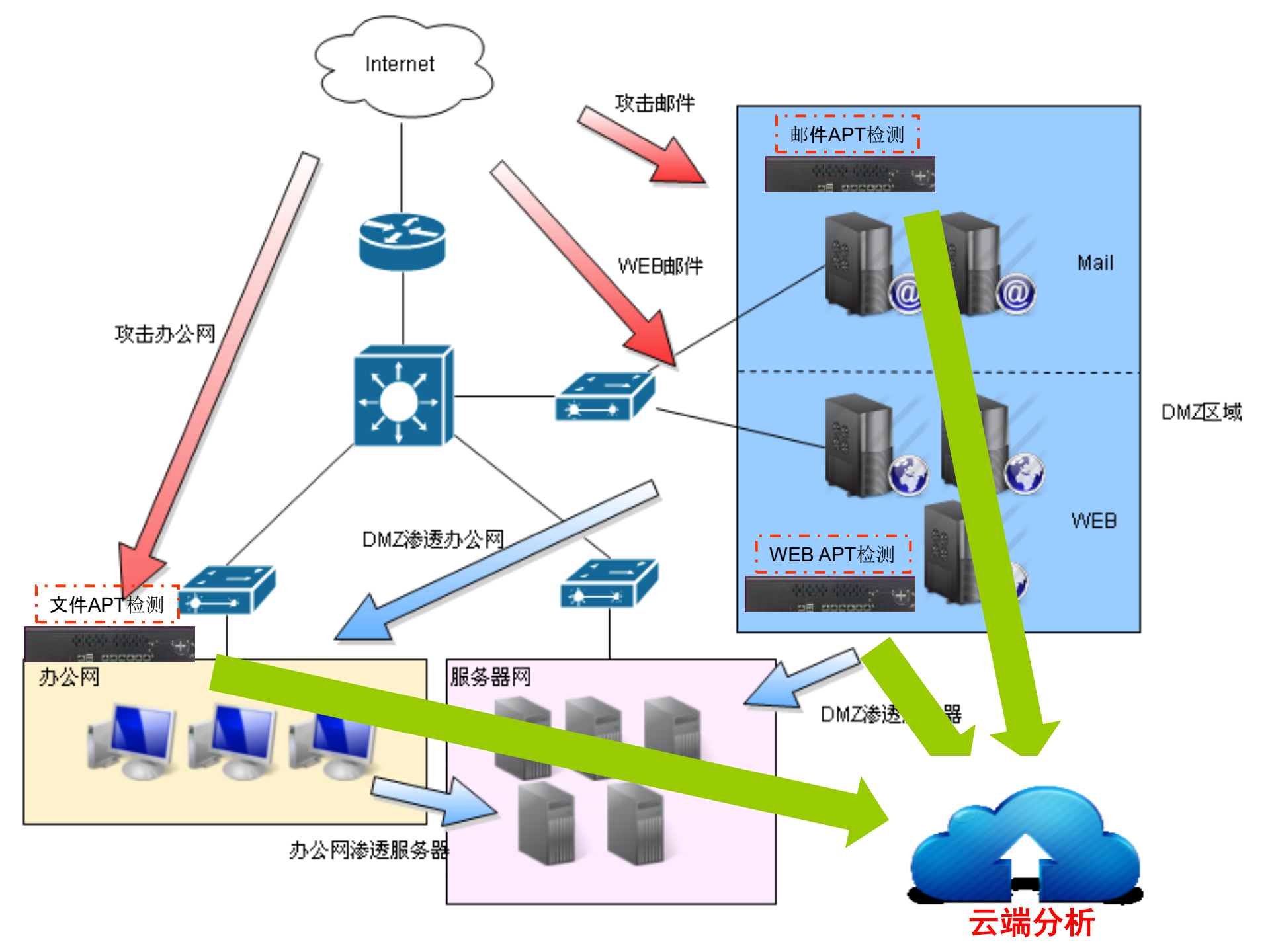

明御-网站管家
首页
Web安全防护
文件实时保护
网页木马检测
防火墙
服务器实时监控
安全事件（个）
一周安全态势
100%
2100
1575
1050
525
0
04/09
04/10
04/11
04/12
04/13
04/14
04/15
日期（月/日）
Web应用攻击
文件实时保护
网页木马检测
网络防火墙
审计日志监控
系统配置监控
系统资源监控
100%
0%
0%
0%
0%
紧急
高危
中危
低危
信息
告警时间
告警内容
告警级别
2014-04-15 22:50:08
检测到CPU使用率11%，已超出了上限阀值10
中危
2014-04-15 22:51:08
检测到CPU使用率12%，已超出了上限阀值10
中危
2014-04-15 22:51:18
检测到CPU使用率12%，已超出了上限阀值10
中危
2014-04-15 22:51:28
检测到CPU使用率13%，已超出了上限阀值10
中危
2014-04-15 22:52:08
检测到CPU使用率12%，已超出了上限阀值10
中危
当前版本: 1.0.613
检查更新
已连接安恒风暴中心

# 风暴中心WAF数据


明御WEB应用防火墙
状态
日志
报表
策略
配置
系统
WEB APPLICATION FIREWALL
应用防护日志
网络防护日志
访问审计
防篡改日志
误判分析
操作日志
系统日志
升级日志
应用防护日志
自定义查询
安恒风暴中心
设置告警显示
导出
动作
安恒风暴中心
说明
WAF可以加密连接到安恒风暴中心，对日志进行实时分析并提供安全预警。
状态
启用
客户ID
DAS_WAF_DEMO
远程服务器
183.129.152.138:65480
确定
取消
缺失报头
192.168.10.118
2014-04-14 10:06:32
告警

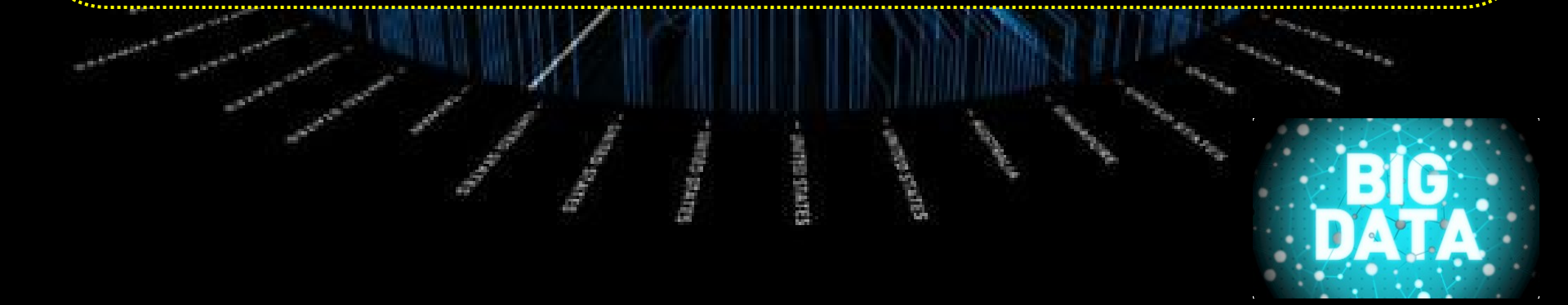
# APT攻击收集




Internet
攻击邮件
邮件APT检测
Mail
WEB邮件
攻击办公网
DMZ区域
DMZ渗透办公网
WEB
WEB APT检测
文件APT检测
办公网
服务器网
DMZ渗透
办公网渗透服务器
云端分析

# 大数据分析平台

- 对搜集海量数据进行综合分析
  - 使用 **Hadoop** 集群
  - 原始数据 **MapReduce** 任务分析
  - Hbase数据使用**hive + Mapreduce**进行分析



# 大数据分析平台

DBAPP Security 安恒信息

## 分析的方式

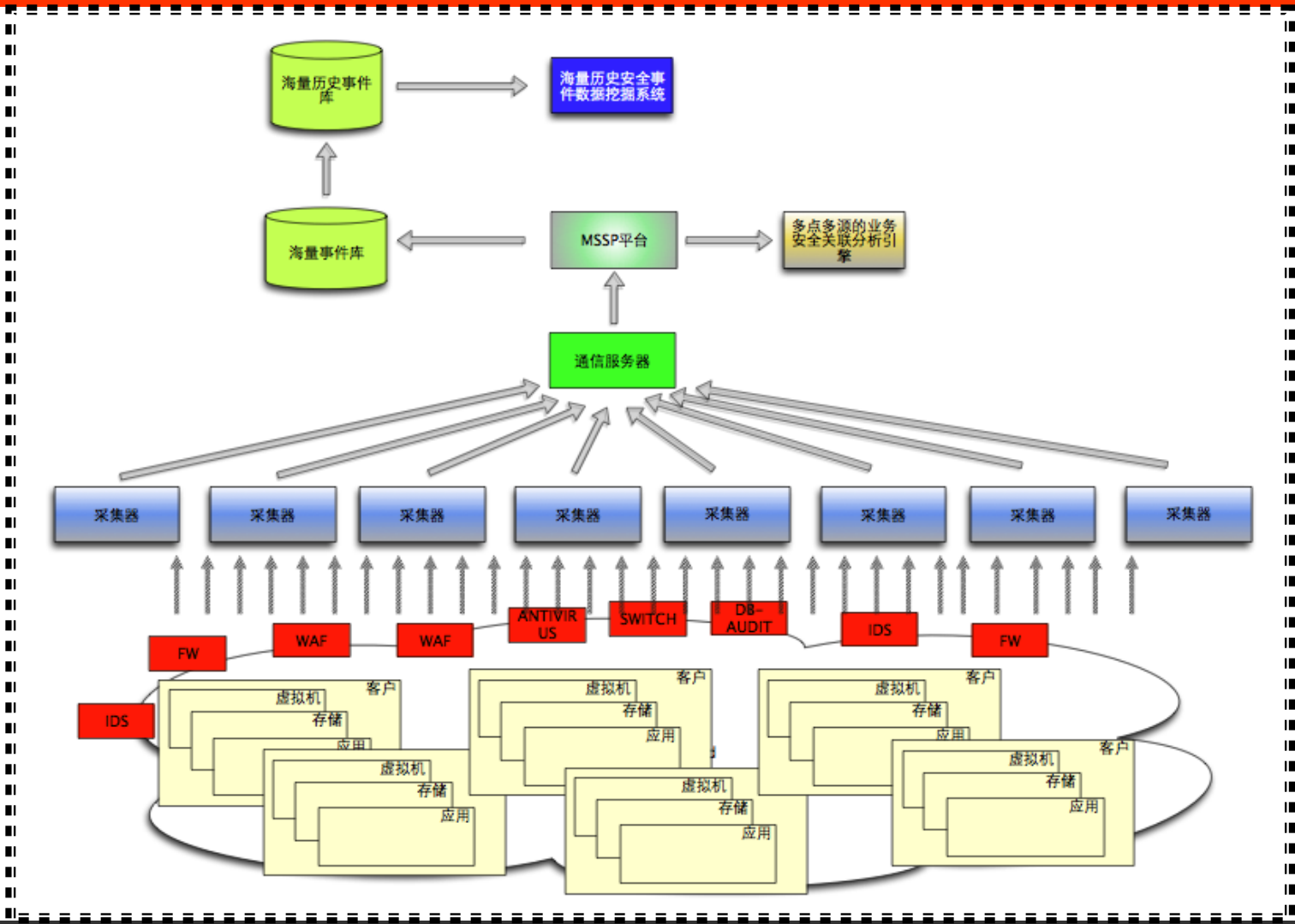
- 简单的统计类
  - 使用 **hive** 进行统计分析
- 综合关联类
  - **Mapreduce** 任务处理
  - 多任务分步处理

# 3 基于大数据的分析方法

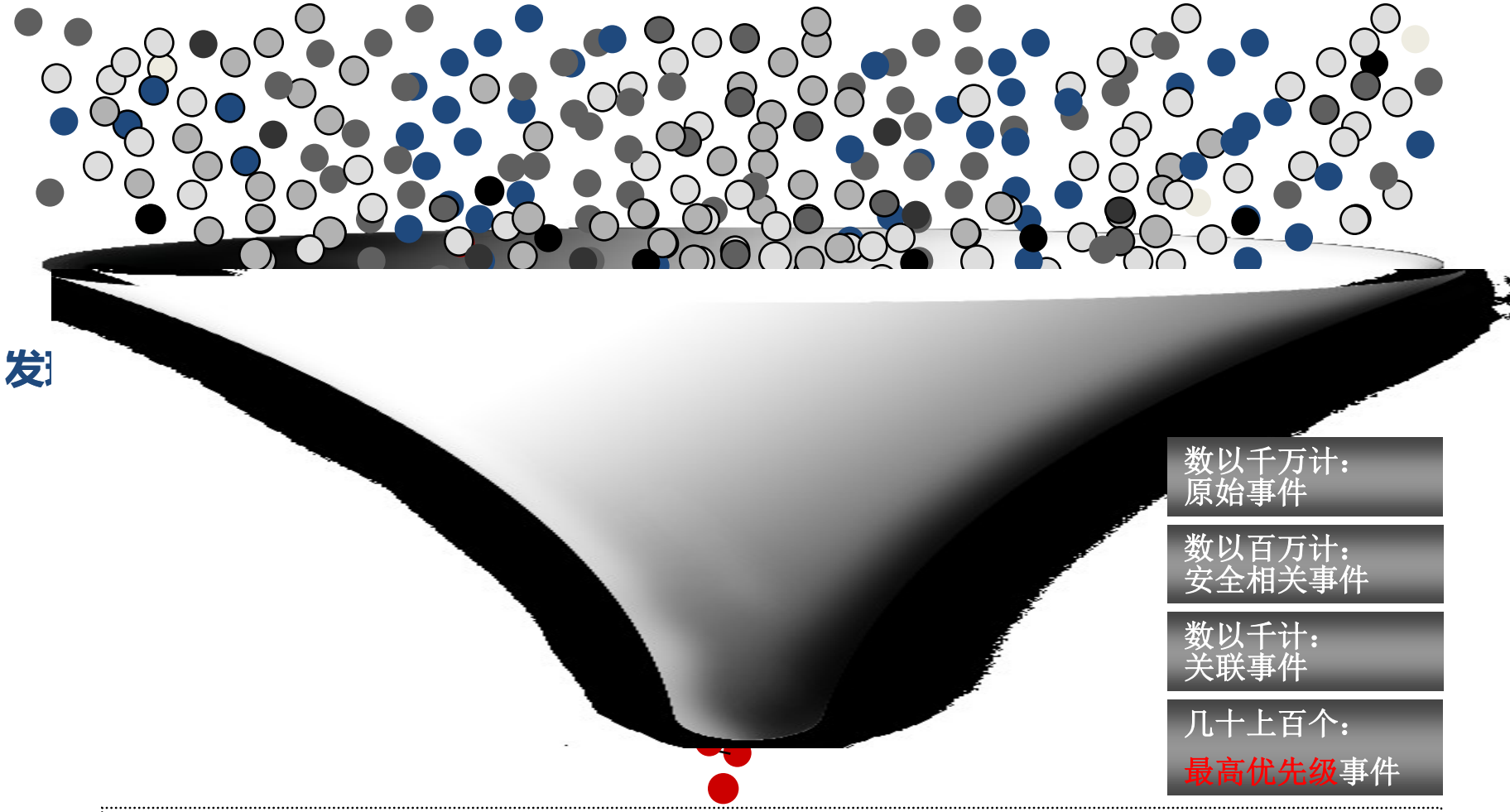
# 大数据安全分析


- 分析异构环境风险
- 多点多源业务安全关联分析
- 海量历史安全信息数据挖掘

# 综合海量数据分析


海量历史事件库
海量历史安全事件数据挖掘系统
海量事件库
MSSP平台
多点多源的业务安全关联分析引擎
通信服务器
采集器
采集器
采集器
采集器
采集器
采集器
采集器
采集器
FW
WAF
WAF
ANTIVIRUS
SWITCH
DB-AUDIT
IDS
FW
IDS
客户
虚拟机
存储
应用
虚拟机
存储
应用
客户
虚拟机
存储
应用
虚拟机
存储
应用
客户
虚拟机
存储
应用
虚拟机
存储
应用
客户

# 综合关联分析




警报：用户BadUser123在尝试对WeakServer的密码进行暴力破解

# 安全态势评分

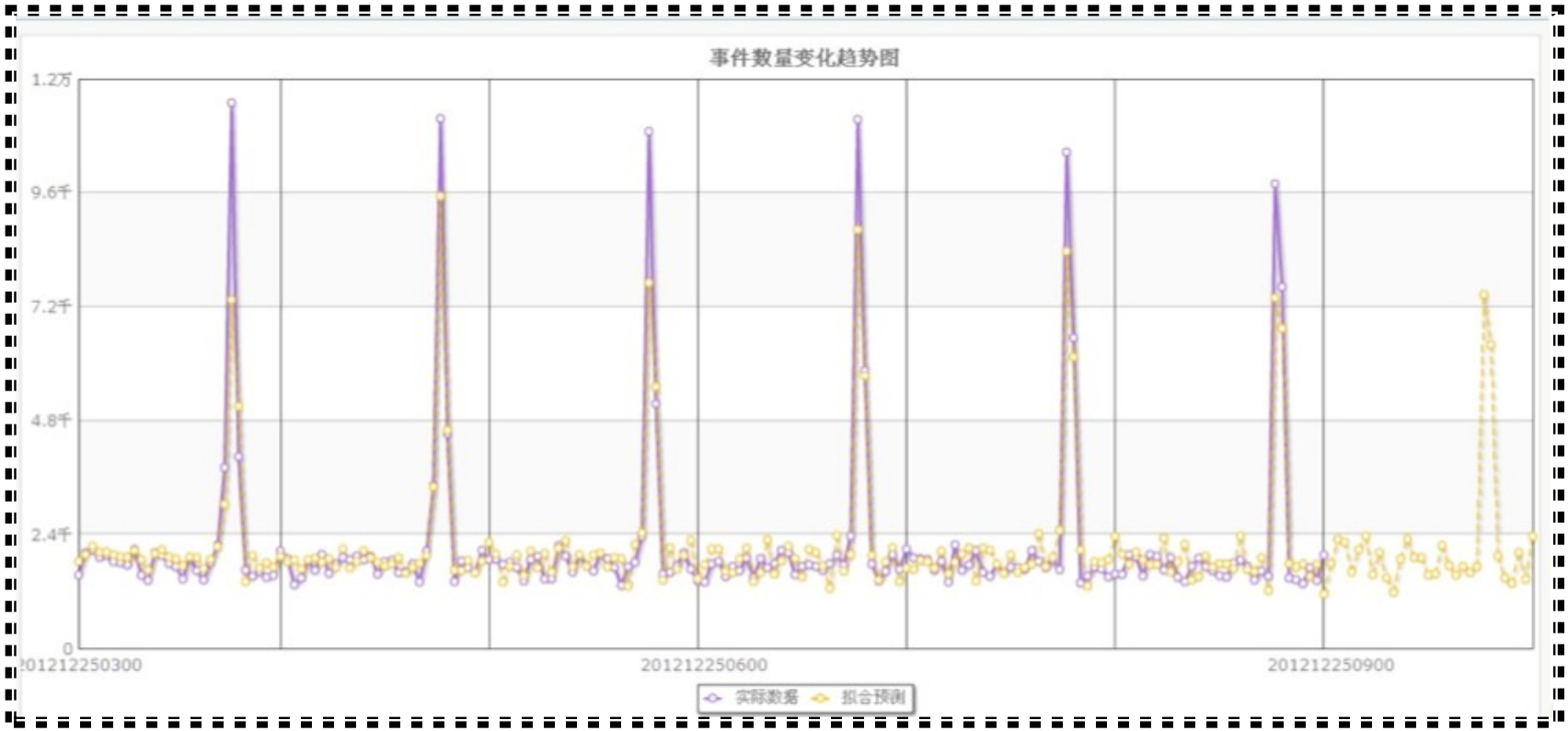

总体评分
100分
历史评分
100
75
50
25
0
01-01
01-06
12-11
12-16
12-21
12-26
12-31
设备故障
100
认证登录
100
攻击威胁
100
应用可用性
100
数据访问
100
系统脆弱性
100
资产 (1)

# 大数据时序趋势预测 - 算法

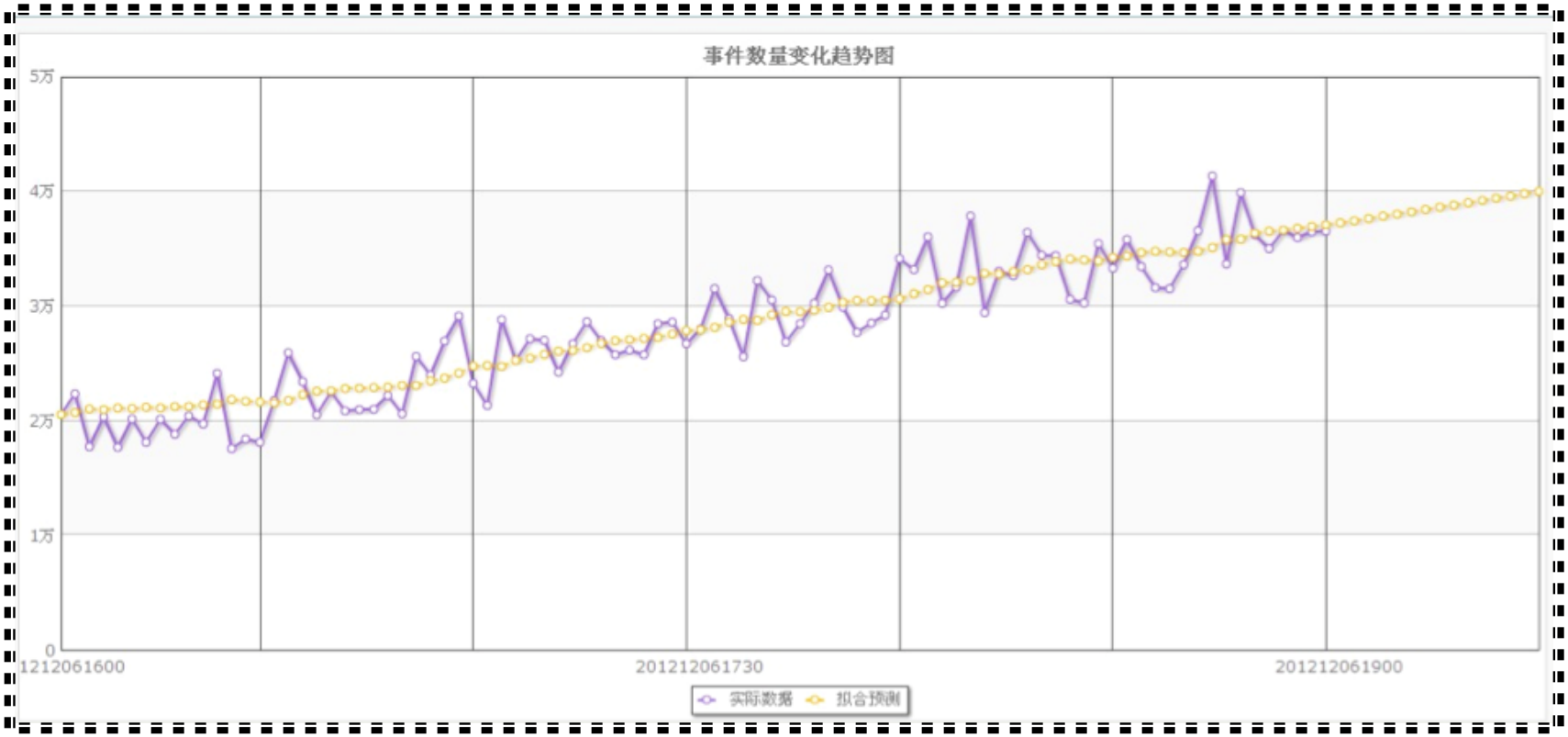
DBAPP Security 安恒信息

## 可利用算法

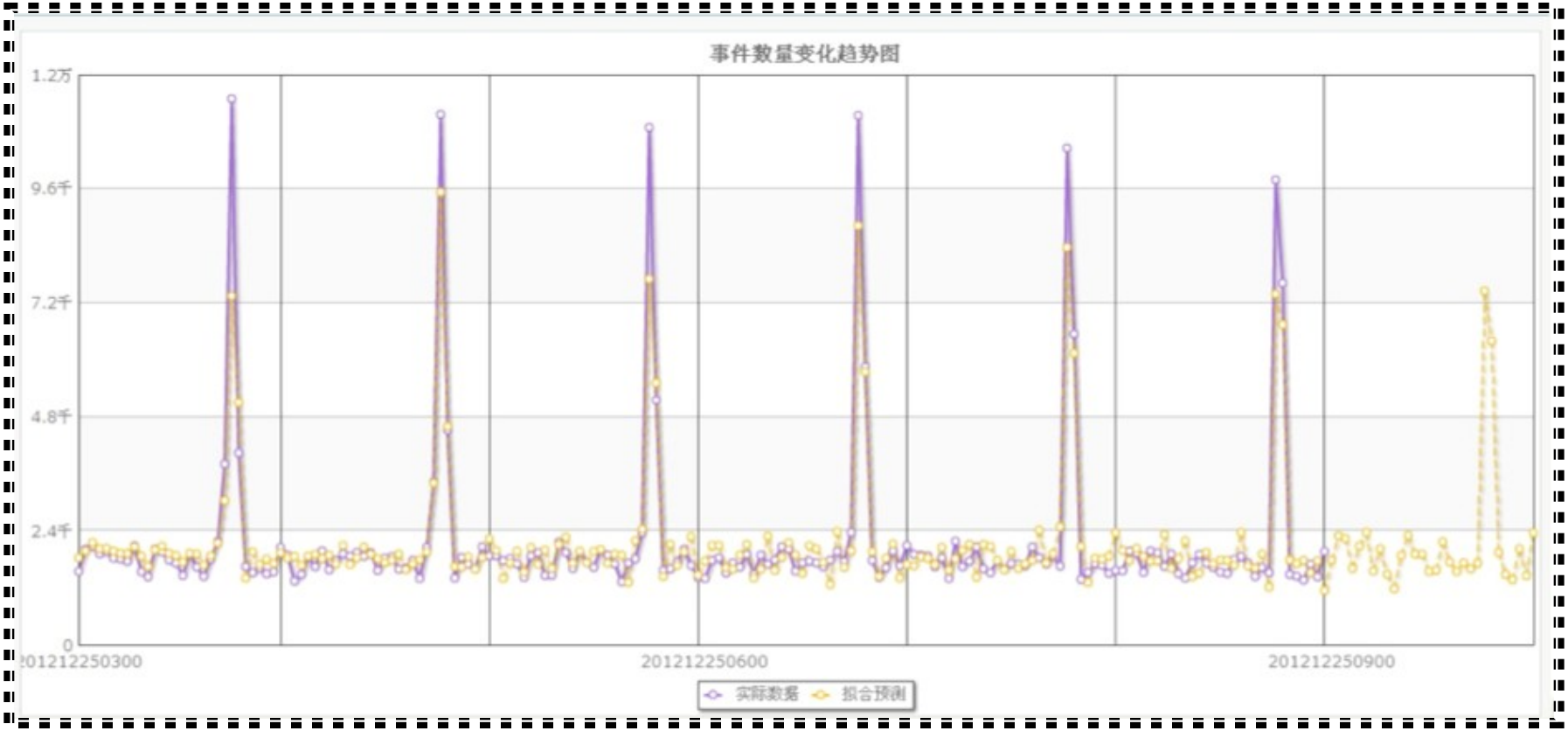
# 趋势预测 - 周期性


事件数量变化趋势图
1.2万
9.6千
7.2千
4.8千
2.4千
0
201212250300
201212250600
201212250900
实际数据
拟合预测

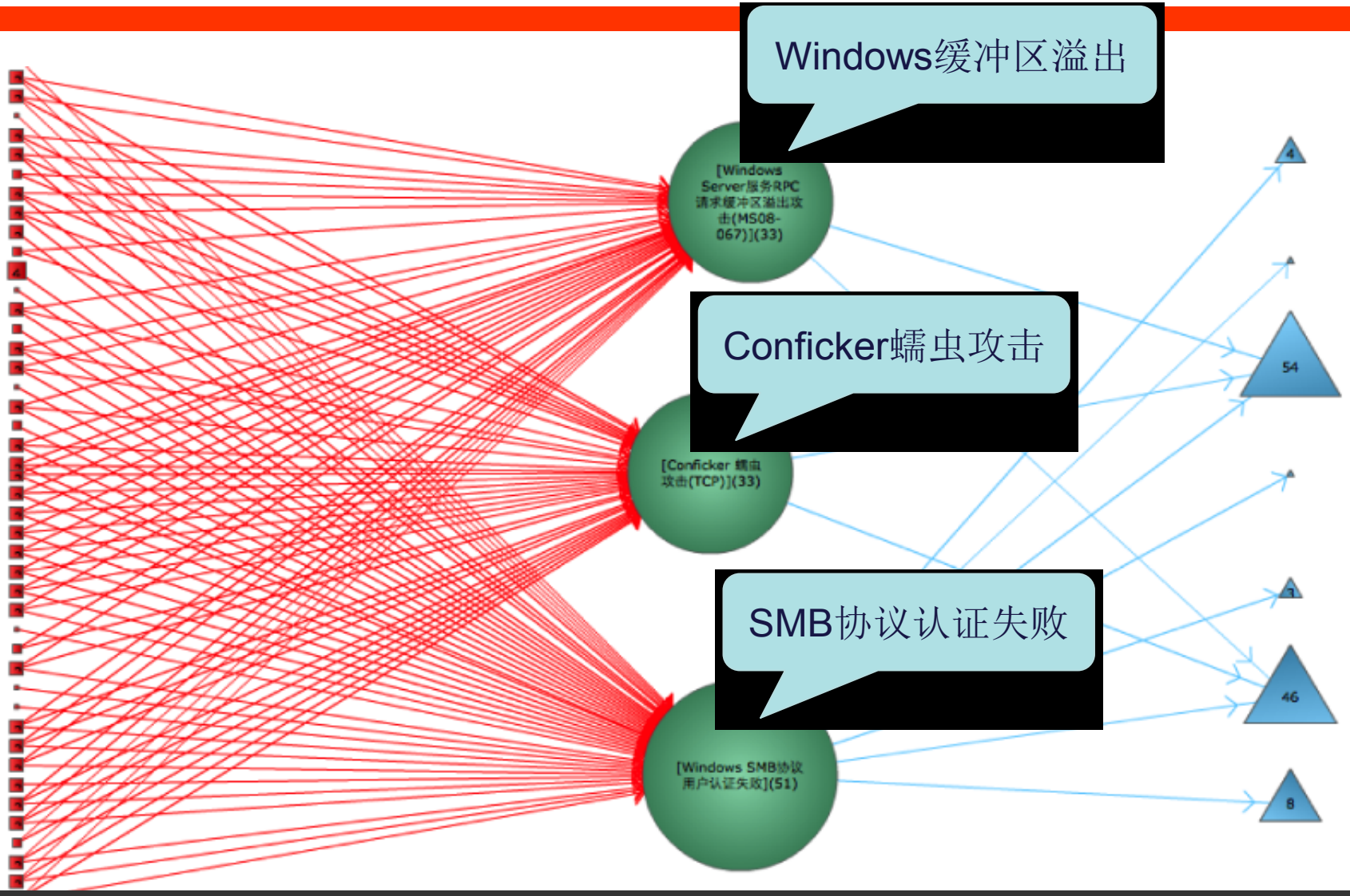
# 趋势预测 - 趋势


事件数量变化趋势图
5万
4万
3万
2万
1万
0
1212061600
201212061730
201212061900
实际数据
拟合预测

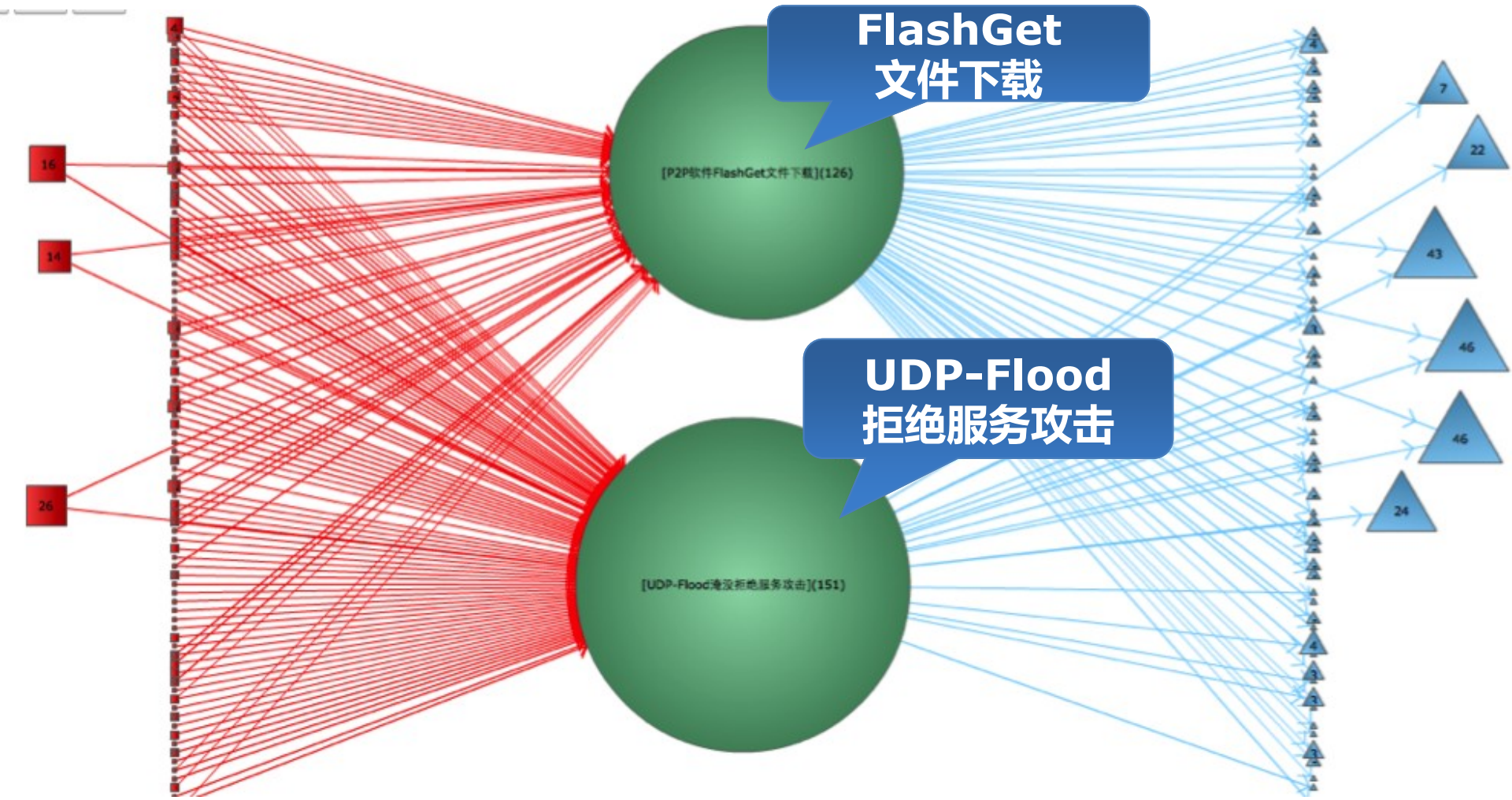
# 综合（周期性、趋势、正态分布）



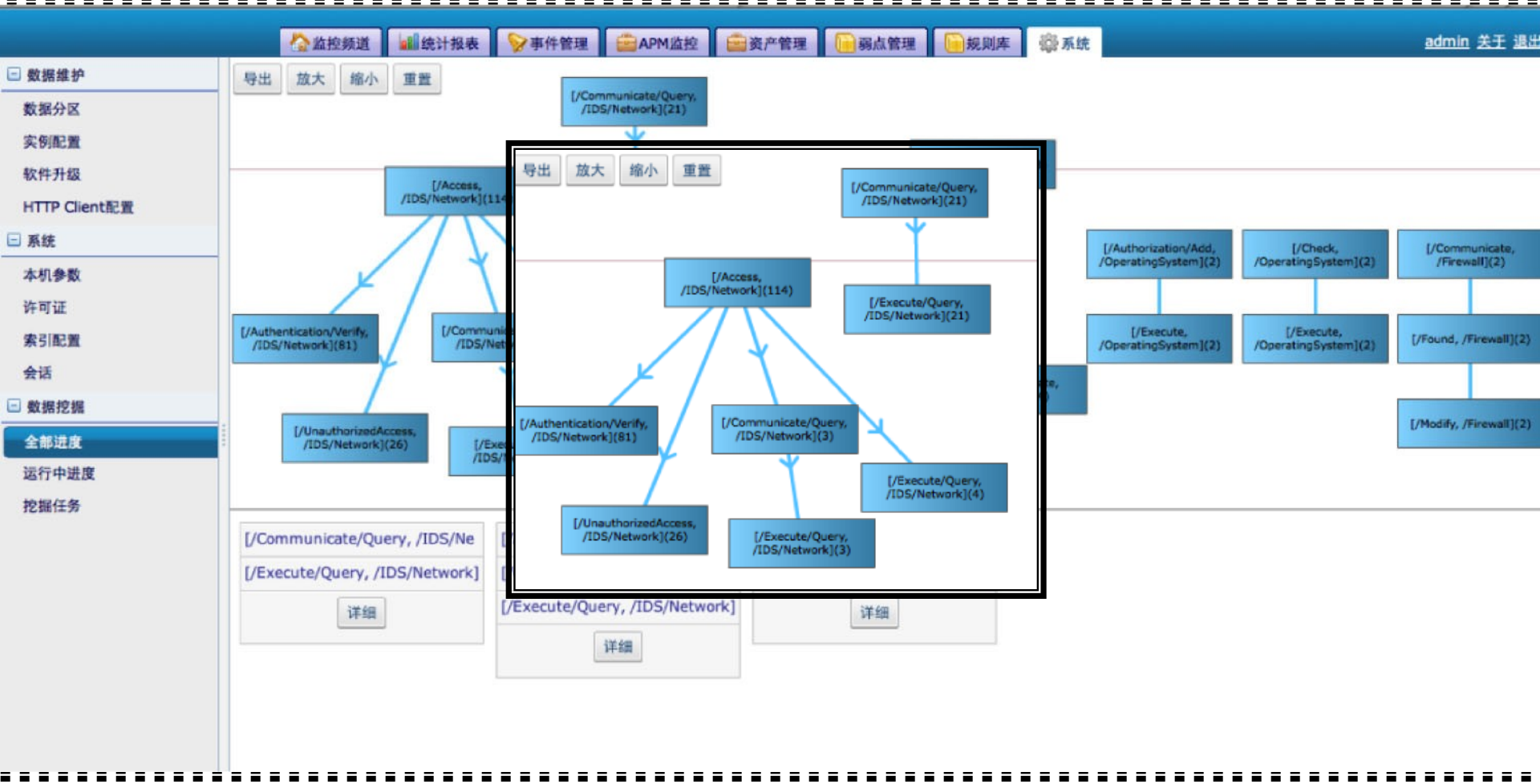
# 大数据挖掘 - 样例1


Windows缓冲区溢出
[Windows Server服务RPC请求缓冲区溢出攻击(MS08-067)](33)
Conficker蠕虫攻击
[Conficker 蠕虫攻击(TCP)](33)
SMB协议认证失败
[Windows SMB协议用户认证失败](51)
4
54
1
46
8

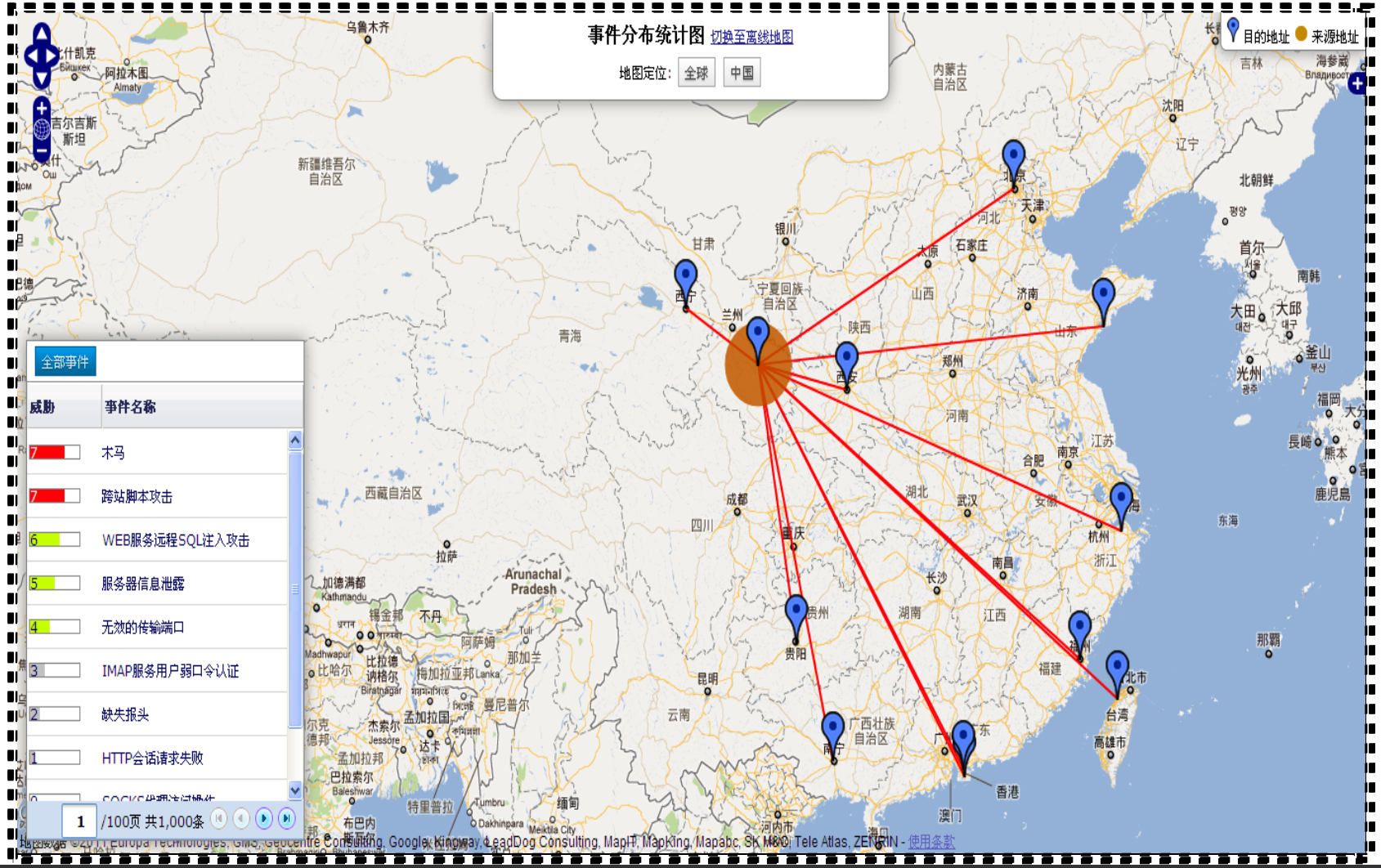
# 数据挖掘-事务分布模式


FlashGet
文件下载
UDP-Flood
拒绝服务攻击
[P2P软件FlashGet文件下载](126)
[UDP-Flood淹没拒绝服务攻击](151)
16
14
26
7
22
43
46
46
24

# 数据挖掘 - 行为模式


监控频道
统计报表
事件管理
APM监控
资产管理
弱点管理
规则库
系统
admin 关于 退出
数据维护
数据分区
实例配置
软件升级
HTTP Client配置
系统
本机参数
许可证
索引配置
会话
数据挖掘
全部进度
运行中进度
挖掘任务
导出
放大
缩小
重置
[/Communicate/Query, /IDS/Network](21)
[/Access, /IDS/Network](114)
[/Authentication/Verify, /IDS/Network](81)
[/UnauthorizedAccess, /IDS/Network](26)
[/Communicate/Query, /IDS/Network](3)
[/Execute/Query, /IDS/Network](21)
[/Execute/Query, /IDS/Network](4)
[/Execute/Query, /IDS/Network](3)
[/Authorization/Add, /OperatingSystem](2)
[/Check, /OperatingSystem](2)
[/Communicate, /Firewall](2)
[/Execute, /OperatingSystem](2)
[/Found, /Firewall](2)
[/Modify, /Firewall](2)
[/Execute/Query, /IDS/Network]
详细

# 攻击分析地图展示


事件分布统计图 切换至离线地图
地图定位: 全球 中国
目的地址 来源地址
全部事件
威胁
事件名称
7 木马
7 跨站脚本攻击
6 WEB服务远程SQL注入攻击
5 服务器信息泄露
4 无效的传输端口
3 IMAP服务用户弱口令认证
2 缺失报头
1 HTTP会话请求失败
1 /100页 共1,000条

# 实时攻击监控


网站监测
扫描网站
62077
发现漏洞
334978
高风险漏洞
中风险漏洞
54993
低风险漏洞
250382
青岛市
漏洞重灾区
唐山市
北京市
长沙市
郑州市
成都市

DBAPPSecurity 安恒信息

WEB应用安全和数据库安全的领航者

# THANK YOU

www.dbappsecurity.com.cn