GOPS2016 Beijing

全球运维大会

2016

DevOps 2.0：重塑运维价值

北京站

会议时间：12月16日 - 12月17日

会议地点：北京国际会议中心

主办单位：高效运维社区 GreatOPS Community　开放运维联盟 OOPSA Open OPS Alliance

YY直播安全运维从“0”到“1”实践

韩方　　运维部安全中心总监

目录

YY Live 主营业务：（直播+游戏）

安全运维使命：为业务保驾护航

安全运维团队需要面对的安全事件

哪些年我们一起救过的“火”

场景一：业务服务器为何每隔5秒连接中断，无法新建连接…

场景二：Nginx fork队列阻塞等待upstream server回包超时…

场景三：运营活动礼物瞬间被“羊毛党”秒杀…

场景四：Struts2/Bash破壳/心脏流血又来一拨0day，升不升级？…

场景五：有IP大量报文流量交换机异常，机器上无可疑进程…

场景六：有台服务器负载异常，有可疑进程，为何杀不掉呢…

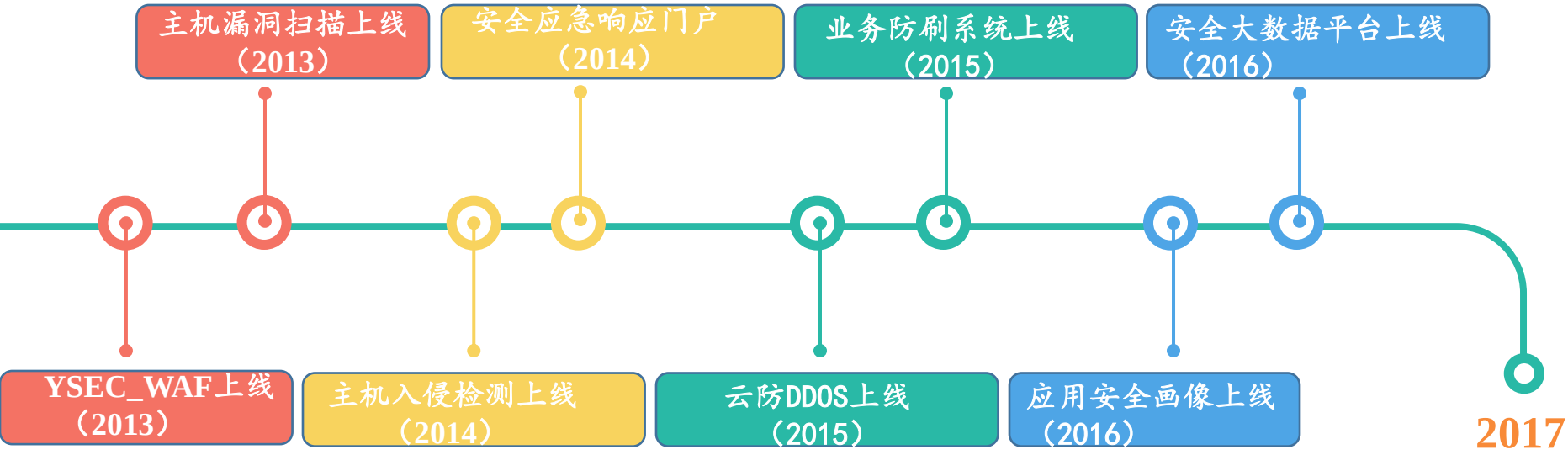
场景七：操作系统大量的会话状态跟踪表full，业务影响严重…

1 那些年我们一起救过的“火”

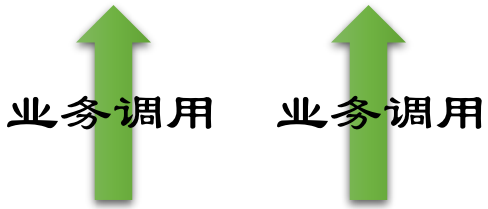
2 YY Live 安全运维体系建设实践

3 安全运维体系建设考虑的因素

YY安全运维发展历程里程碑



YY安全平台框架



Security As A Service 接口层

逆向破解 → 客户端安全

应用渗透 → 应用安全

嗅探入侵 → 主机安全

DDOS攻击 → 网络安全

安全画像库
（用户、设备、IP）

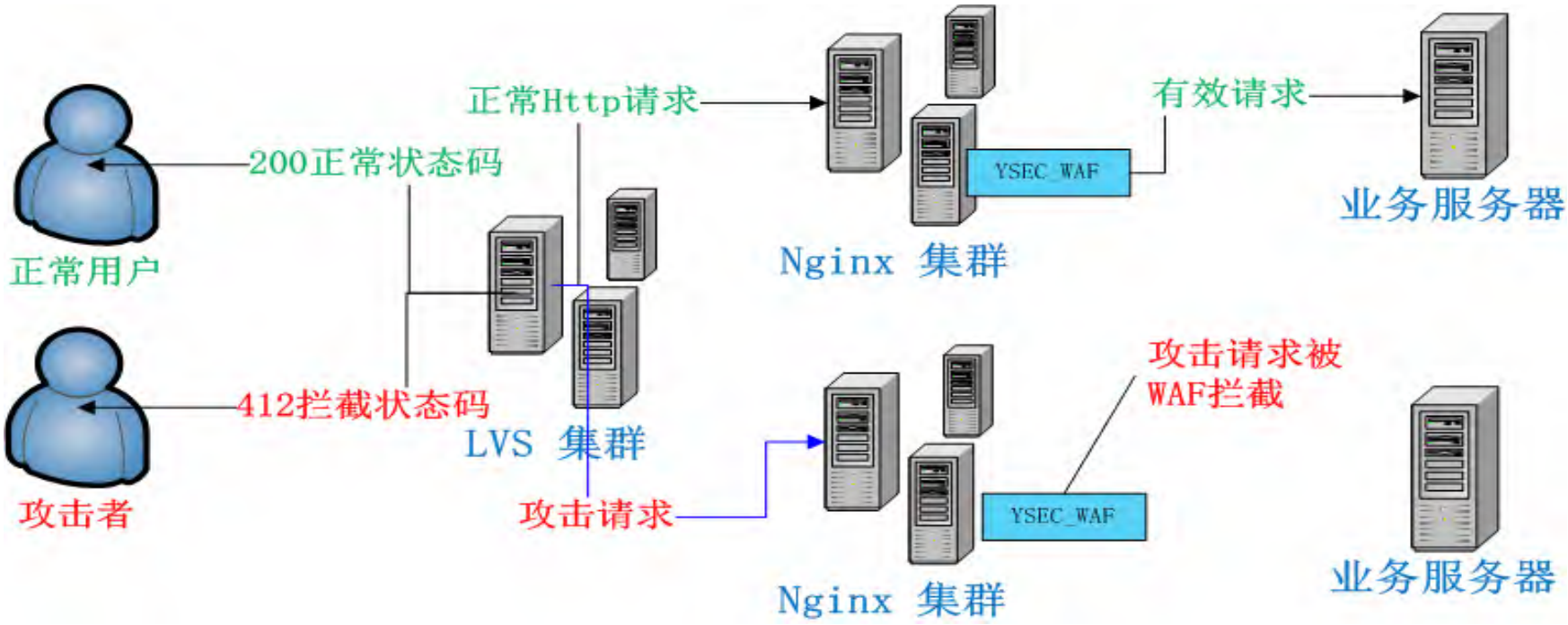
安全大数据计算平台

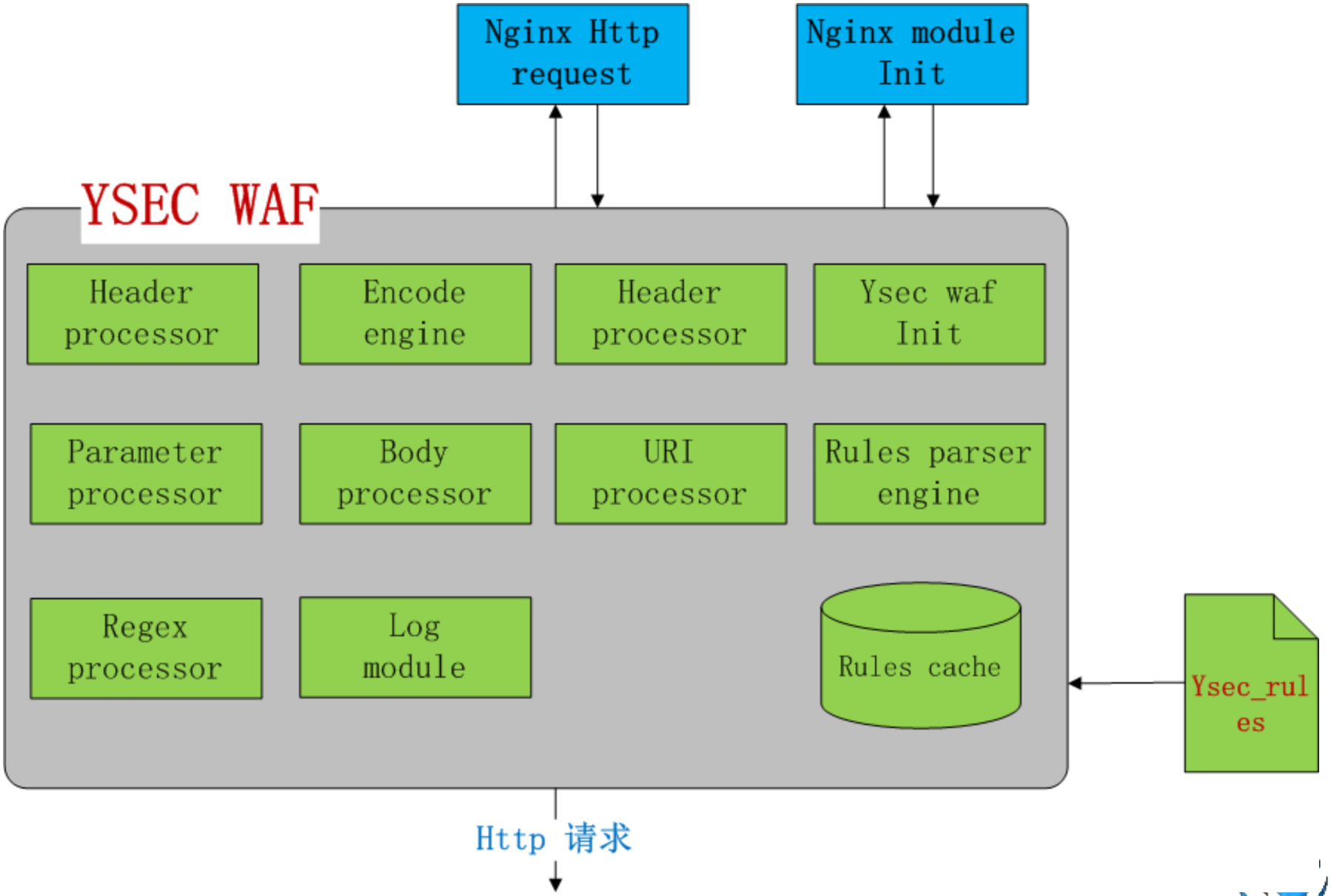
安全应急响应

YSRC门户


欢聚时代安全应急响应中心
YY SECURITY RESPONSE CENTER
【登录】 【注册】
首页
公告
提交漏洞
排行榜
礼品商城
应用加固
欢聚时代 YY.Inc
安全应急响应中心
YY SECURITY RESPONSE CENTER
提交漏洞
平台简介
欢聚时代对自身产品和业务的安全问题非常重视，也一直致力于保障用户安全，我们也希望通过此平台（YY安全应急响应中心）加强与业界合作和交流。您可以通过如下几种方式反馈：
1. 通过 “YY漏洞反馈平台” 在线提交。（推荐）
2. 发送邮件到漏洞接收专用邮箱：security@yy.com
排行榜
更多+
排名 昵称 总积分
1 梧桐雨 404
2 路人丙 370
3 琪宝爱小仰 340

应用安全—YSEC_WAF技术架构




Nginx Http request
Nginx module Init
YSEC WAF
Header processor
Encode engine
Header processor
Ysec waf Init
Parameter processor
Body processor
URI processor
Rules parser engine
Regex processor
Log module
Rules cache
Ysec_rules
Http 请求

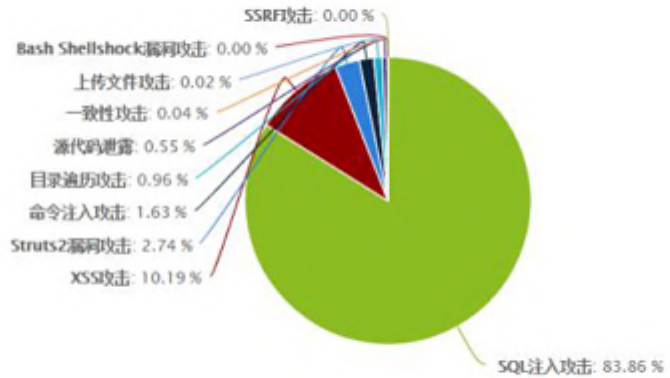
WAF拦截恶意请求


412
非常抱歉，由于您的请求URL有可能对网站造成安全威胁，您的访问被阻断。
Hacker
正常用户
网站应用防火墙
正常用户
源站
欢聚云安全

WAF实时拦截数据明细

WAF攻击类型统计数据

≡ 防御类型数据统计

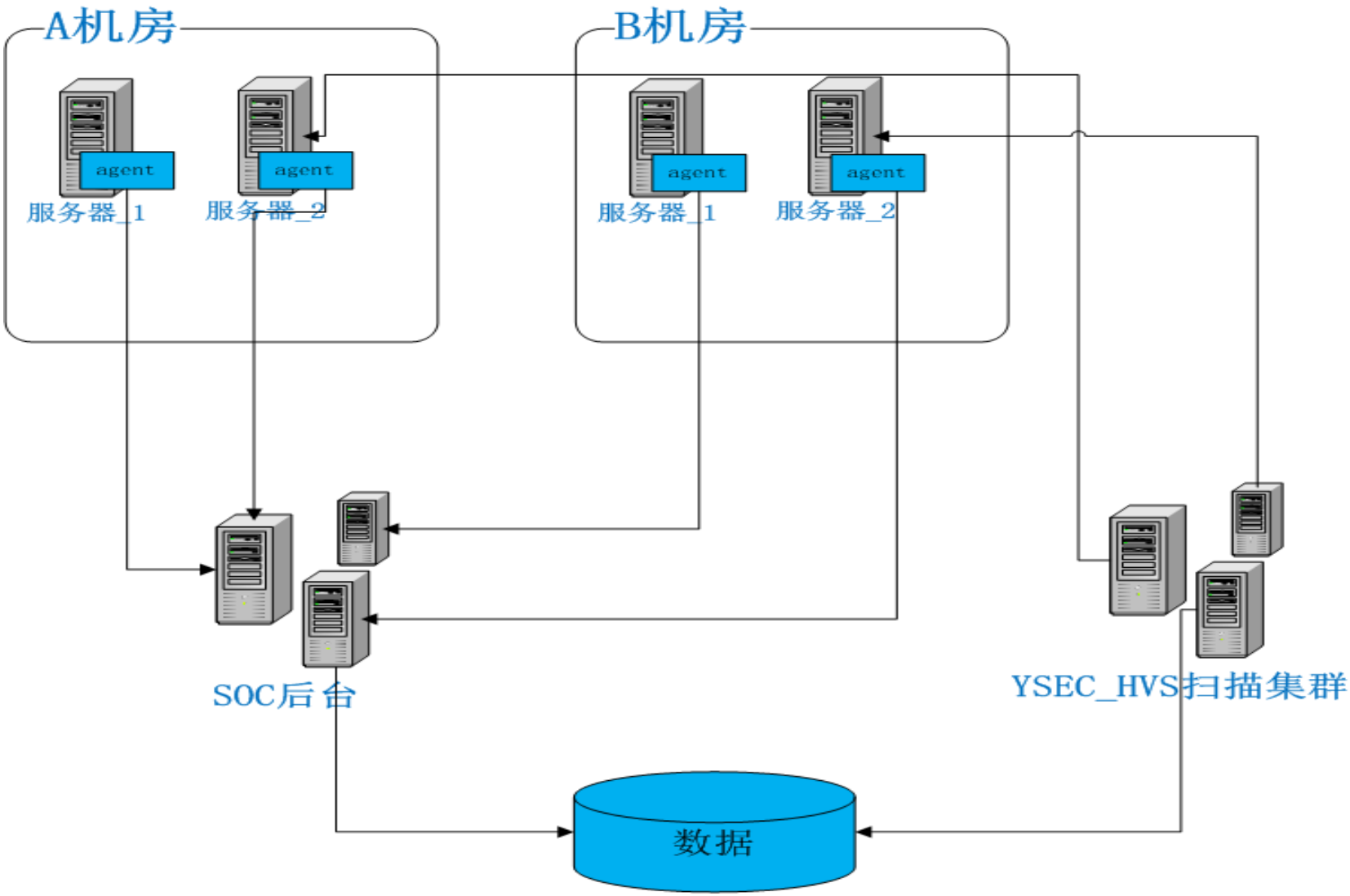


SQL注入攻击 XSS攻击 Struts2漏洞攻击 命令注入攻击 目录遍历攻击 源代码泄露 一致性攻击 上传文件攻击 Bash Shellshock漏洞攻击 SSRF攻击

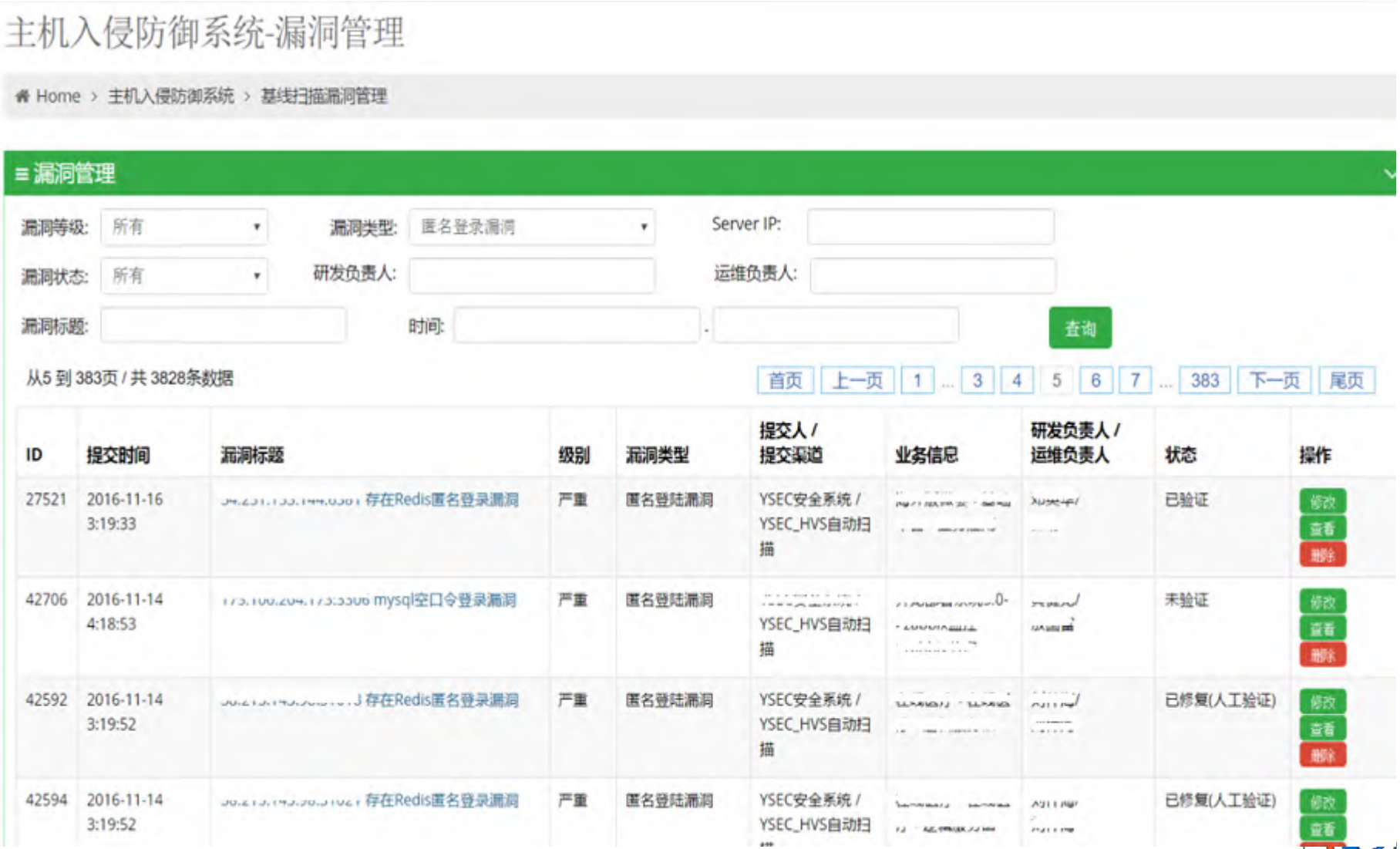
每页显示 10 条记录　　筛选:

序号	防御类型	累计次数
1	SQL注入攻击	1408321
2	XSS攻击	171140
3	Struts2漏洞攻击	46020
4	命令注入攻击	27448

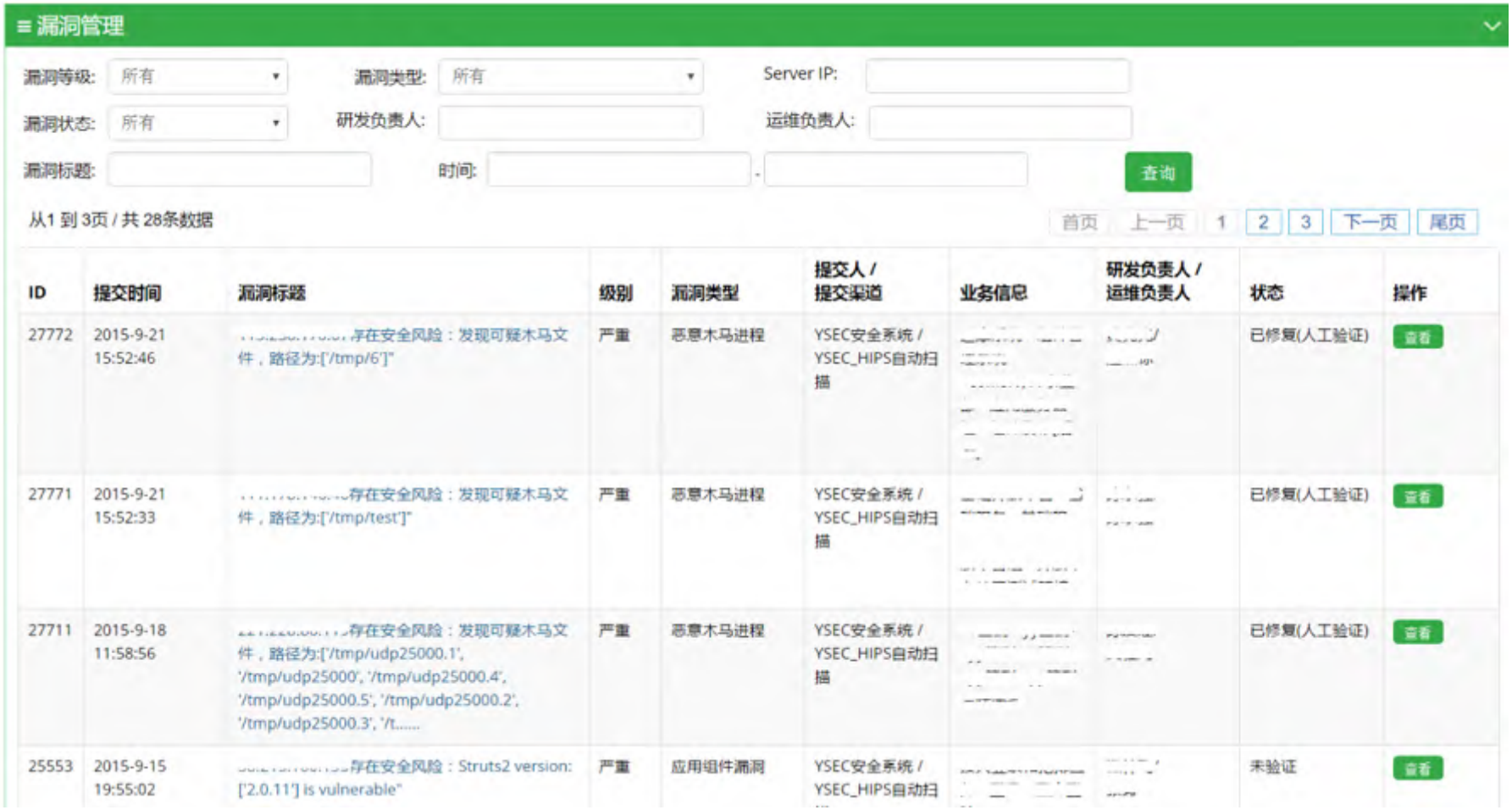
HVS&HIPS系统的架构图



HVS漏洞预警


主机入侵防御系统-漏洞管理
Home › 主机入侵防御系统 › 基线扫描漏洞管理
≡ 漏洞管理
漏洞等级: 所有
漏洞类型: 匿名登录漏洞
Server IP:
漏洞状态: 所有
研发负责人:
运维负责人:
漏洞标题:
时间:
查询
从5 到 383页 / 共 3828条数据
首页 上一页 1 ... 3 4 5 6 7 ... 383 下一页 尾页
ID 提交时间 漏洞标题 级别 漏洞类型 提交人 / 提交渠道 业务信息 研发负责人 / 运维负责人 状态 操作
27521 2016-11-16 3:19:33 存在Redis匿名登录漏洞 严重 匿名登陆漏洞 YSEC安全系统 / YSEC_HVS自动扫描 已验证 修改 查看 删除
42706 2016-11-14 4:18:53 mysql空口令登录漏洞 严重 匿名登陆漏洞 YSEC_HVS自动扫描 未验证 修改 查看 删除
42592 2016-11-14 3:19:52 存在Redis匿名登录漏洞 严重 匿名登陆漏洞 YSEC安全系统 / YSEC_HVS自动扫描 已修复(人工验证) 修改 查看 删除
42594 2016-11-14 3:19:52 存在Redis匿名登录漏洞 严重 匿名登陆漏洞 YSEC安全系统 / YSEC_HVS自动扫 已修复(人工验证) 修改 查看

HIPS系统入侵预警


≡ 漏洞管理
漏洞等级: 所有
漏洞类型: 所有
Server IP:
漏洞状态: 所有
研发负责人:
运维负责人:
漏洞标题:
时间:
查询
从1 到 3页 / 共 28条数据
首页 上一页 1 2 3 下一页 尾页
ID 提交时间 漏洞标题 级别 漏洞类型 提交人 / 提交渠道 业务信息 研发负责人 / 运维负责人 状态 操作
27772 2015-9-21 15:52:46 存在安全风险：发现可疑木马文件，路径为:['/tmp/6']" 严重 恶意木马进程 YSEC安全系统 / YSEC_HIPS自动扫描 已修复(人工验证) 查看
27771 2015-9-21 15:52:33 存在安全风险：发现可疑木马文件，路径为:['/tmp/test']" 严重 恶意木马进程 YSEC安全系统 / YSEC_HIPS自动扫描 已修复(人工验证) 查看
27711 2015-9-18 11:58:56 存在安全风险：发现可疑木马文件，路径为:['/tmp/udp25000.1', '/tmp/udp25000', '/tmp/udp25000.4', '/tmp/udp25000.5', '/tmp/udp25000.2', '/tmp/udp25000.3', '/t..... 严重 恶意木马进程 YSEC安全系统 / YSEC_HIPS自动扫描 已修复(人工验证) 查看
25553 2015-9-15 19:55:02 存在安全风险：Struts2 version: ['2.0.11'] is vulnerable" 严重 应用组件漏洞 YSEC安全系统 / YSEC_HIPS自动扫 未验证 查看

漏洞预警邮件通知

欢聚云安全
Huanju Cloud Security

漏洞预警通知

2016-11-30

亲、你好!

这是一封来自欢聚云安全的漏洞提醒信，为了提醒您及时修复漏洞，我们发送此邮件。

您名下机器存在4个漏洞，请点击漏洞标题查看详情修复方案.

批量修复

级别	类型	漏洞类型	剩余修复时间	操作
严重	非授权开放高危服务	memcached未授权访问漏洞	12小时	确认修复 忽略
严重	非授权开放高危服务	memcached未授权访问漏洞	12小时	确认修复 忽略
严重	匿名登陆漏洞	存在Redis匿名登录漏洞	12小时	确认修复 忽略
严重	非授权开放高危服务	memcached未授权访问漏洞	12小时	确认修复 忽略

修复期限:

严重漏洞：24小时内修复

中等漏洞：48小时内修复

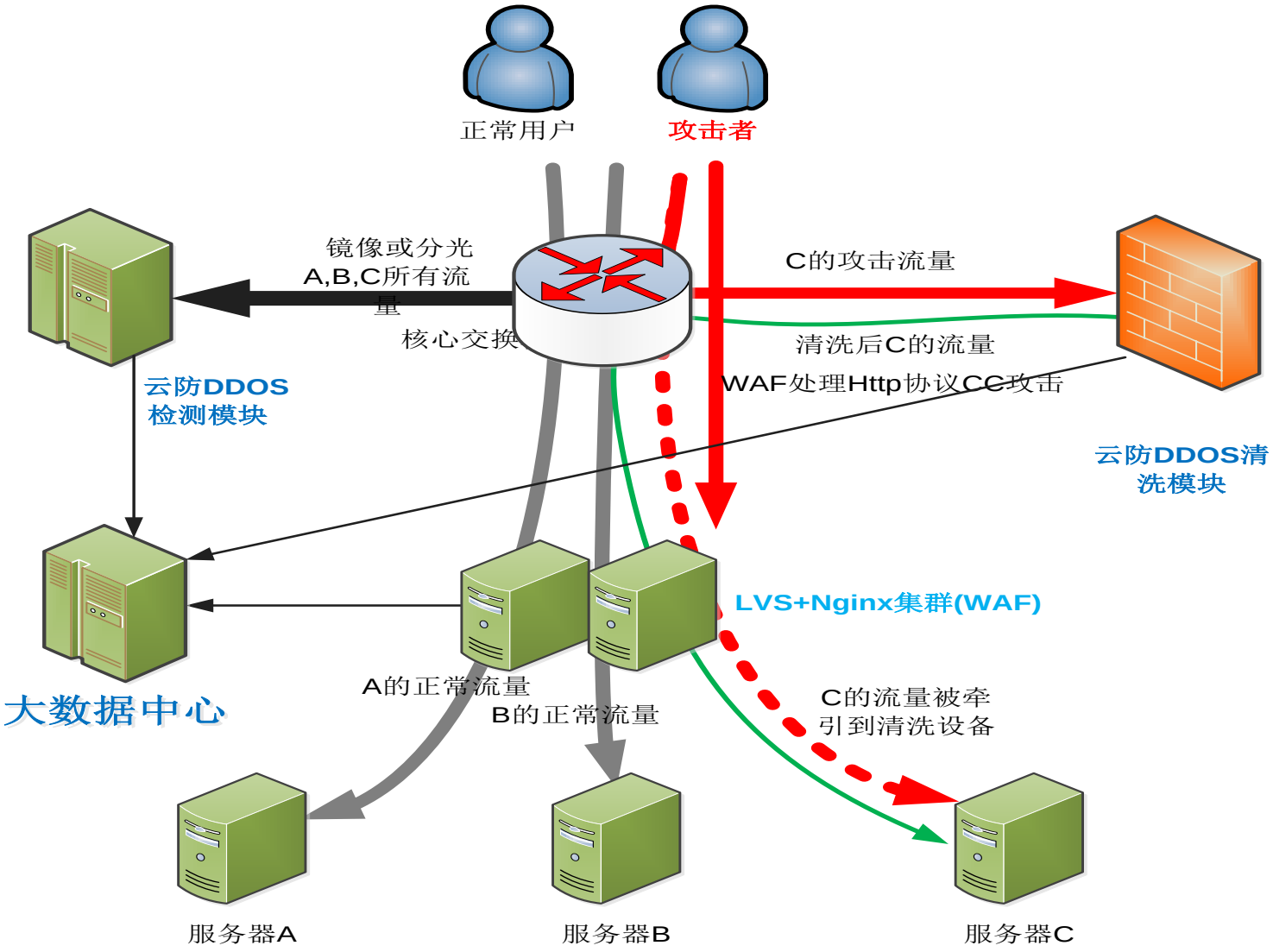
轻微漏洞：72小时内修复

漏洞案例:

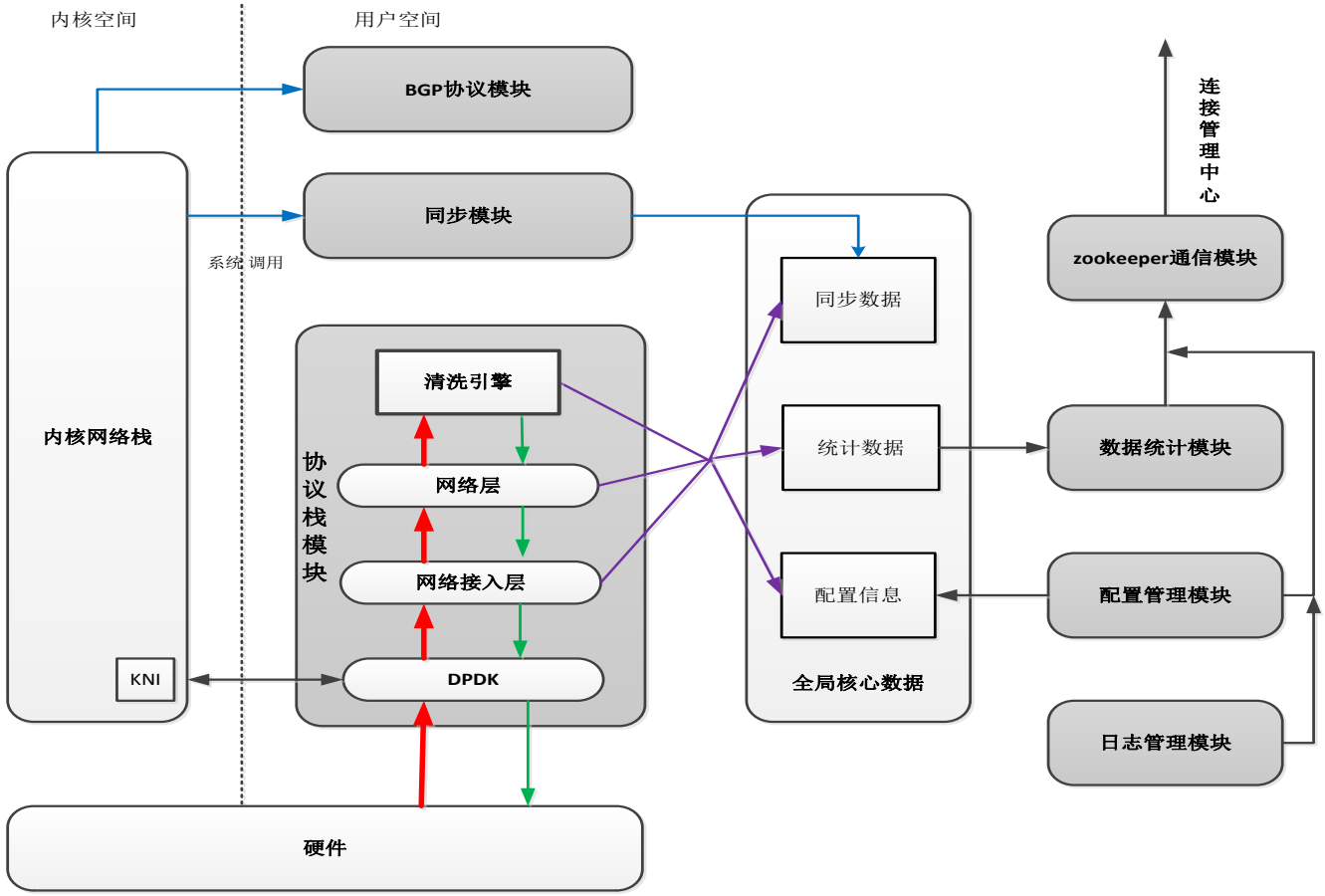
2015年2月，国家互联网应急中心（CNCERT）发现我司多台主机的memcached数据库存在未授权访问漏洞，可未经授权查看、修改、删除memcache缓存内容，对机密性、完整性、可用性构成部分影响。

2014年8月，安全系统扫描出某内部监控系统存在mysql匿名登录漏洞，允许root账户空密码登录，危害极大。

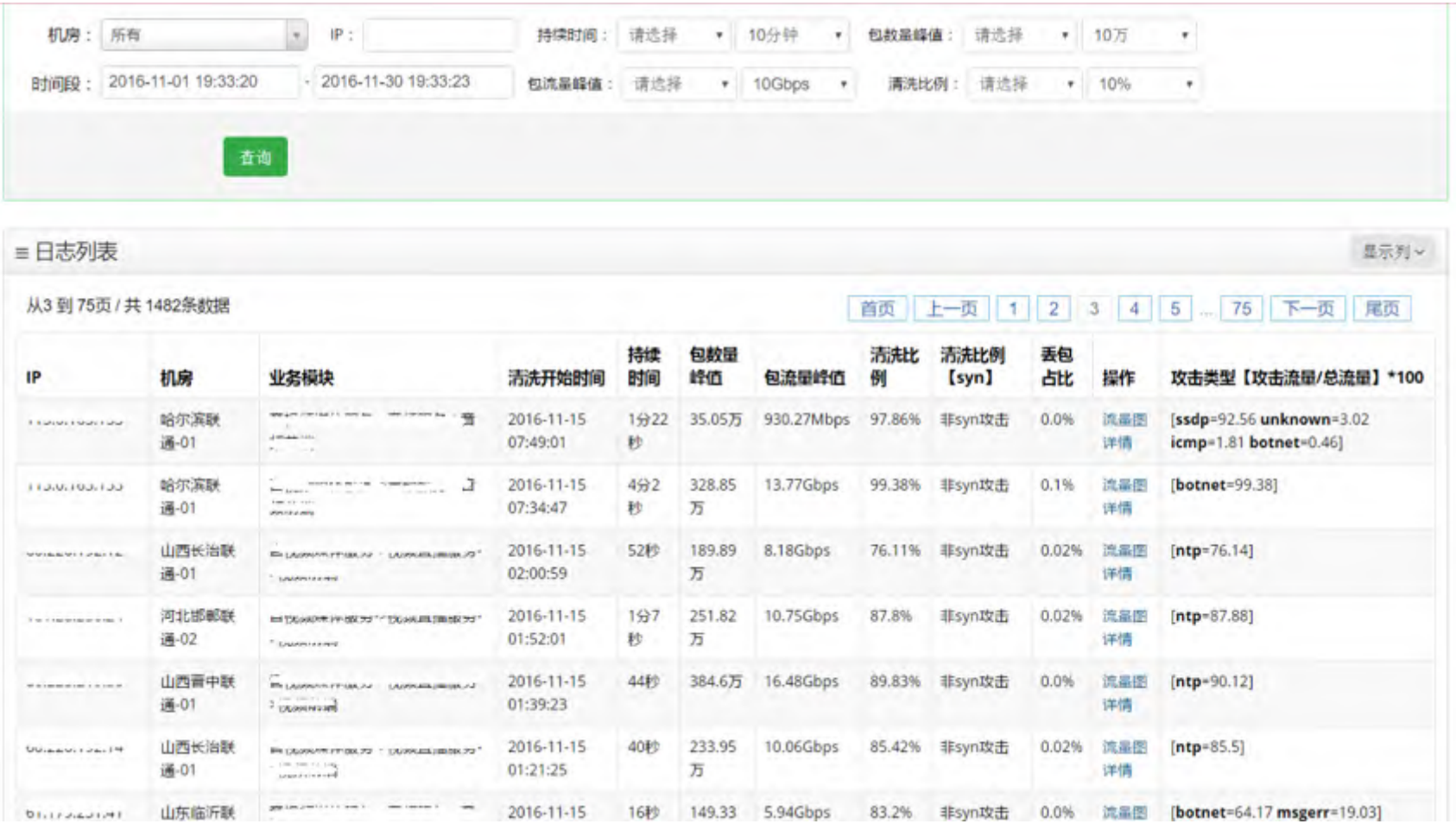
云防DDOS技术架构


正常用户
攻击者
镜像或分光
A,B,C所有流量
核心交换
C的攻击流量
清洗后C的流量
WAF处理Http协议CC攻击
云防DDOS
检测模块
云防DDOS清
洗模块
LVS+Nginx集群(WAF)
大数据中心
A的正常流量
B的正常流量
C的流量被牵
引到清洗设备
服务器A
服务器B
服务器C

清洗模块结构设计


内核空间
用户空间
BGP协议模块
同步模块
系统调用
内核网络栈
KNI
协议栈模块
清洗引擎
网络层
网络接入层
DPDK
硬件
同步数据
统计数据
配置信息
全局核心数据
连接管理中心
zookeeper通信模块
数据统计模块
配置管理模块
日志管理模块

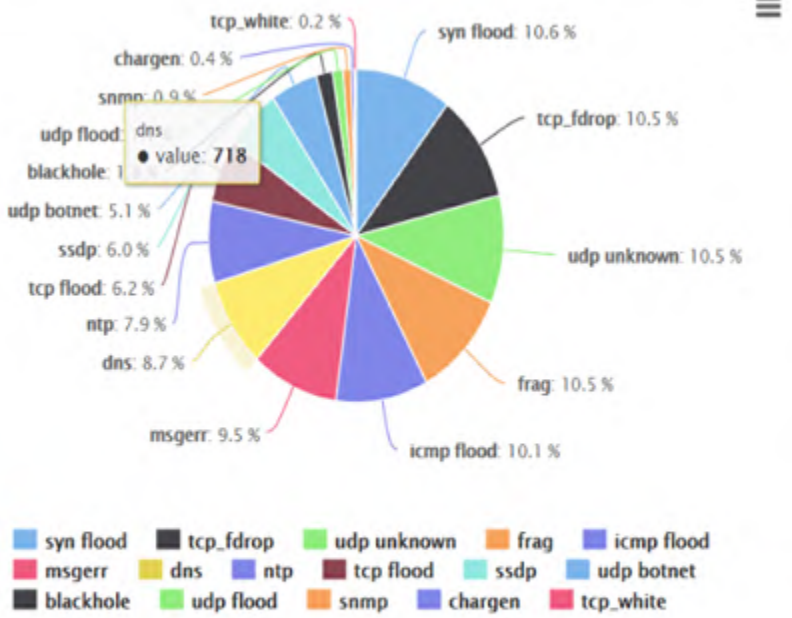
云防DDOS攻击流量清洗实时查询



IP	机房	业务模块	清洗开始时间	持续时间	包数量峰值	包流量峰值	清洗比例	清洗比例【syn】	丢包占比	操作	攻击类型【攻击流量/总流量】*100
[redacted]	哈尔滨联通-01	[redacted]	2016-11-15 07:49:01	1分22秒	35.05万	930.27Mbps	97.86%	非syn攻击	0.0%	流量图 详情	[ssdp=92.56 unknown=3.02 icmp=1.81 botnet=0.46]
[redacted]	哈尔滨联通-01	[redacted]	2016-11-15 07:34:47	4分2秒	328.85万	13.77Gbps	99.38%	非syn攻击	0.1%	流量图 详情	[botnet=99.38]
[redacted]	山西长治联通-01	[redacted]	2016-11-15 02:00:59	52秒	189.89万	8.18Gbps	76.11%	非syn攻击	0.02%	流量图 详情	[ntp=76.14]
[redacted]	河北邯郸联通-02	[redacted]	2016-11-15 01:52:01	1分7秒	251.82万	10.75Gbps	87.8%	非syn攻击	0.02%	流量图 详情	[ntp=87.88]
[redacted]	山西晋中联通-01	[redacted]	2016-11-15 01:39:23	44秒	384.6万	16.48Gbps	89.83%	非syn攻击	0.0%	流量图 详情	[ntp=90.12]
[redacted]	山西长治联通-01	[redacted]	2016-11-15 01:21:25	40秒	233.95万	10.06Gbps	85.42%	非syn攻击	0.02%	流量图 详情	[ntp=85.5]
[redacted]	山东临沂联	[redacted]	2016-11-15	16秒	149.33	5.94Gbps	83.2%	非syn攻击	0.0%	流量图	[botnet=64.17 msgerr=19.03]

云防DDOS攻击统计数据查询

≡ 按攻击类型统计



每页显示 10 条记录　　筛选:

序号	攻击类型	攻击次数
1	syn flood	879
2	tcp_fdrop	872
3	udp unknown	872
4	frag	872
5	icmp flood	839
6	msgerr	792
7	dns	718
8	ntp	658
9	tcp flood	514
10	ssdp	494

从 1 到 10 /共 16 条数据　　← 前一页　1　2　后一页 →

DDOS攻击预警邮件通知

发件人：security<security@yy.com>
收件人：
抄送：ysrc<ysrc@yy.com>, security<security@yy.com>
时间：2016年12月1日 (周四) 00:04
大小：75 KB

欢聚云安全
Huanju Cloud Security

攻击预警通知

2016-12-01

亲、你好!

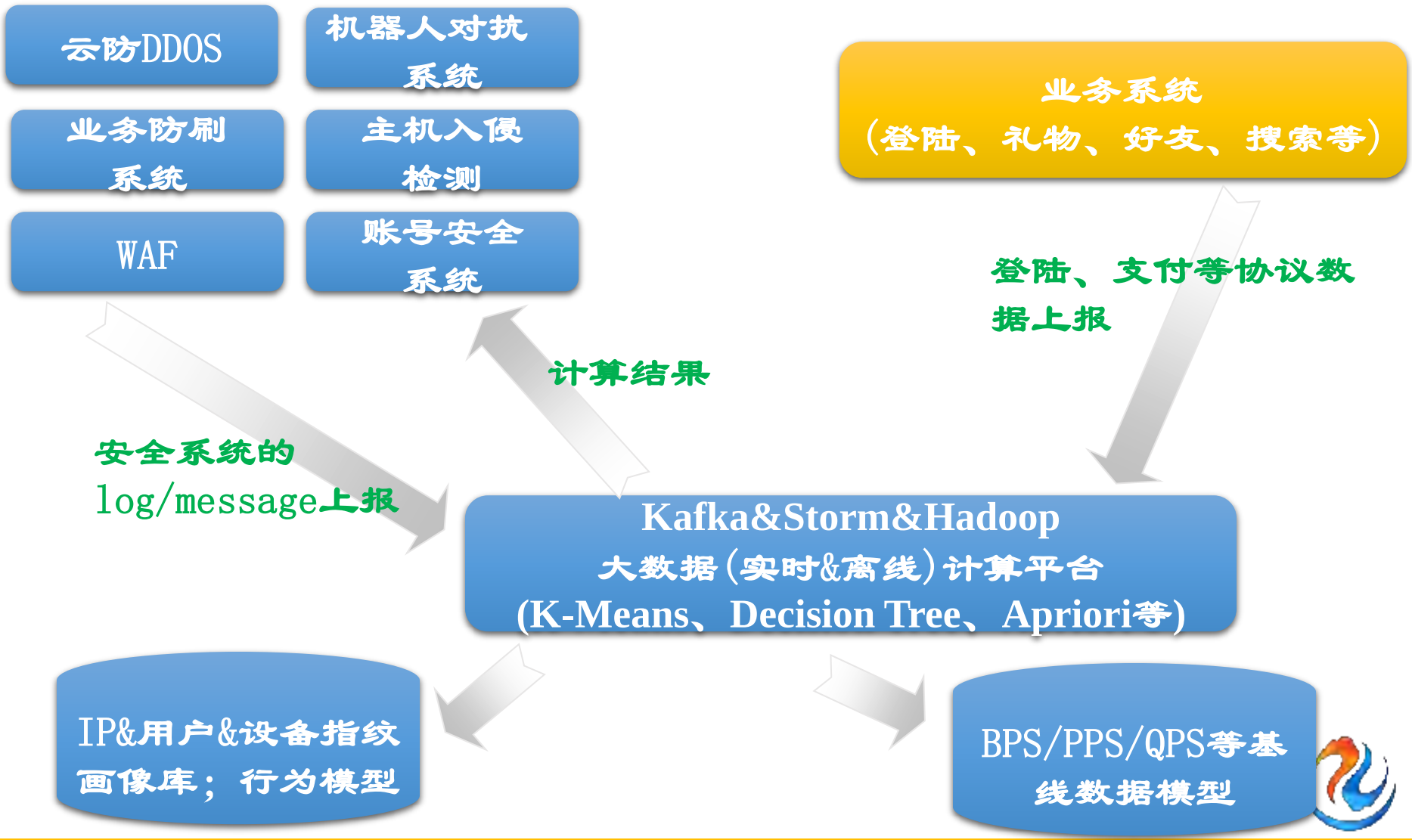
这是一封来自欢聚云安全的云防DDOS系统的预警邮件，云防DDOS为您名下机器防御的网络攻击如下表：

IP	机房	运维负责人	研发负责人	业务模块
[redacted]	浙[redacted]	[redacted]	[redacted]	[redacted]

清洗开始时间	持续时间	包数量峰值	包流量峰值	牵引总包量	清洗总包量	牵引总流量	清洗总流量	清洗比例
2016-11-30 23:53:03	5分24秒	1571.28万	44.31Gbps	143927.55万	143786.39万	481.44GB	481.05GB	99.9%

如果你收到了此封邮件，说明云防DDOS系统为你名下的机器防御了一次DDOS网络流量攻击！
此封邮件是流量清洗过程结束后产生的邮件，里面各字段的含义分别是
受保护IP的相关信息
1）受保护IP：云防DDOS系统此次保护的IP地址
2）所在机房：受保护IP所在的IDC机房
3）运维负责人：受保护IP对应服务器的运维负责人

大数据计算在平台框架


云防DDOS
机器人对抗系统
业务防刷系统
主机入侵检测
WAF
账号安全系统
业务系统
（登陆、礼物、好友、搜索等）
登陆、支付等协议数据上报
计算结果
安全系统的
log/message上报
Kafka&Storm&Hadoop
大数据（实时&离线）计算平台
(K-Means、Decision Tree、Apriori等)
IP&用户&设备指纹画像库；行为模型
BPS/PPS/QPS等基线数据模型

安全大数据2016年度报告

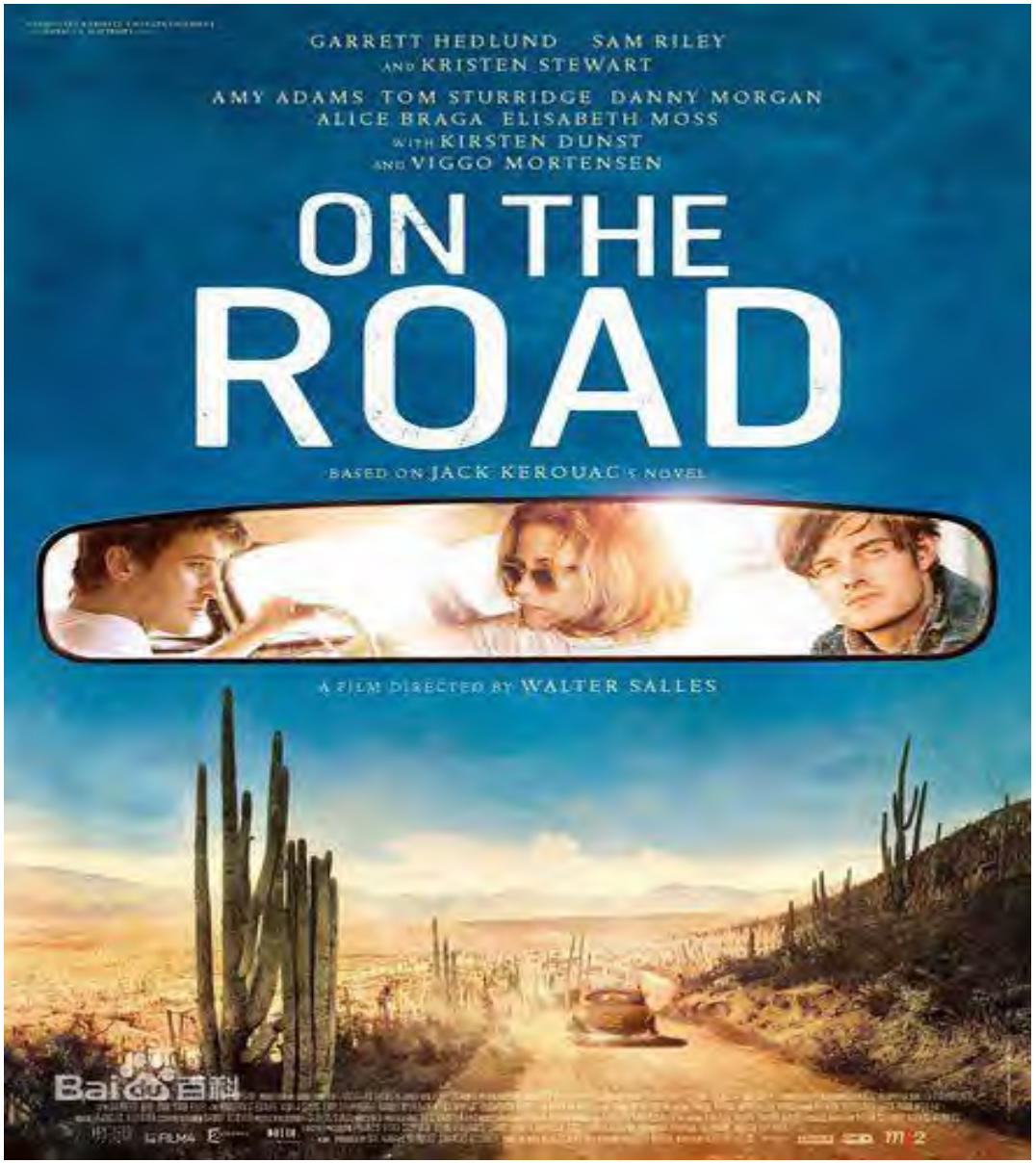
1 那些年我们一起救过的“火”

2 YY Live 安全运维体系建设实践

3 安全运维体系建设考虑的因素

考虑的几个因素：

1. 投入产出比
2. 关键矛盾
3. 不一定100分
4. 分阶段实施
5. 数据化、可视化、自动化
6. “安全”VS“业务”的平衡


GARRETT HEDLUND SAM RILEY
AND KRISTEN STEWART
AMY ADAMS TOM STURRIDGE DANNY MORGAN
ALICE BRAGA ELISABETH MOSS
WITH KIRSTEN DUNST
AND VIGGO MORTENSEN
ON THE ROAD
BASED ON JACK KEROUAC'S NOVEL
A FILM DIRECTED BY WALTER SALLES

QA

DevOpsDays 即将首次登陆中国

DevOps 之父 Patrick Debois 与您相约

DevOpsDays 北京站 2017年3月18日

门票早鸟价仅限前100名，请从速哟

http://2017-beijing.devopsdayschina.org/

想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好

Thanks

高效运维社区

开放运维联盟

荣誉出品