



GOPPS2016
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：



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



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 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…

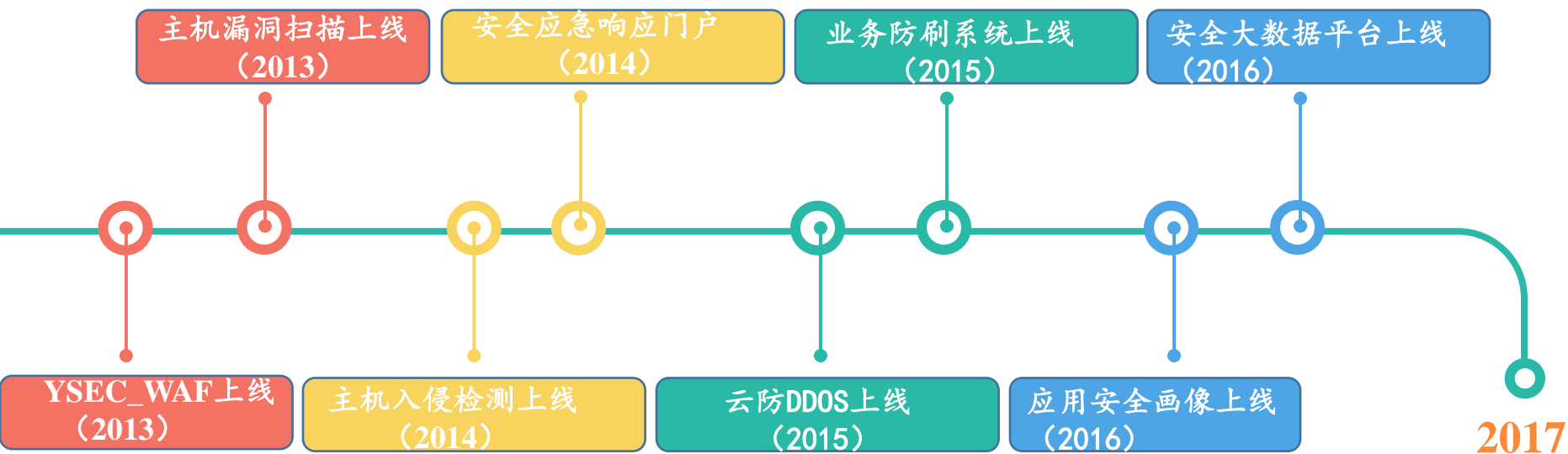


1 那些年我们一起救过的“火”

➔ **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



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

YY会员
vip.yy.com

虎牙直播
www.huya.com



娱乐直播
www.yy.com

多玩游戏网
www.duowan.com

100教育
www.100.com

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：

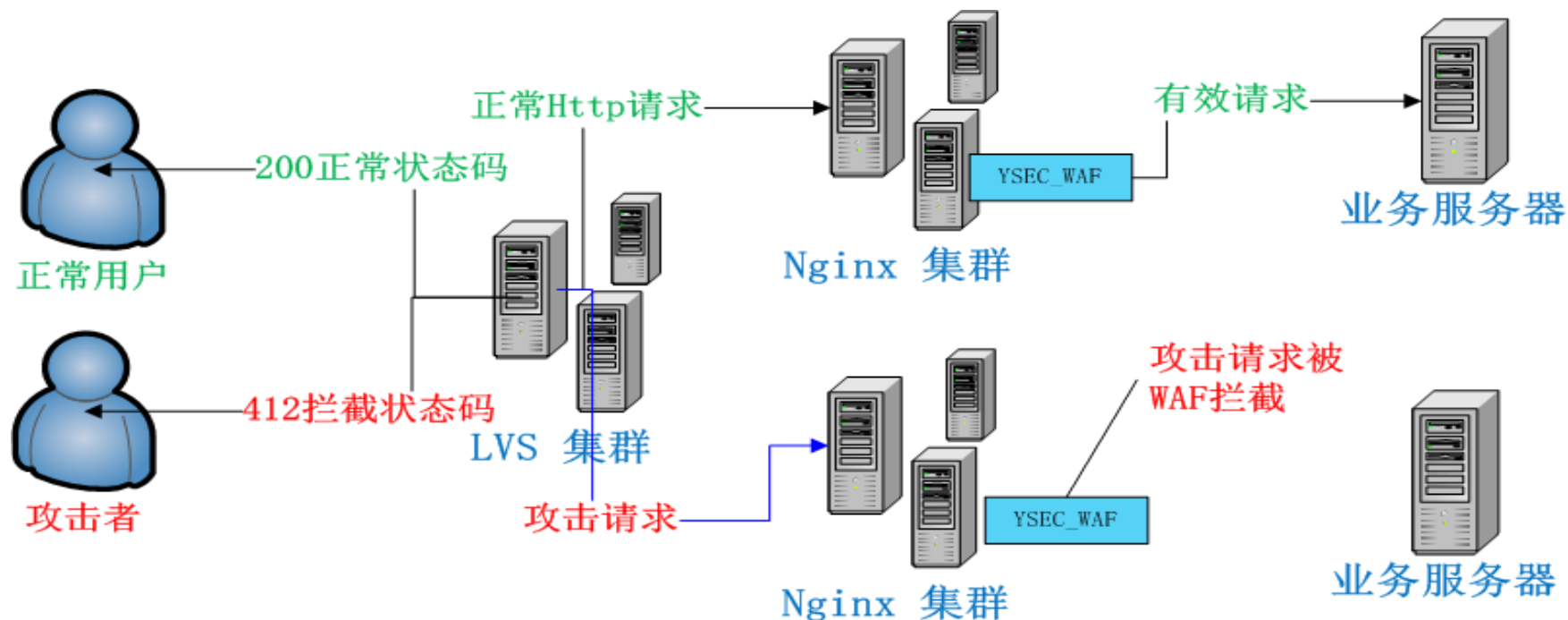
1. 通过“YY漏洞反馈平台”在线提交。（推荐）
2. 发送邮件到漏洞接收专用邮箱：security@yy.com

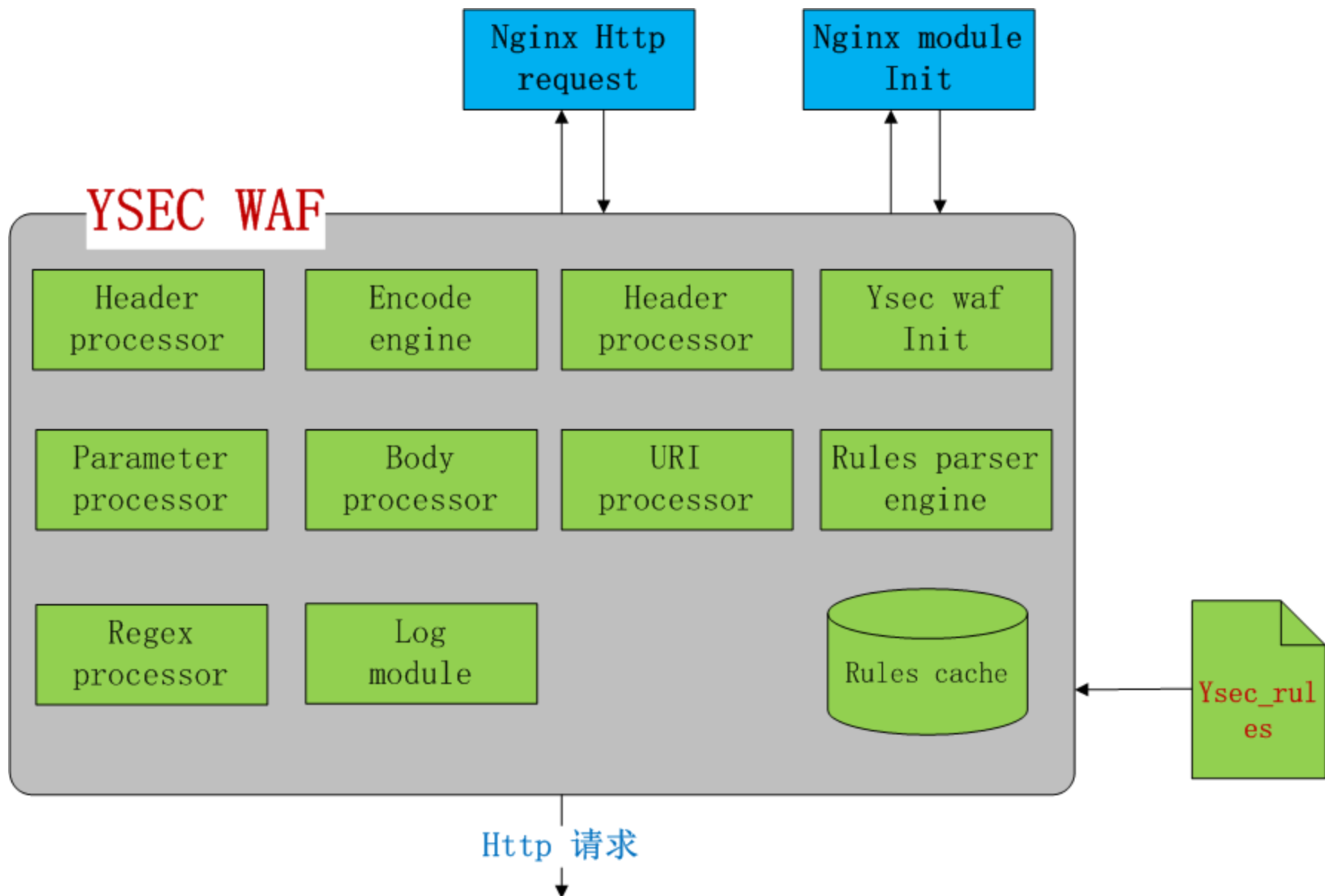
排行榜

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





WAF拦截恶意请求



WAF实时拦截数据明细

WEB入侵防御系统-日志中心

Home > Web入侵防御系统 > 防御日志查询

日志查询

Server IP: 防御模式: 规则id: Domain 域名:

Client IP: 防御类型: 内部IP: 时间: - ☐ 所有

从1 到 5页 / 共 89条数据

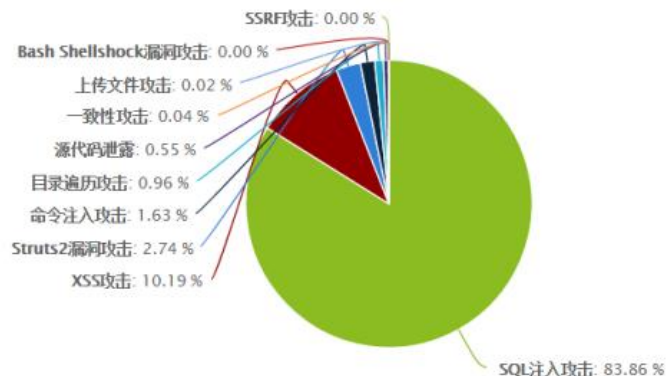
[首页](#) [上一页](#) [1](#) [2](#) [3](#) ... [5](#) [下一页](#) [尾页](#)

时间戳	防御类型	防御模式	域名	用户IP	日志
2016-11-17 19:11:32	Struts2漏洞攻击	拦截	m.yy.com	[REDACTED]	2016/11/17 19:11:32 [error] 20988#0: *1417943978 [ysec_waf] block id: 1701 var: redirect:\${%23w%3d%23context.get('com.opensymphony.xwork2.dispatcher.HttpServletRe client_ip: [REDACTED] server_ip: [REDACTED] client: [REDACTED] server: m.yy.com request: "GET /live/anchor.html?redirect=\${%23w%3d%23context.get('com.op host: "m.yy.com"
2016-11-17 19:11:29	Struts2漏洞攻击	拦截	m.yy.com	[REDACTED]	2016/11/17 19:11:29 [error] 7140#0: *1411920089 [ysec_waf] block id: 1701 var: method:%23_memberAccess%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%2C%23 client_ip: [REDACTED]



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

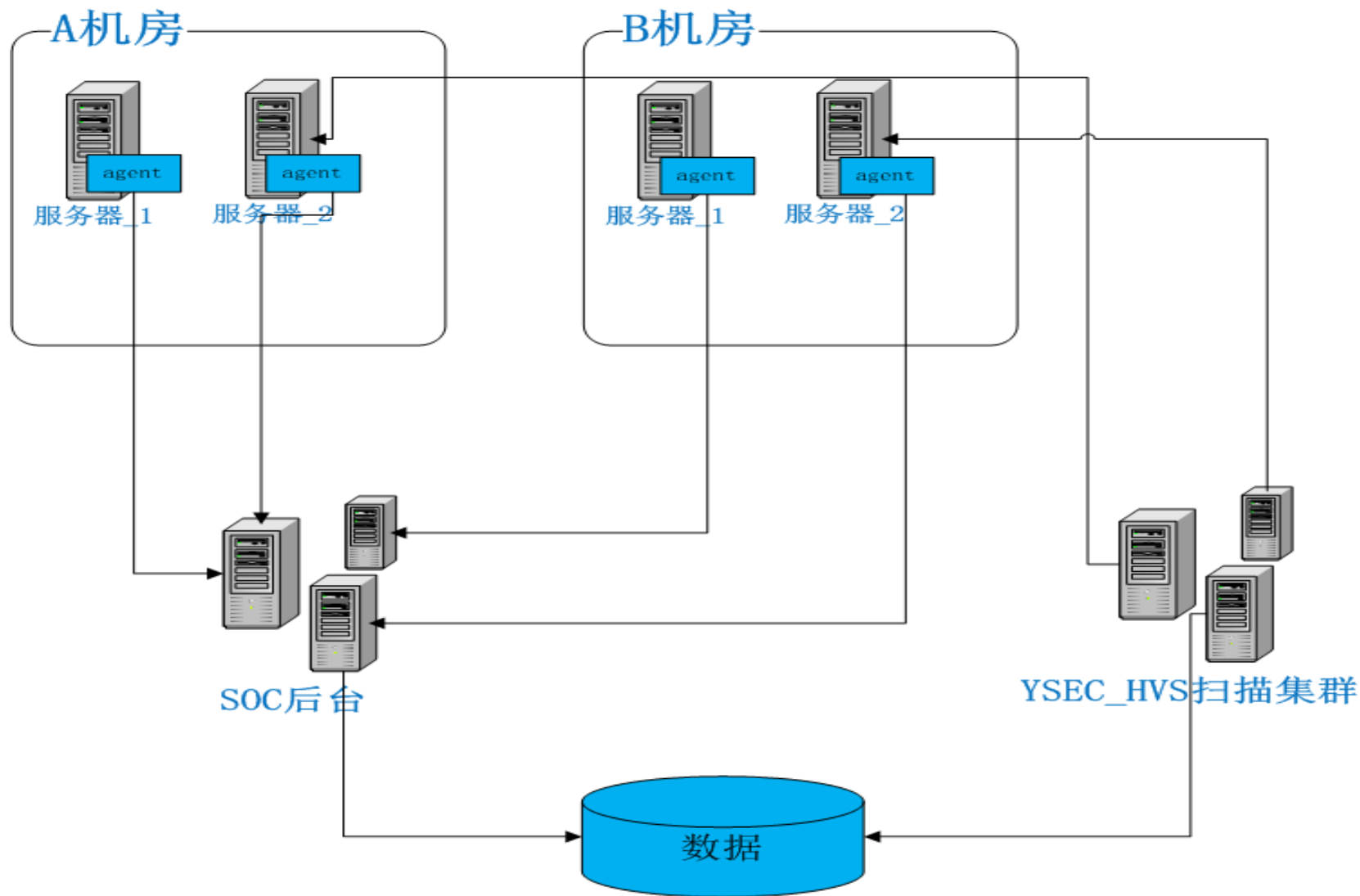
每页显示 10 条记录

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	<div>修改查看删除</div>
42706	2016-11-14 4:18:53	mysql空口令登录漏洞	严重	匿名登陆漏洞	YSEC安全系统 / YSEC_HVS自动扫描			未验证	<div>修改查看删除</div>
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)	<div>修改查看删除</div>
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自动扫描			已修复(人工验证)	<div>修改查看</div>

HIPS系统入侵预警

漏洞管理

漏洞等级: 漏洞类型: Server IP:

漏洞状态: 研发负责人: 运维负责人:

漏洞标题: 时间: -

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	172.20.17.60 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	172.20.17.60 存在安全风险: 发现可疑木马文件, 路径为:['/tmp/6']"	52000 / 172.20.17.60	已修复(人工验证)	<input type="button" value="查看"/>
27771	2015-9-21 15:52:33	172.20.17.60 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	172.20.17.60 存在安全风险: 发现可疑木马文件, 路径为:['/tmp/test']"	52000 / 172.20.17.60	已修复(人工验证)	<input type="button" value="查看"/>
27711	2015-9-18 11:58:56	172.20.17.60 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	172.20.17.60 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.....	52000 / 172.20.17.60	已修复(人工验证)	<input type="button" value="查看"/>
25553	2015-9-15 19:55:02	172.20.17.60 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自动扫描	172.20.17.60 存在安全风险: Struts2 version: ['2.0.11'] is vulnerable"	52000 / 172.20.17.60	未验证	<input type="button" value="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	173.20.87.192:11211 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	173.20.87.192:11211 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	10.128.10.100:6379 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	50.128.10.100:11211 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

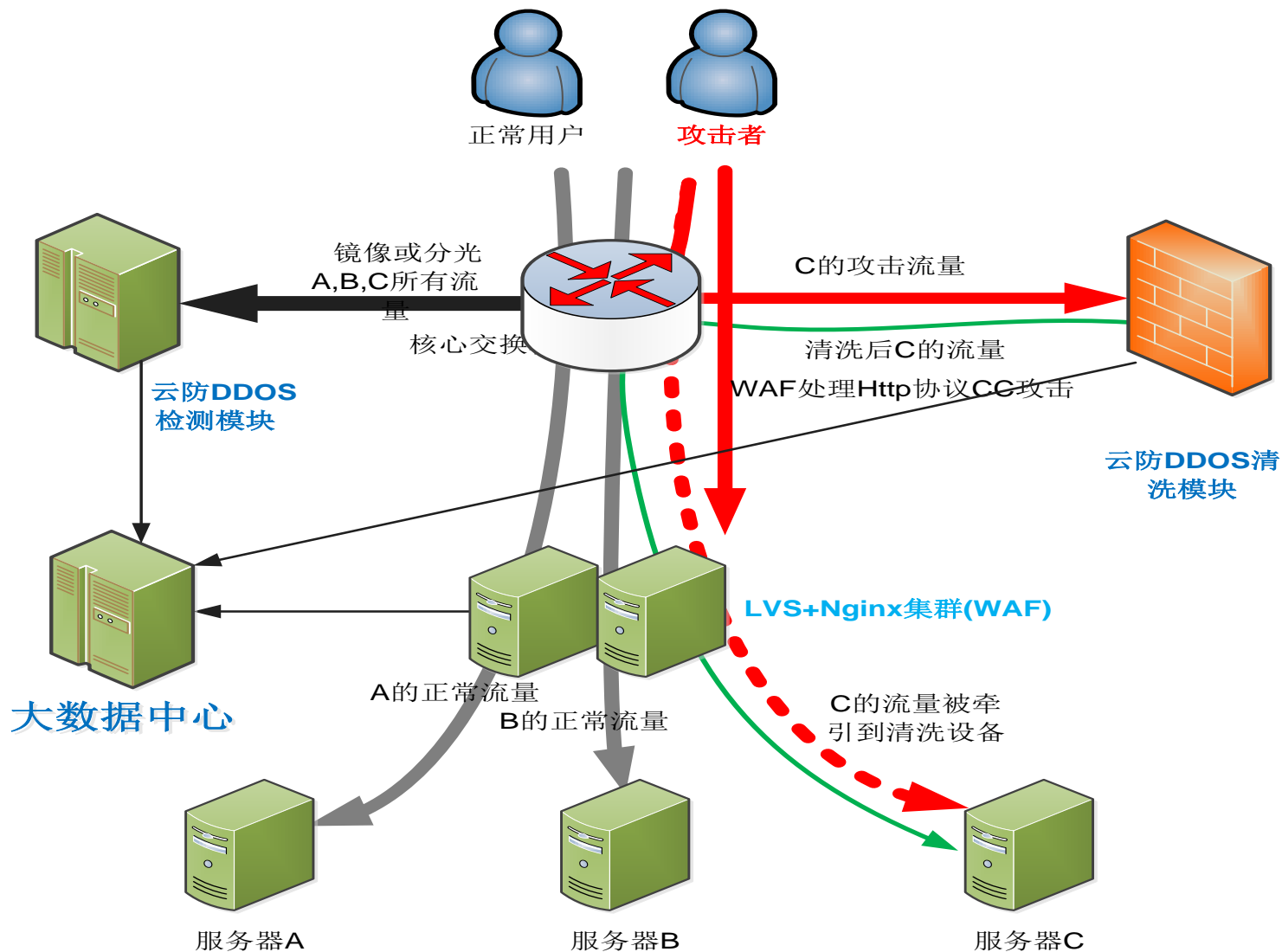
轻微漏洞：72小时内修复

漏洞案例:

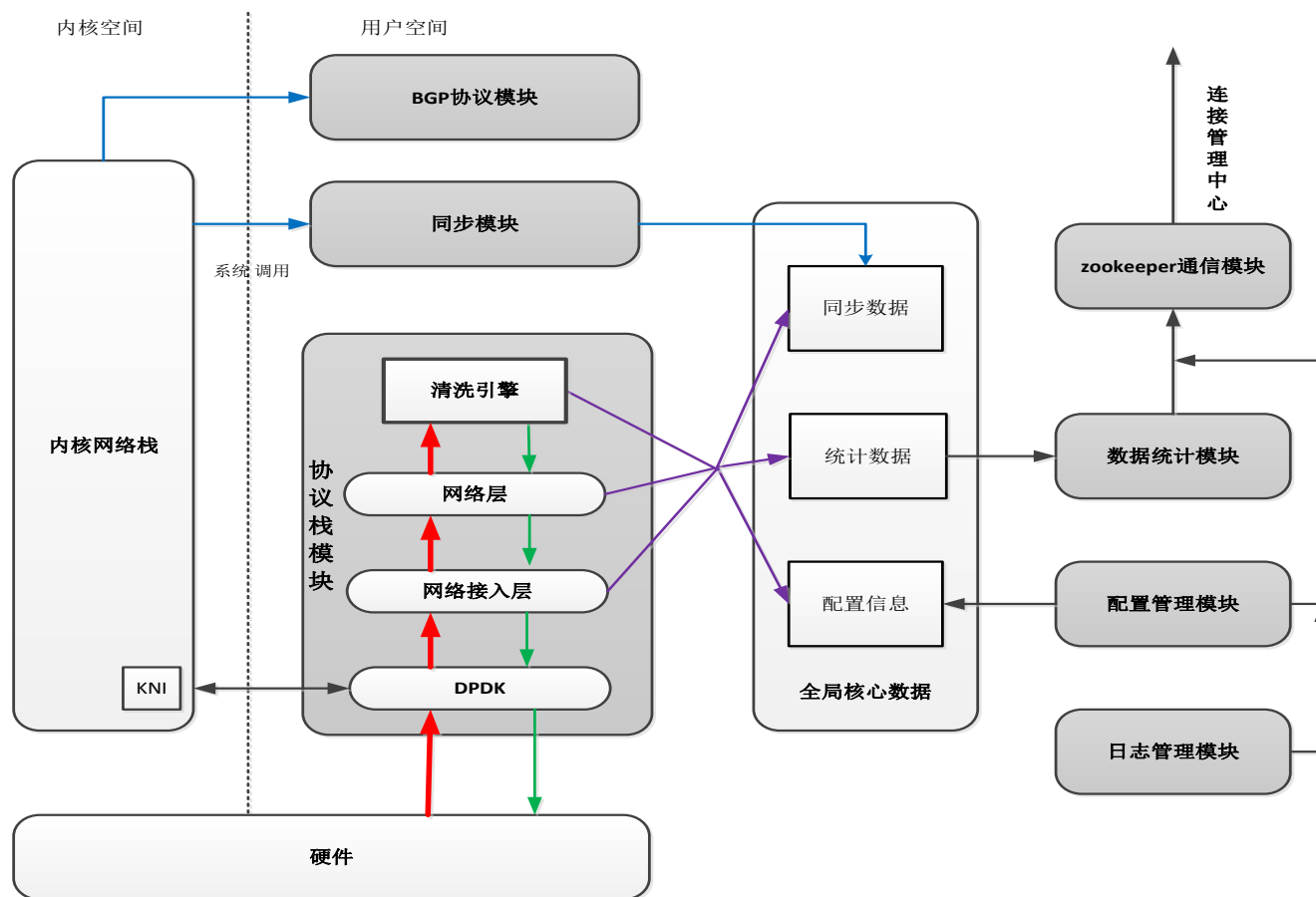
2015年2月，国家互联网应急中心（CNCERT）发现我司多台主机的memcached数据库存在未授权访问漏洞，可未经授权查看、修改、删除memcache缓存内容，对机密性、完整性、可用性构成部分影响。

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



清洗模块结构设计



云防DDOS攻击流量清洗实时查询

机房: IP: 持续时间: 包数量峰值:

时间段: - 包流量峰值: 清洗比例:

≡ 日志列表

显示列 ▾

从3 到 75页 / 共 1482条数据

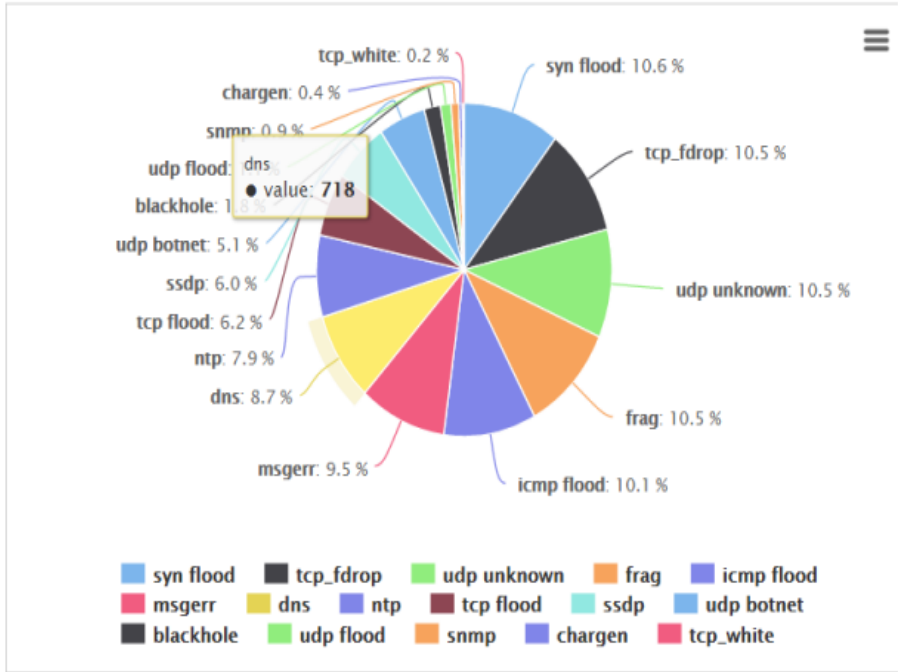
[首页](#) [上一页](#) [1](#) [2](#) [3](#) [4](#) [5](#) ... [75](#) [下一页](#) [尾页](#)

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
113.0.103.133	哈尔滨联通-01	业务模块	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]
113.0.103.133	哈尔滨联通-01	业务模块	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]
202.20.128.116	山西长治联通-01	业务模块	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]
101.202.251.11	河北邯郸联通-02	业务模块	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]
202.20.128.116	山西晋中联-01	业务模块	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]
202.20.128.116	山西长治联通-01	业务模块	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]
61.17.242.111	山东临沂联	业务模块	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：[redacted]
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



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]		浙江 [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！

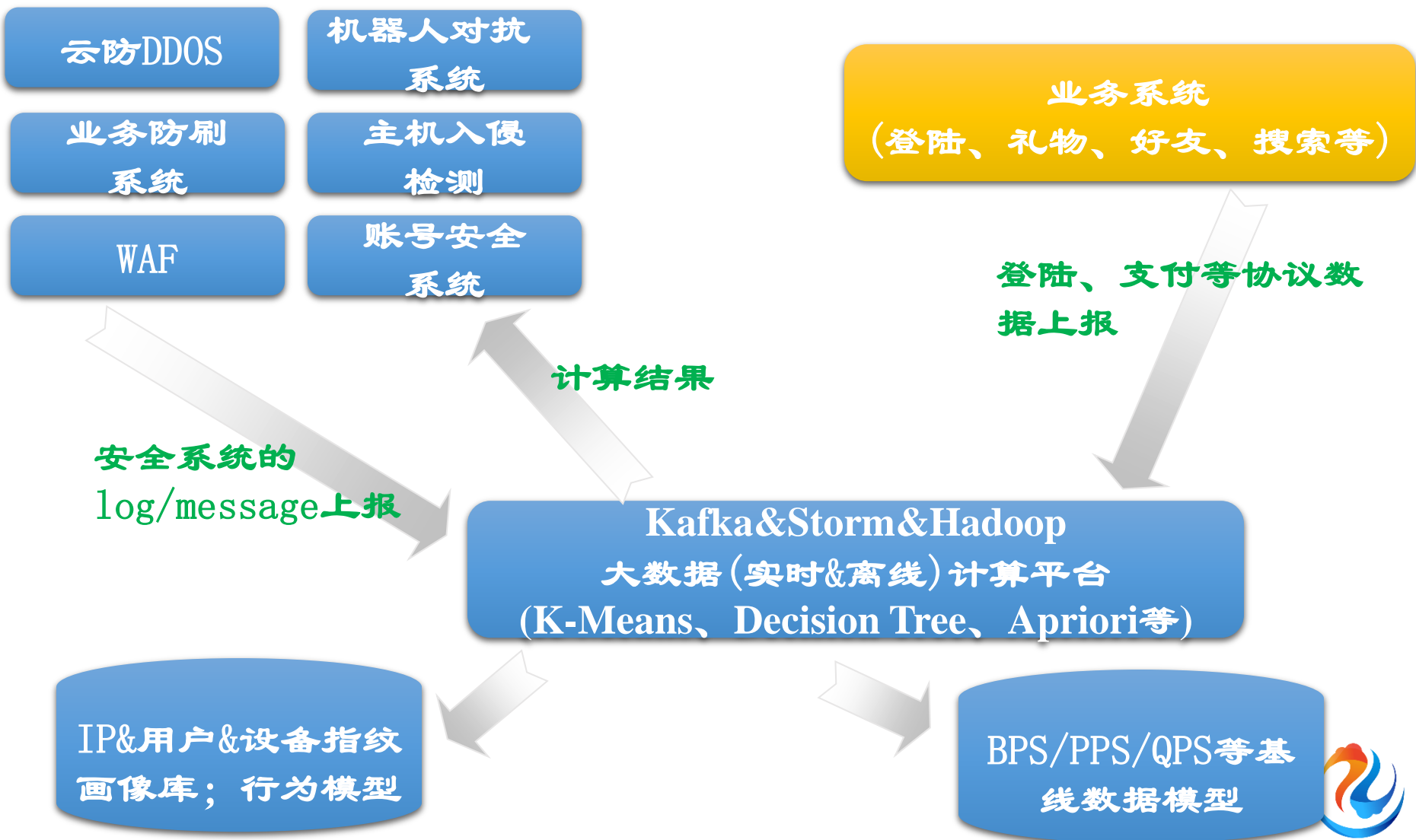
此封邮件是流量清洗过程结束后产生的邮件，里面各字段的含义分别是

受保护IP的相关信息

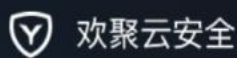
- 1) 受保护IP：云防DDOS系统此次保护的IP地址
- 2) 所在机房：受保护IP所在的IDC机房
- 3) 运维负责人：受保护IP对应服务器的运维负责人



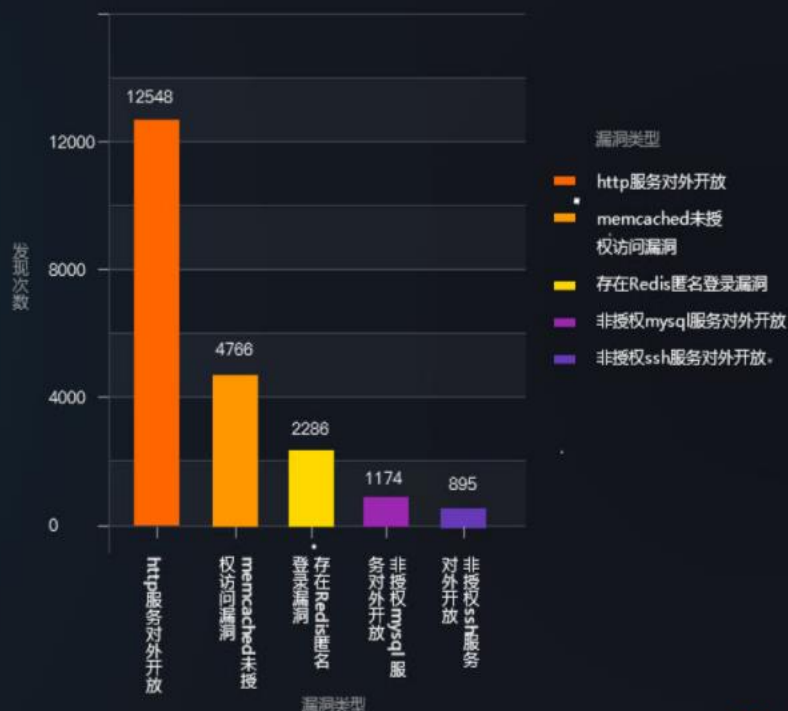
大数据计算在平台框架



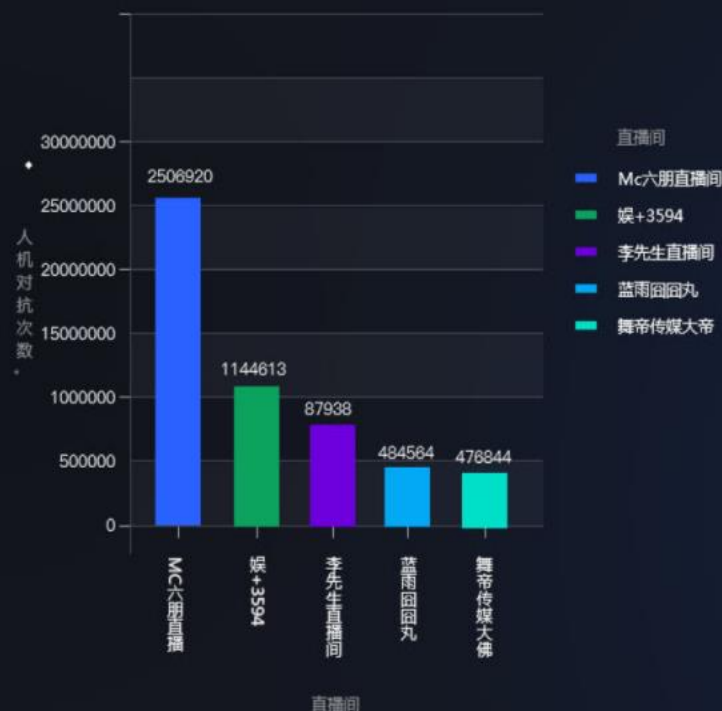
安全大数据2016年度报告



Top 5 发现漏洞类型统计



Top 5 人机对抗统计



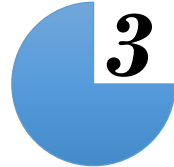





1 那些年我们一起救过的“火”

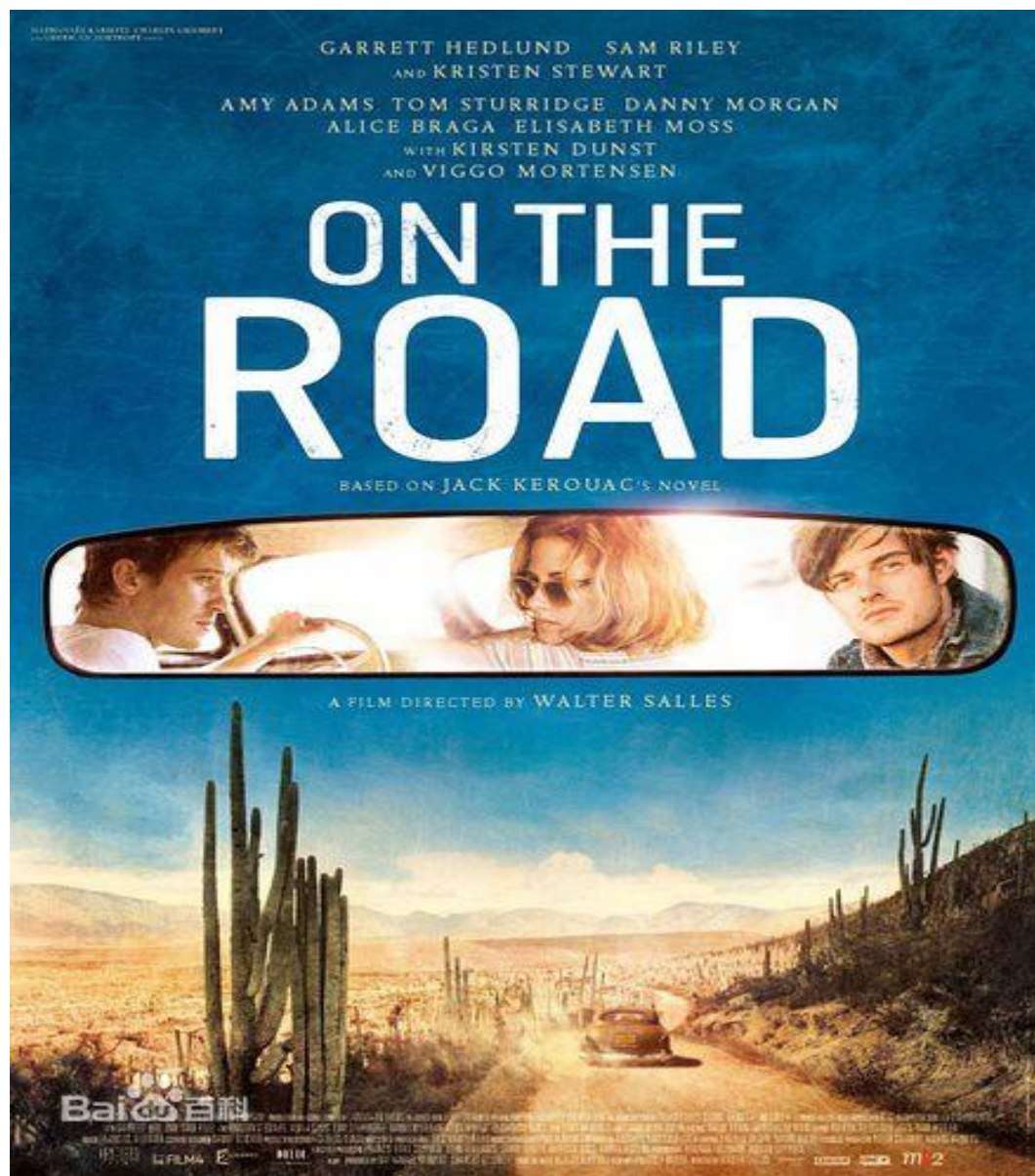
2 YY Live 安全运维体系建设实践

➔ **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





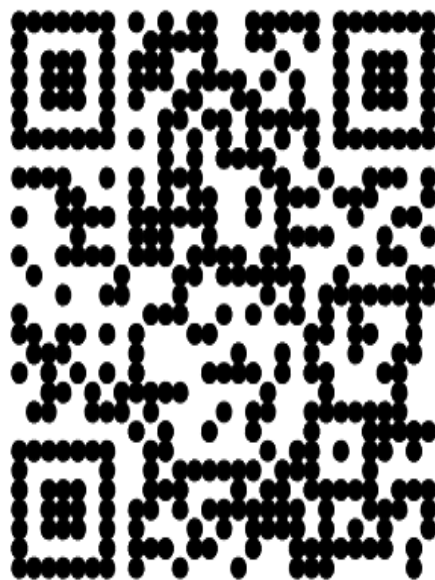
QA

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