云WAF与大数据实时分析实践

携程技术保障中心资深安全工程师　　张亮

2016携程信息安全沙龙

关于我

个人	• 张亮 • 携程信息安全部
方向	• WEB安全、网络安全、安全产品开发

大纲

背景	闭环设计	构建实践	大数据分析	以后的路
• 痛点 • 难点 • 方案	• 规则源 • 部署 • 日志	• 架构 • 特色 • 现状 • 可视化	• 前置分析 • 接口提供 • 后置学习	• 自动化 • 计划

背景

- 痛点

业务安全需求	• 恶意IP封禁 • 恶意用户封禁 • ..
应用安全防护	• SQL注入 • XSS跨站 • LFI、RCE • ..
0day应急响应	• 精确拦截 • 无缝发布 • 秒级生效

背景

- 痛点

硬件WAF

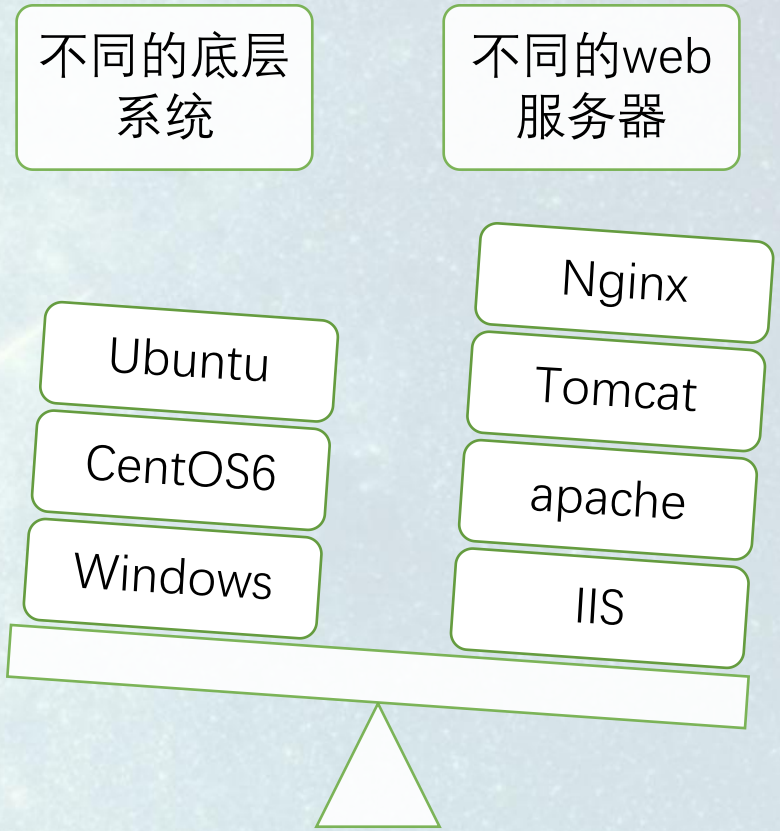
- 带宽、效率瓶颈
- 成本高昂
- 不适合分布式多机房
- s2-032之类的0day或应急很多商业WAF都不支持，并且响应更新慢

商业云WAF

- 规则定制难
- 业务线长难以全部迁移

背景

- 难点
- 10种左右的系统版本
- 5种左右的web容器
- N种不同的编码语言



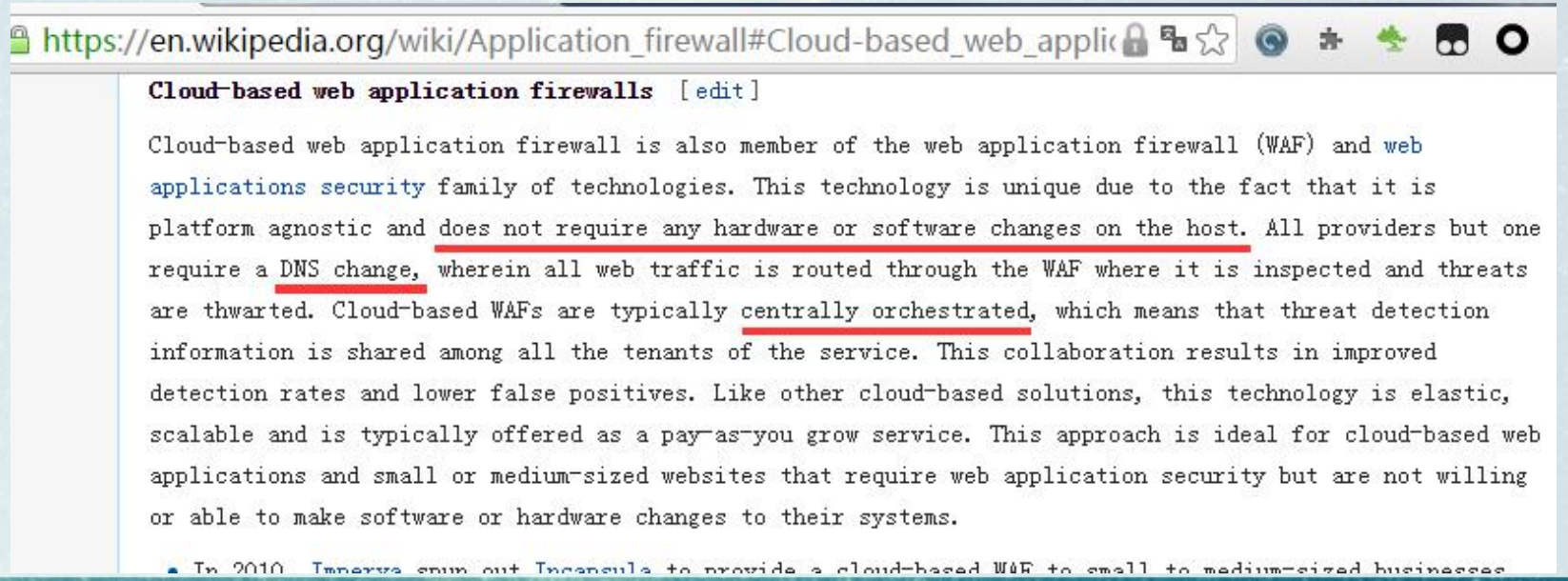
背景

- 优势

✓集中式平台，客户端无需任何改变

✓仅需要DNS解析指向

✓检测信息共享


https://en.wikipedia.org/wiki/Application_firewall#Cloud-based_web_appli

Cloud-based web application firewalls [edit]

Cloud-based web application firewall is also member of the web application firewall (WAF) and web applications security family of technologies. This technology is unique due to the fact that it is platform agnostic and does not require any hardware or software changes on the host. All providers but one require a DNS change, wherein all web traffic is routed through the WAF where it is inspected and threats are thwarted. Cloud-based WAFs are typically centrally orchestrated, which means that threat detection information is shared among all the tenants of the service. This collaboration results in improved detection rates and lower false positives. Like other cloud-based solutions, this technology is elastic, scalable and is typically offered as a pay-as-you grow service. This approach is ideal for cloud-based web applications and small or medium-sized websites that require web application security but are not willing or able to make software or hardware changes to their systems.

闭环设计

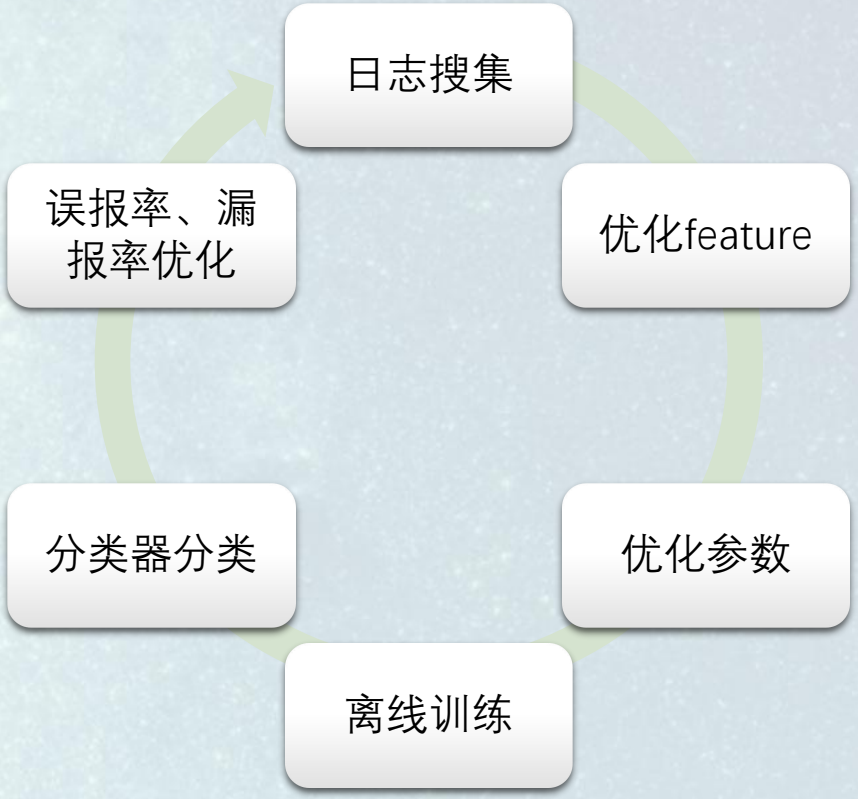
- 规则源
- 外部搜集，内部整理
- 通过日志、流量运用规则做离线计算
- 将实时计算的结果进行分析
- 将误报率低、漏报率低的规则策略发至线上

闭环设计

- 部署
  - 结合nginx，一行配置，无缝开启waf
  - 结合ngx_lua，luajit，实现核心高速检测逻辑
  - 结合Load Balance，低成本部署产生高性能
  - REST API用于管理

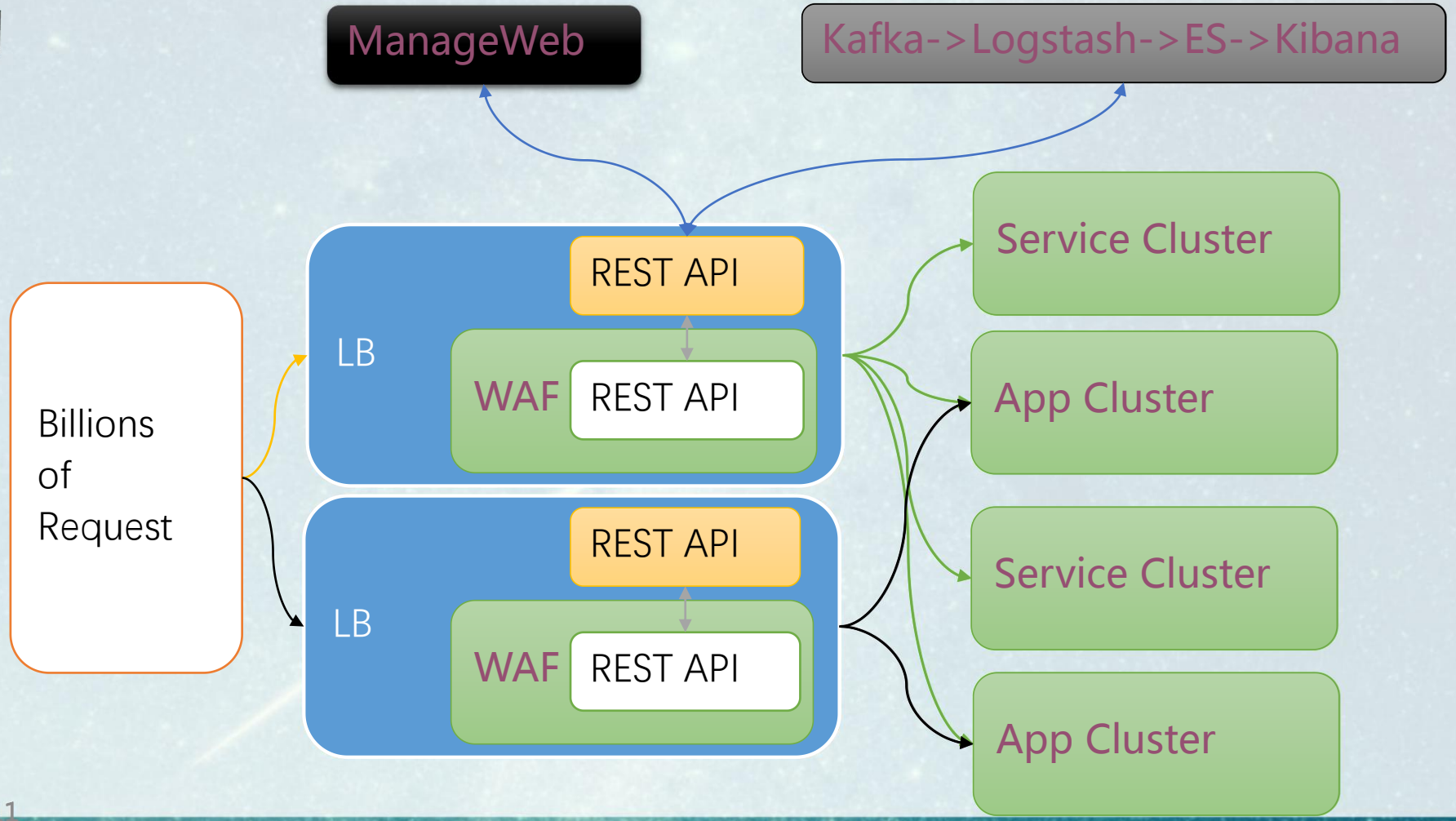
闭环设计

- 日志处理
  - Supervised Learning
  - 误报率、漏报率
  - 机器学习为辅、人工为主



构建实践

- 架构


ManageWeb
Kafka->Logstash->ES->Kibana
Billions of Request
LB
REST API
WAF
REST API
LB
REST API
WAF
REST API
Service Cluster
App Cluster
Service Cluster
App Cluster

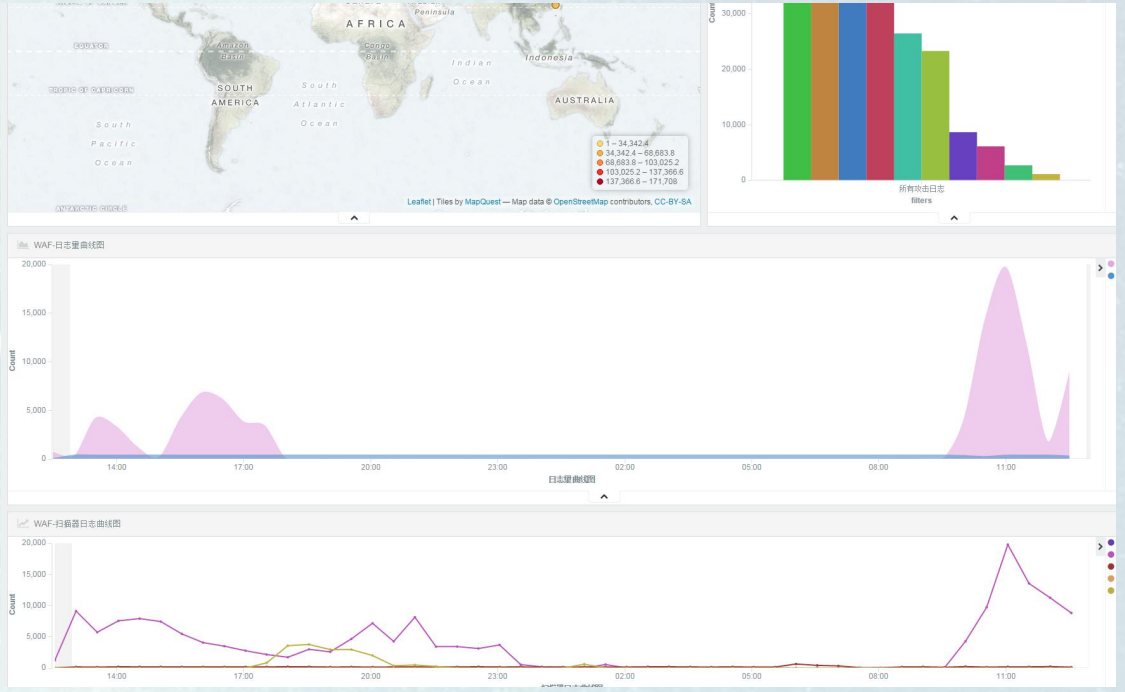
构建实践

- 特色

- 结合LB，对HTTPS友好
- 快速部署、规则策略秒级生效
- 支持人工bypass、自动bypass
- 引擎一键进入拦截、检测、关闭模式
- 秒级statics统计、状态记录
- 预留REST API接口，配合风控、反爬
- 规则来源于Storm离线计算优化后

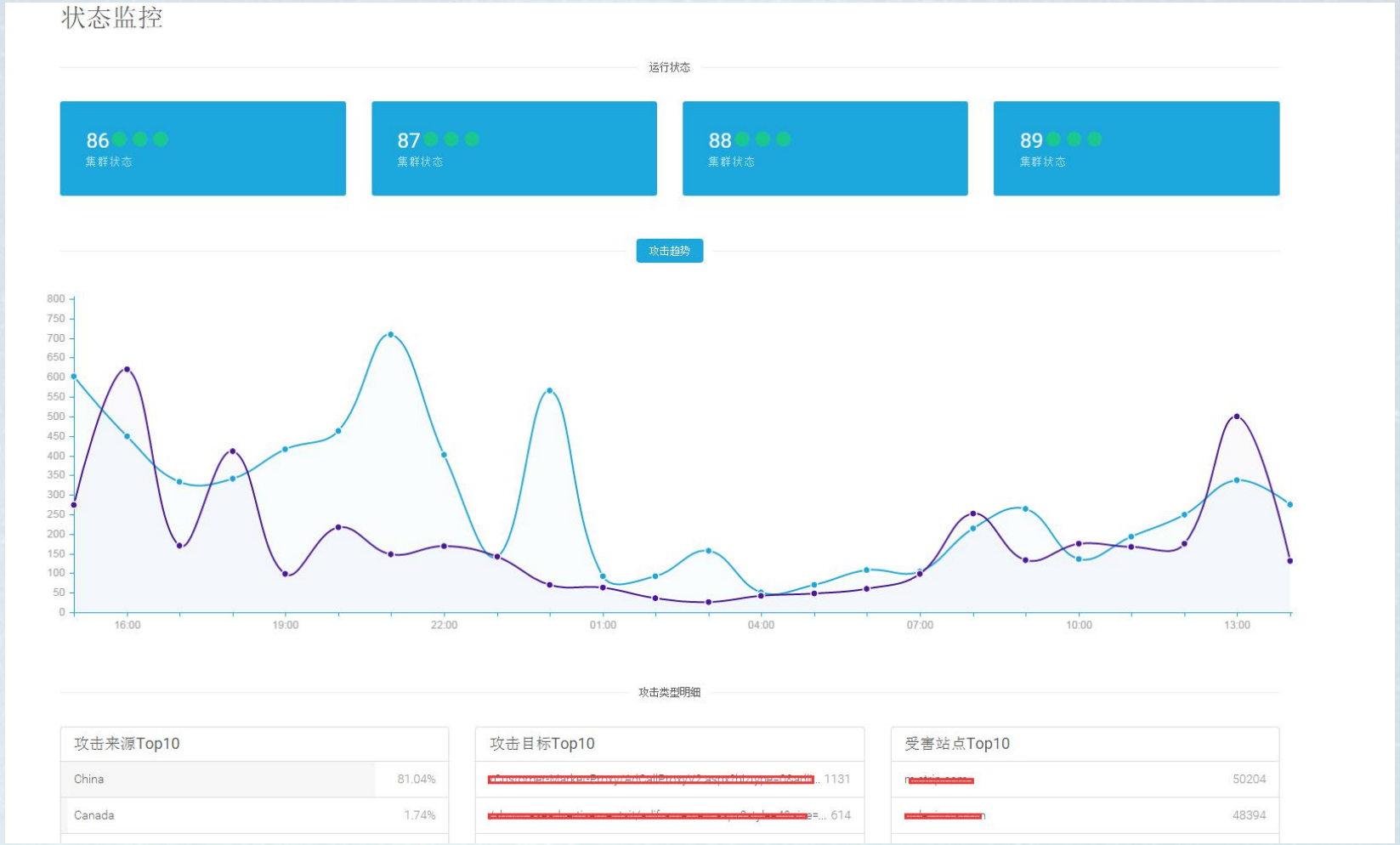
构建实践

- 现状
  - 每天处理十亿级请求，每次耗时微秒级
  - 每天拦截百万次攻击，误报率千万分之一
  - 保护成千上万的应用



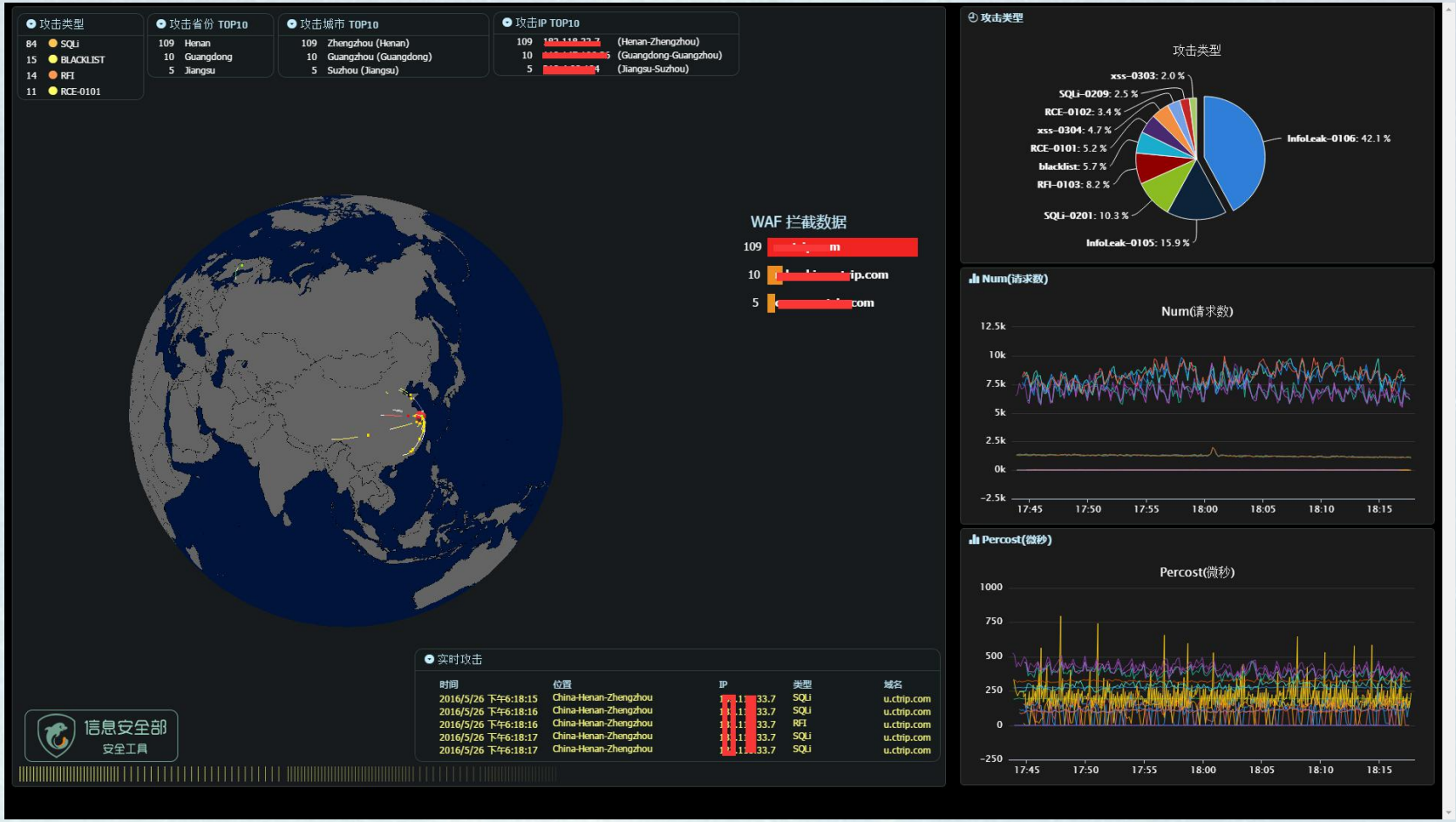
构建实践

- 现状


状态监控
运行状态
86
集群状态
87
集群状态
88
集群状态
89
集群状态
攻击趋势
800
750
700
650
600
550
500
450
400
350
300
250
200
150
100
50
0
16:00
19:00
22:00
01:00
04:00
07:00
10:00
13:00
攻击类型明细
攻击来源Top10
China
81.04%
Canada
1.74%
攻击目标Top10
1131
614
受害站点Top10
50204
48394

构建实践

- 现状


攻击类型
84 SQLi
15 BLACKLIST
14 RFI
11 RCE-0101
攻击省份 TOP10
109 Henan
10 Guangdong
5 Jiangsu
攻击城市 TOP10
109 Zhengzhou (Henan)
10 Guangzhou (Guangdong)
5 Suzhou (Jiangsu)
攻击IP TOP10
109 (Henan-Zhengzhou)
10 (Guangdong-Guangzhou)
5 (Jiangsu-Suzhou)
WAF 拦截数据
109
10
5
攻击类型
xss-0303: 2.0 %
SQLi-0209: 2.5 %
RCE-0102: 3.4 %
xss-0304: 4.7 %
RCE-0101: 5.2 %
blacklist: 5.7 %
RFI-0103: 8.2 %
SQLi-0201: 10.3 %
InfoLeak-0105: 15.9 %
InfoLeak-0106: 42.1 %
Num(请求数)
12.5k
10k
7.5k
5k
2.5k
0k
-2.5k
17:45
17:50
17:55
18:00
18:05
18:10
18:15
Percost(微秒)
1000
750
500
250
0
-250
实时攻击
时间 位置 IP 类型 域名
2016/5/26 下午6:18:15 China-Henan-Zhengzhou SQLi u.ctrip.com
2016/5/26 下午6:18:16 China-Henan-Zhengzhou SQLi u.ctrip.com
2016/5/26 下午6:18:16 China-Henan-Zhengzhou RFI u.ctrip.com
2016/5/26 下午6:18:17 China-Henan-Zhengzhou SQLi u.ctrip.com
2016/5/26 下午6:18:17 China-Henan-Zhengzhou SQLi u.ctrip.com
信息安全部
安全工具

大数据分析

- 前置分析
- 基于STORM对流量进行实时计算
- 更宽泛的规则策略
- 实时分数计算
- 可自动或手动与WAF联动

☑ 时间 ☑ 攻击源 ☑ 攻击目标 ☑ 全部访问的域名 ☐ 攻击时带的ua ☐ 全部访问的ua ☑ 归属地 ☑ 分数 ☑ 攻击类型 ☑ 攻击次数/访问总次数

时间	攻击源	攻击目标	全部访问的域名	归属地	分数	攻击类型	攻击次数/访问总次数	深度分析	操作
开始时间：2016-04-22 07:43:01 结束时间：2016-04-22 07:48:01	[redacted]	[redacted](2028)	[redacted](2309)	河南 郑州	6451	SQLi-2008(454) SQLi-2005(394) SQLi-2009(182) XSS-3001(116) RFI-1004(109)	2309/2028	攻击详情 访问详情	确认 误报 拦截IP 加入黑名单库 加入白名单库
开始时间：2016-04-22 07:58:01 结束时间：2016-04-22 08:03:01	[redacted]	[redacted](140)	[redacted](101)	北京 北京	615	RFI-1004(40) SQLi-2005(23) SQLi-2010(22) SQLi-2008(21) SQLi-2002(20)	101/140	攻击详情 访问详情	确认 误报 拦截IP 加入黑名单库 加入白名单库
开始时间：2016-04-22 07:58:01 结束时间：2016-04-22 08:03:01	[redacted]	[redacted](10)	[redacted](2)	河南 郑州	39	SQLi-2008(2) SQLi-2009(2) SQLi-2010(2) RCE-1001(1) SQLi-2003(1)	2/10	攻击详情 访问详情	确认 误报 拦截IP 加入黑名单库 加入白名单库
开始时间：2016-04-22 07:53:01	[redacted]	[redacted](298)	[redacted](366)	北京 北京	1155	SQLi-2008(46) SQLi-2005(39)	366/298	攻击详情 访问详情	确认 误报

大数据分析

- 接口提供
- RESTful API接口
- 支持动态规则，拦截基于IP、UA、UID等策略组合
- 支持静态规则，拦截基于参数、内容的web攻击拦截
- 支持一键开启关闭WAF、一键切换拦截、检测模式、一键bypass
- 支持状态查询、规则下发、规则更新等功能

大数据分析

- 后置学习
- 基于SPARK stream、SPARK mllib
- 针对WAF日志进行解析、分析、统计、学习
- 自动分析每日上百万日志中误报条目
- 人工确认结果作为训练数据输入

以后的路

- 自动化
- 无人值守？
- 自动化运维？
- 自动加白？
- 自动识别可疑访问？

未来的路

- 计划
  - High performance
  - More feature
  - More api

未来的路

携程云安全-security.ctrip.com

- ✓免费
- ✓200+企业用户入驻

THANKS

Q&A