

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

- 痛点
- 难点
- 方案

闭环设计

- 规则源
- 部署
- 日志

构建实践

- 架构
- 特色
- 现状
- 可视化

大数据分析

- 前置分析
- 接口提供
- 后置学习

以后的路

- 自动化
- 计划



背景

• 痛点





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

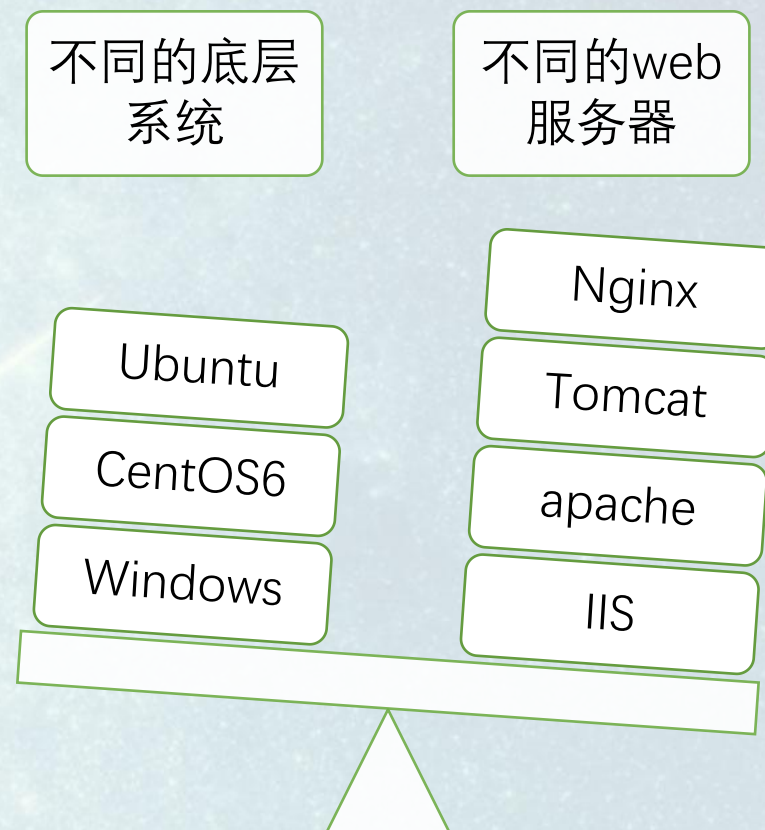
- 规则定制难
- 业务线长难以全部迁移



背景

• 难点

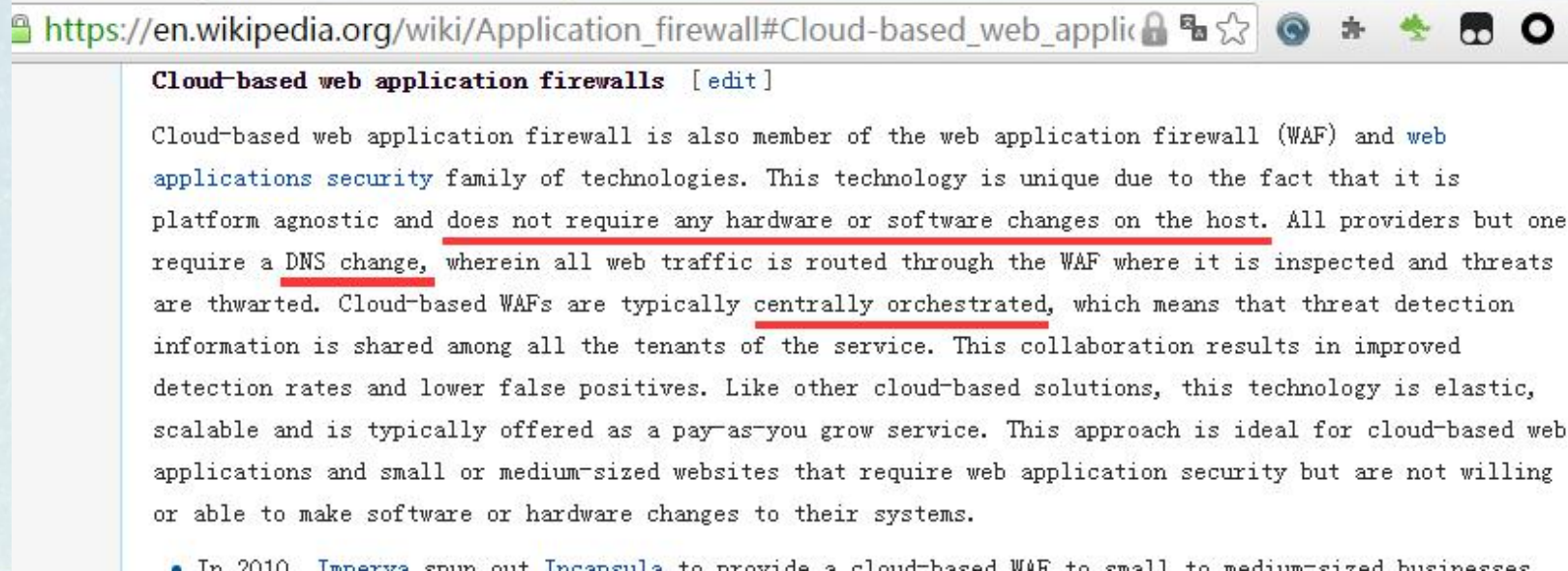
- 10种左右的系统版本
- 5种左右的web容器
- N种不同的编码语言





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





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

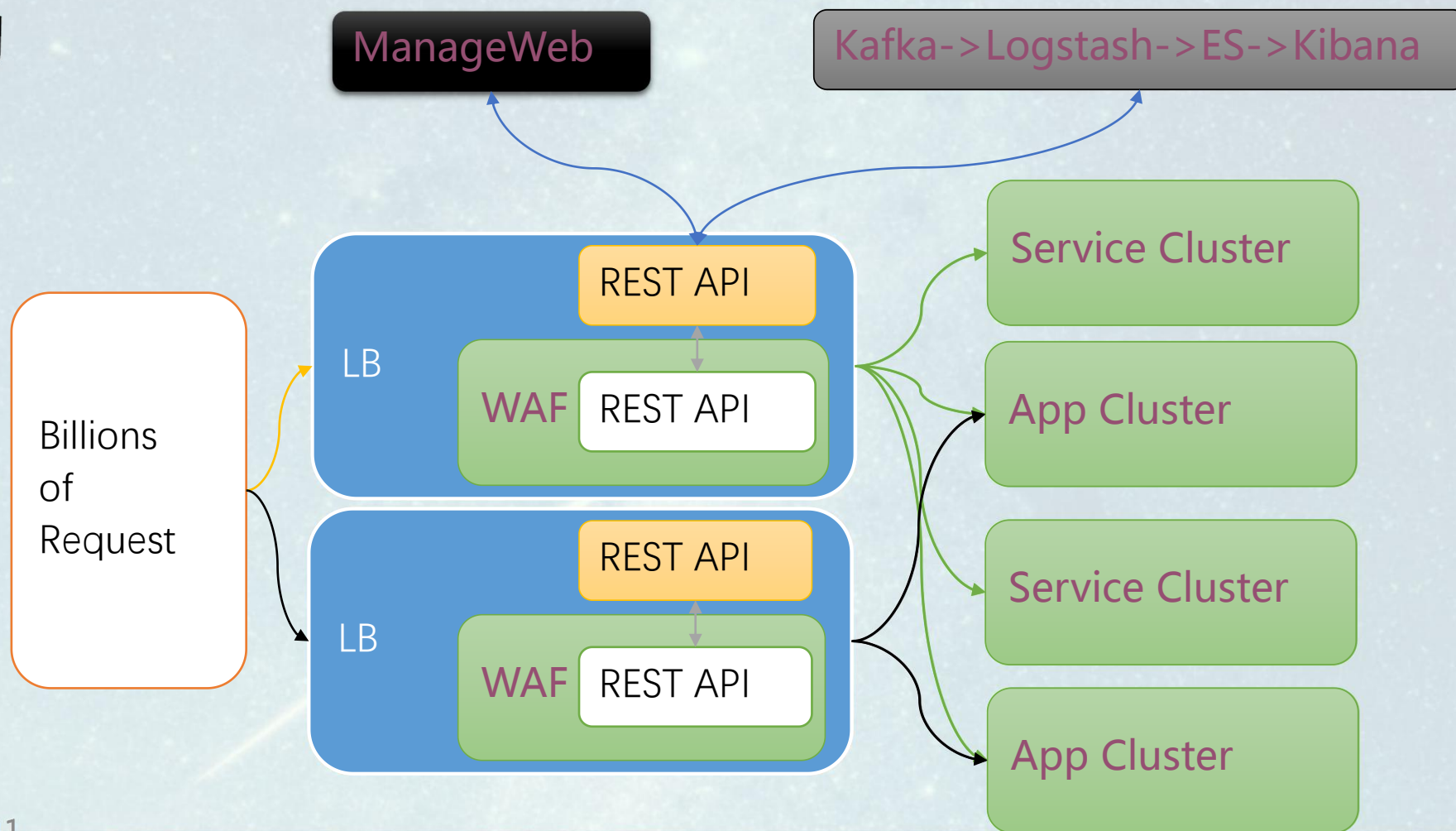
- 日志处理
 - Supervised Learning
 - 误报率、漏报率
 - 机器学习为辅、人工为主





构建实践

• 架构





构建实践

• 特色

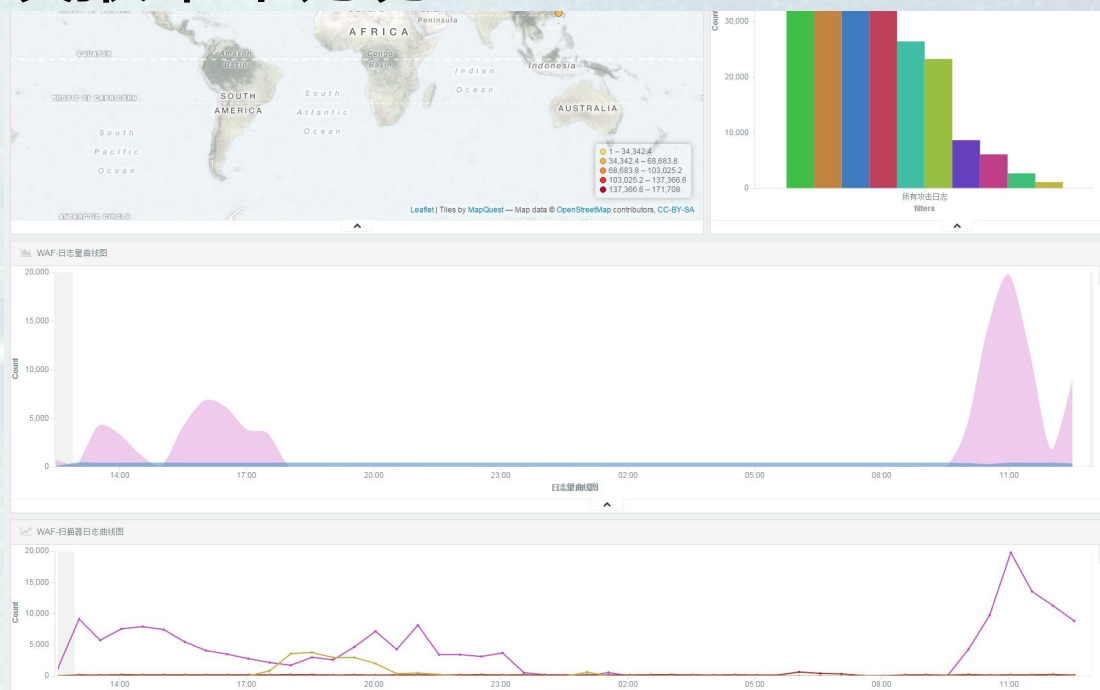




构建实践

• 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

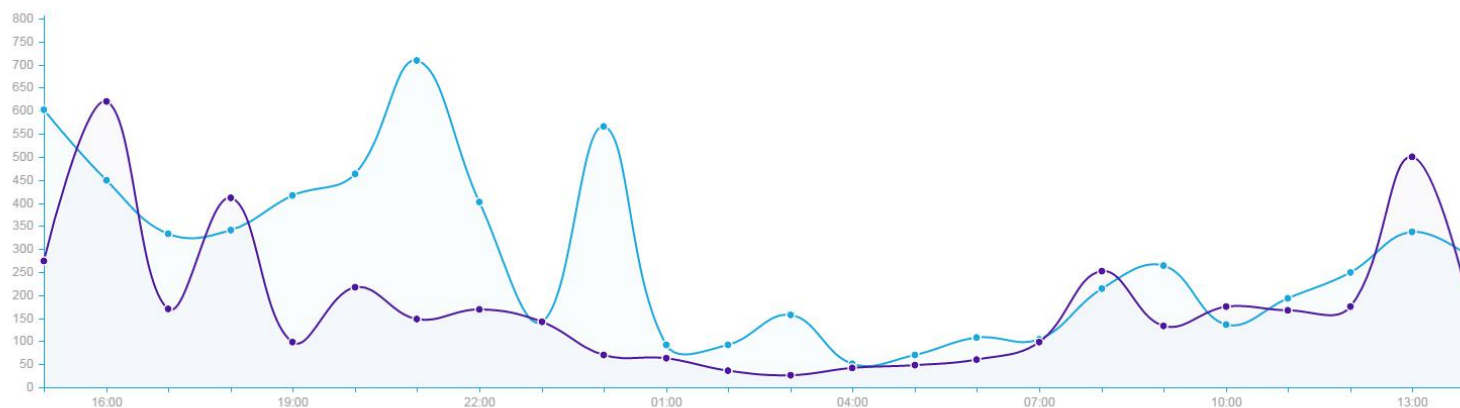
86 集群状态

87 集群状态

88 集群状态

89 集群状态

攻击趋势



攻击类型明细

攻击来源Top10

China	81.04%
Canada	1.74%

攻击目标Top10

1131
614

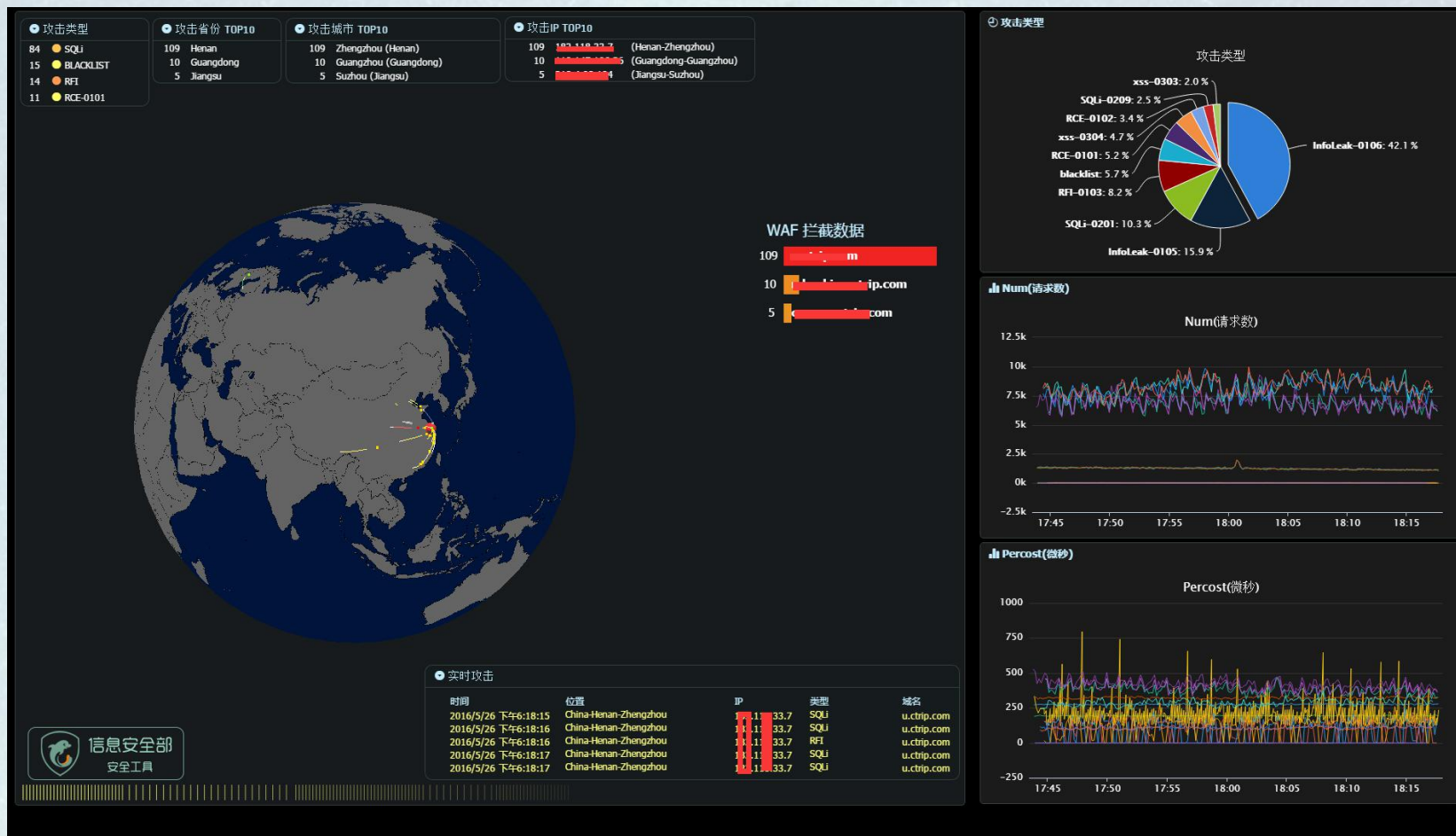
受害站点Top10

50204
48394



构建实践

• 现状





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	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						河南 郑州	6451	SQLI-2008(454) SQLI-2005(394) SQLI-2009(182) XSS-3001(116) RFI-1004(100)	2309/2028	攻击详情 访问详情	确认 误报 拦截IP 加入黑名单 加入白名单
开始时间: 2016-04-22 07:58:01 结束时间: 2016-04-22 08:03:01						北京 北京	615	RFI-1004(40) SQLI-2005(23) SQLI-2010(22) SQLI-2008(21) SQLI-2007(20)	101/140	攻击详情 访问详情	确认 误报 拦截IP 加入黑名单 加入白名单
开始时间: 2016-04-22 07:58:01 结束时间: 2016-04-22 08:03:01						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 加入白名单
开始时间: 2016-04-22 07:53:01						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

规则策略
版本发布

线上规则版本: 3.06 线上名单版本: 1.29 规则: [redacted] [上传]

规则ID	规则描述	服务器名	服务器IP	规则版本	名单版本	工作状态	BYPASS	24HOUR	上次E
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未
[redacted]	[redacted]	[redacted]	[redacted]	✓ 3.06	✓ 1.29	拦截模式	未开启	0	从未

1条 - 10条 / 当前12条记录, 总计12条记录



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

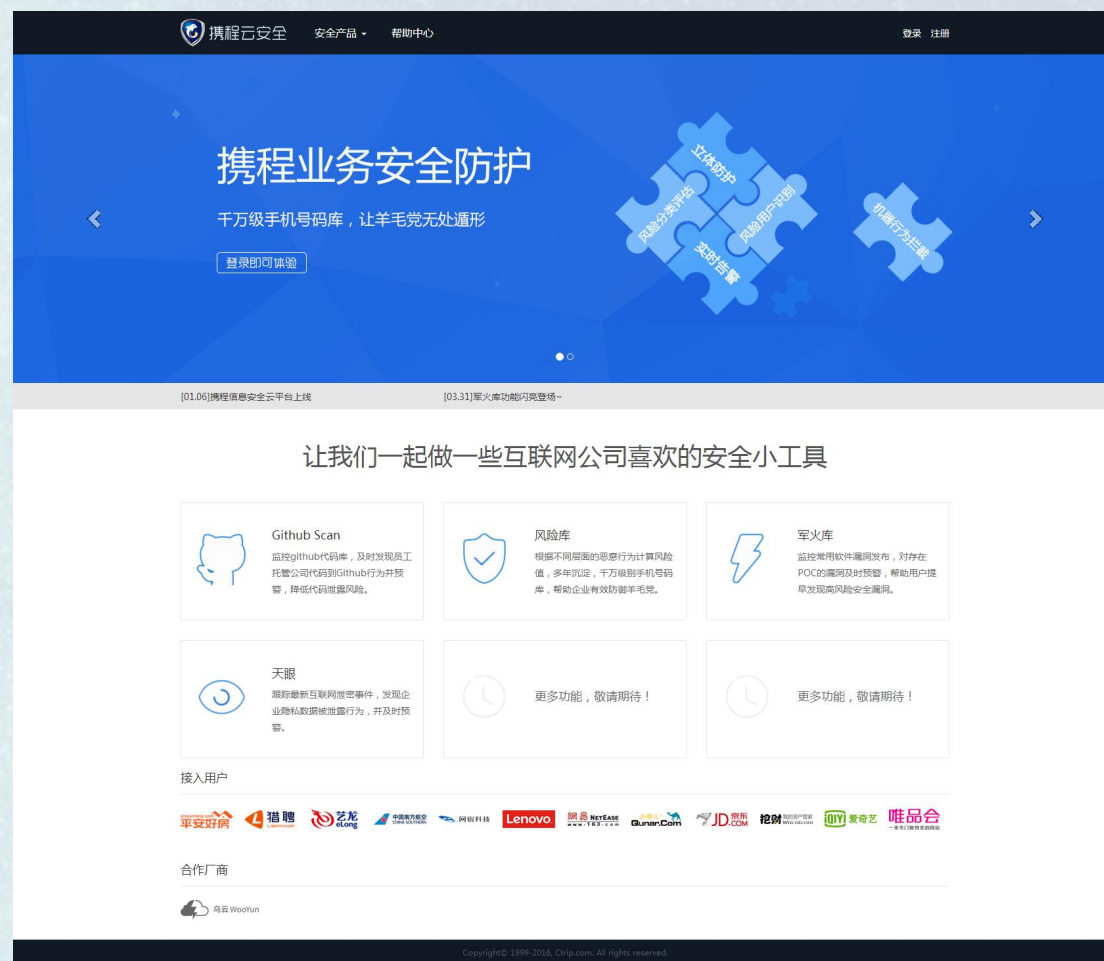


未来的路

携程云安全-security.ctrip.com

✓免费

✓200+企业用户入驻



THANKS
Q&A