饿了么

美好生活 共享安全

饿了么第一届信息安全峰会

企业安全技术体系建设与实践

拉扎斯网络科技（上海）有限公司
Rajax Network & Tehnology Co

关于我

胡珀 ， lake2

- 2007年加入腾讯安全平台部
- 腾讯T4安全专家，目前负责应用运维安全
- Web漏洞扫描器、恶意网址检测系统、主机安全Agent建设和运营
- 安全事件响应、渗透测试、安全培训、安全评估、安全规范
- 腾讯安全应急响应中心（TSRC）与威胁情报奖励计划
- 移动安全 & 智能设备安全

关于腾讯

互联网之王，囊括几乎所有的互联网业务模式，安全上是巨大挑战

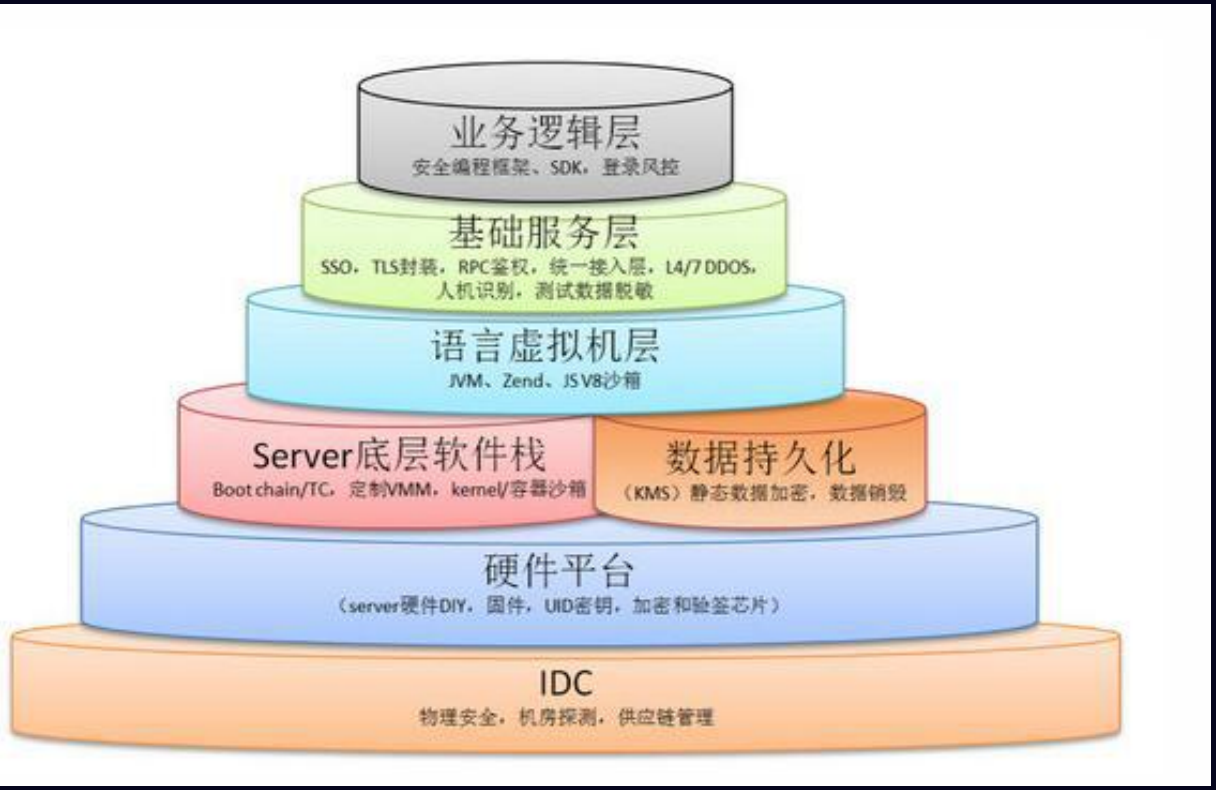
安全的三个阶段

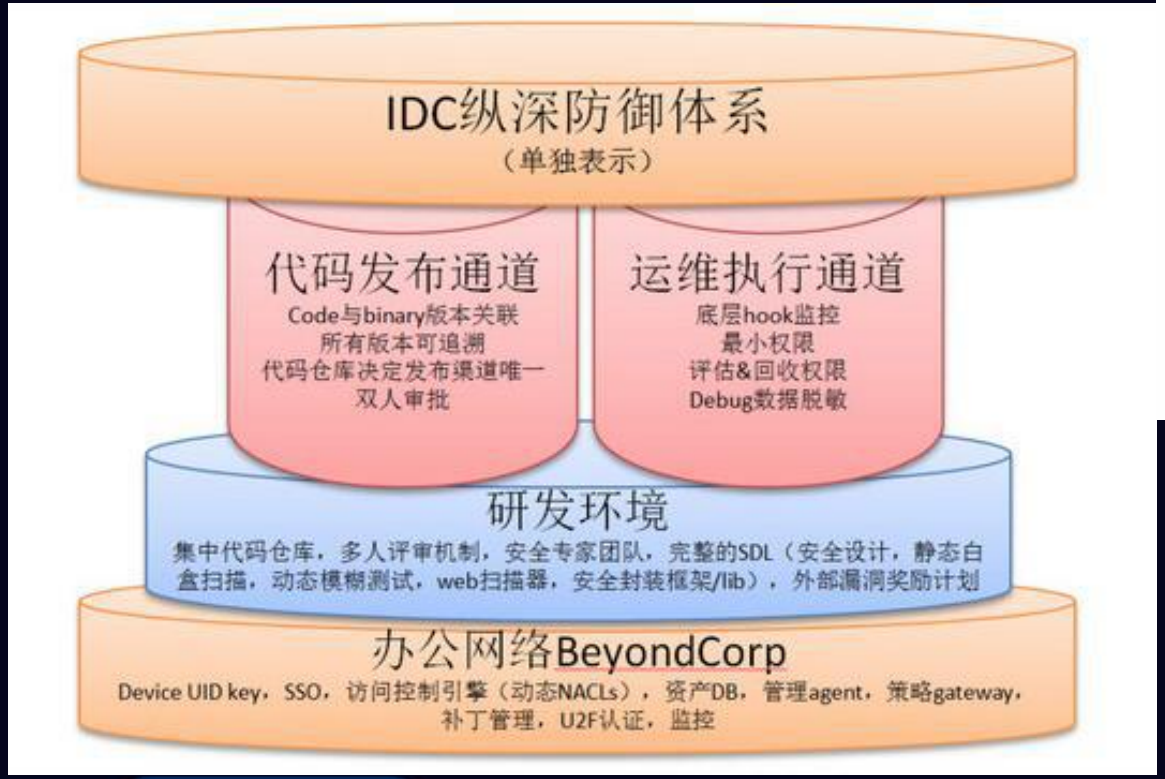
救火队 -> 全面保障业务发展 -> 业务的核心竞争力

安全生命周期（SDL）


Training
Requirements
Design
Implementation
Verification
Release
Response
安全技术培训
安全意识培训
安全规范
安全需求建立
质量标准建立
风险识别
安全设计
攻击面分析
威胁建模
提供安全开发工具
安全开发规范和最佳实践
安全API
代码审计
渗透测试
应急响应方案
上线前集成环境安全检查
安全运维规范
应急响应执行
人工巡查
漏洞扫描系统
安全情报系统

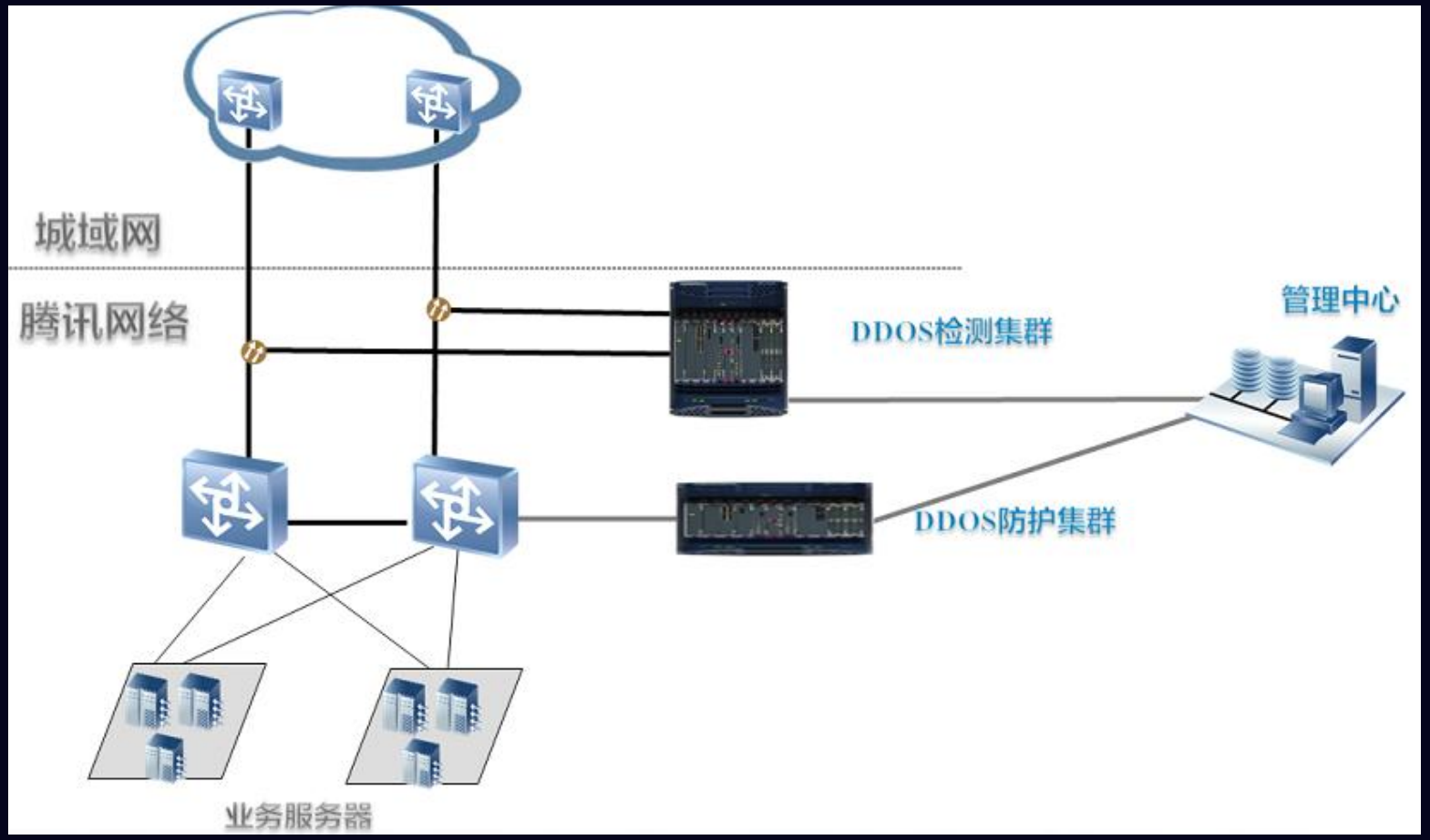
谷歌基础设施安全





学习谷歌先进经验

DDoS攻击防护

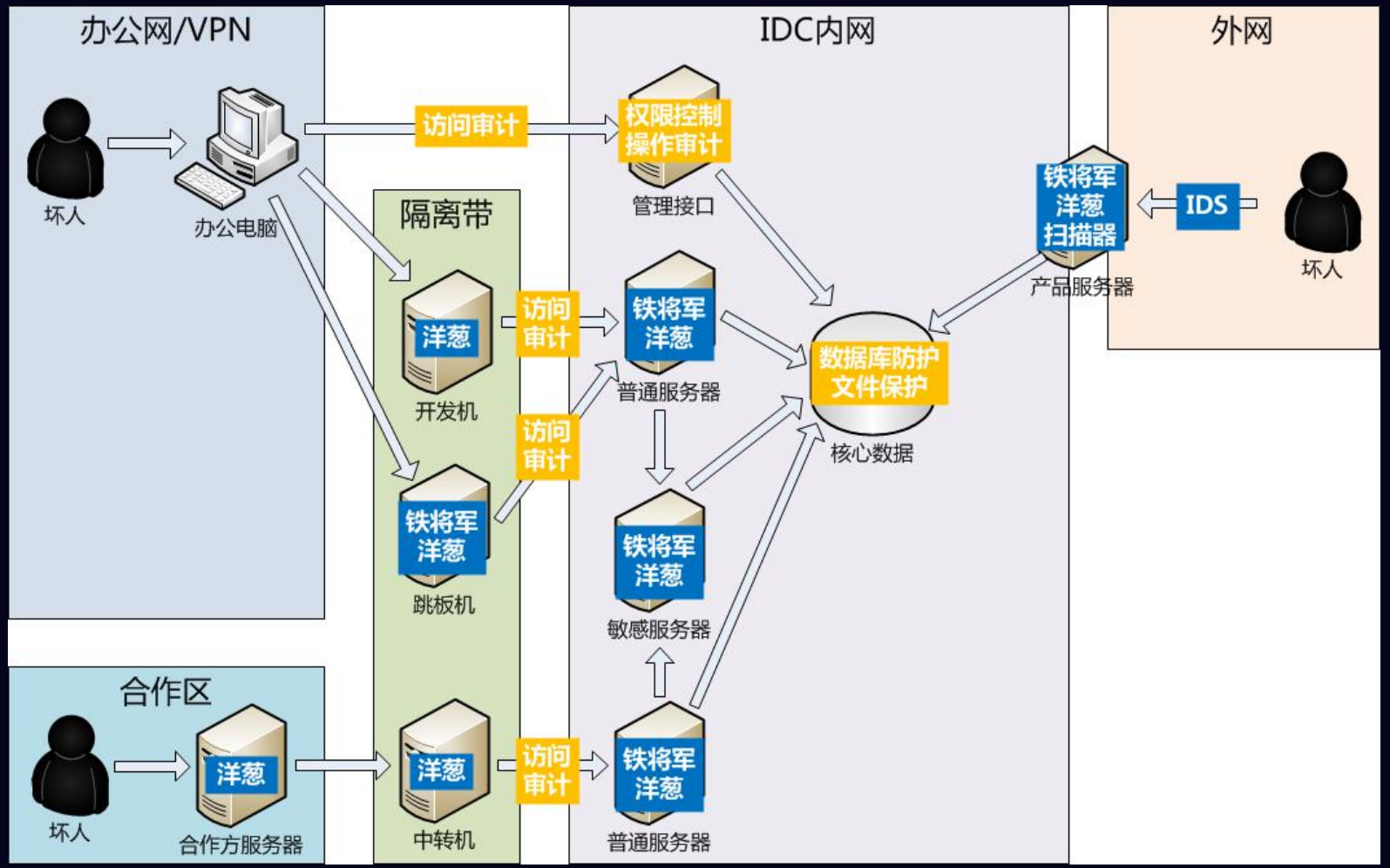


腾讯云

大禹BGP（BGPAntiDDoS）高防是腾讯云针对游戏、金融、网站等用户遭受大流量DDoS攻击时服务不可用的情况推出的增值服务。高达300G的防护服务和多达21线的BGP线路，让您的业务不再畏惧DDoS攻击的挑战，同时拥有极速的访问体验。

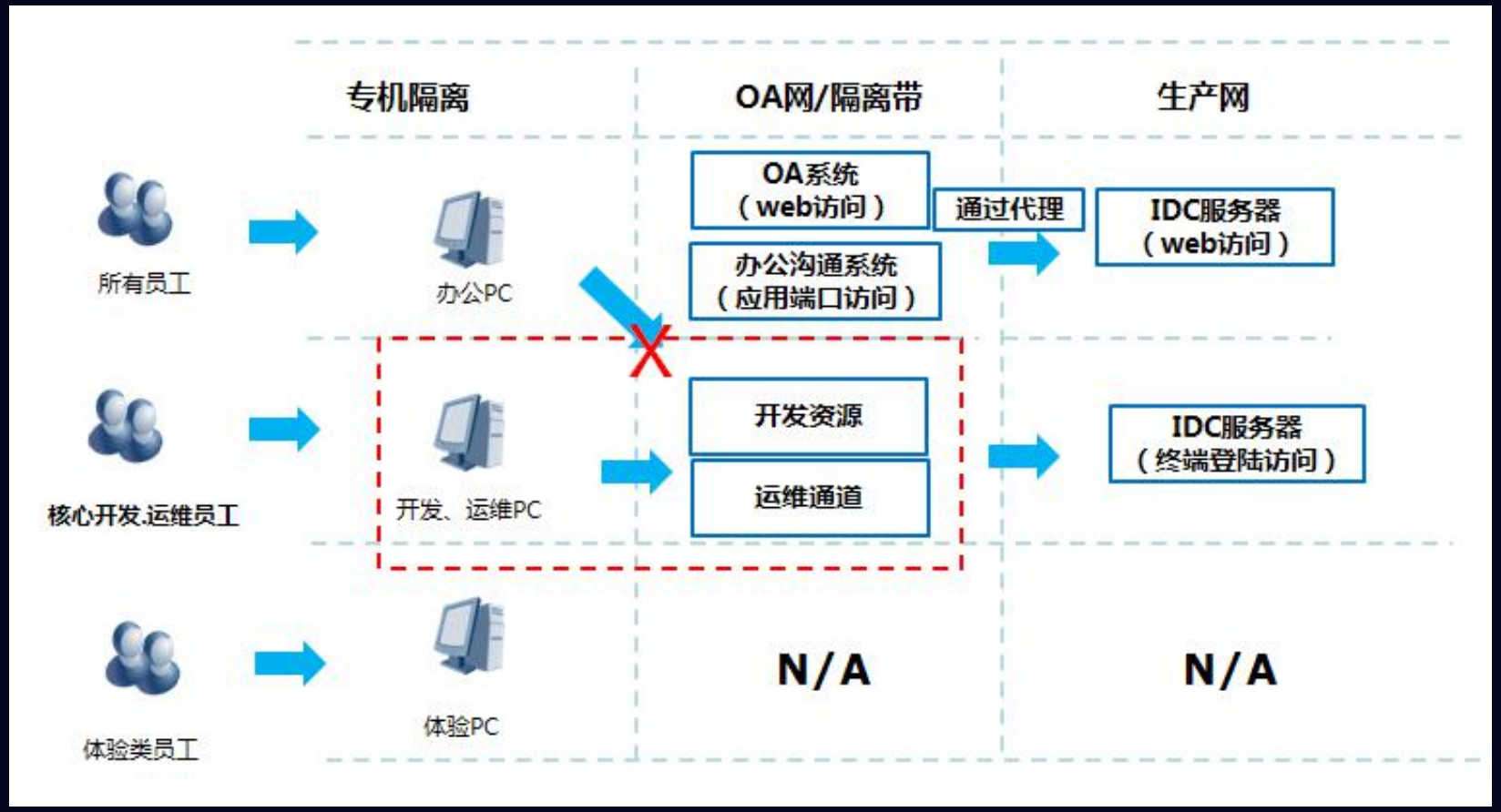
全国分布式防护
近源清洗 – 与云堤合作/终端预研中
最大防护流量 600+Gbps
常见DDoS攻击
10000+ 次攻击每月
响应时间小于10s
For 腾讯云•大禹/知道创宇

Anti-APT：生产环境安全



缩小攻击面：高危端口管控
划区治理：按业务隔离
纵深防御：入侵行为全过程检测
基线模型：异常检测（UEBA）
终端防御：主机安全Agent
网络防御：流量分析

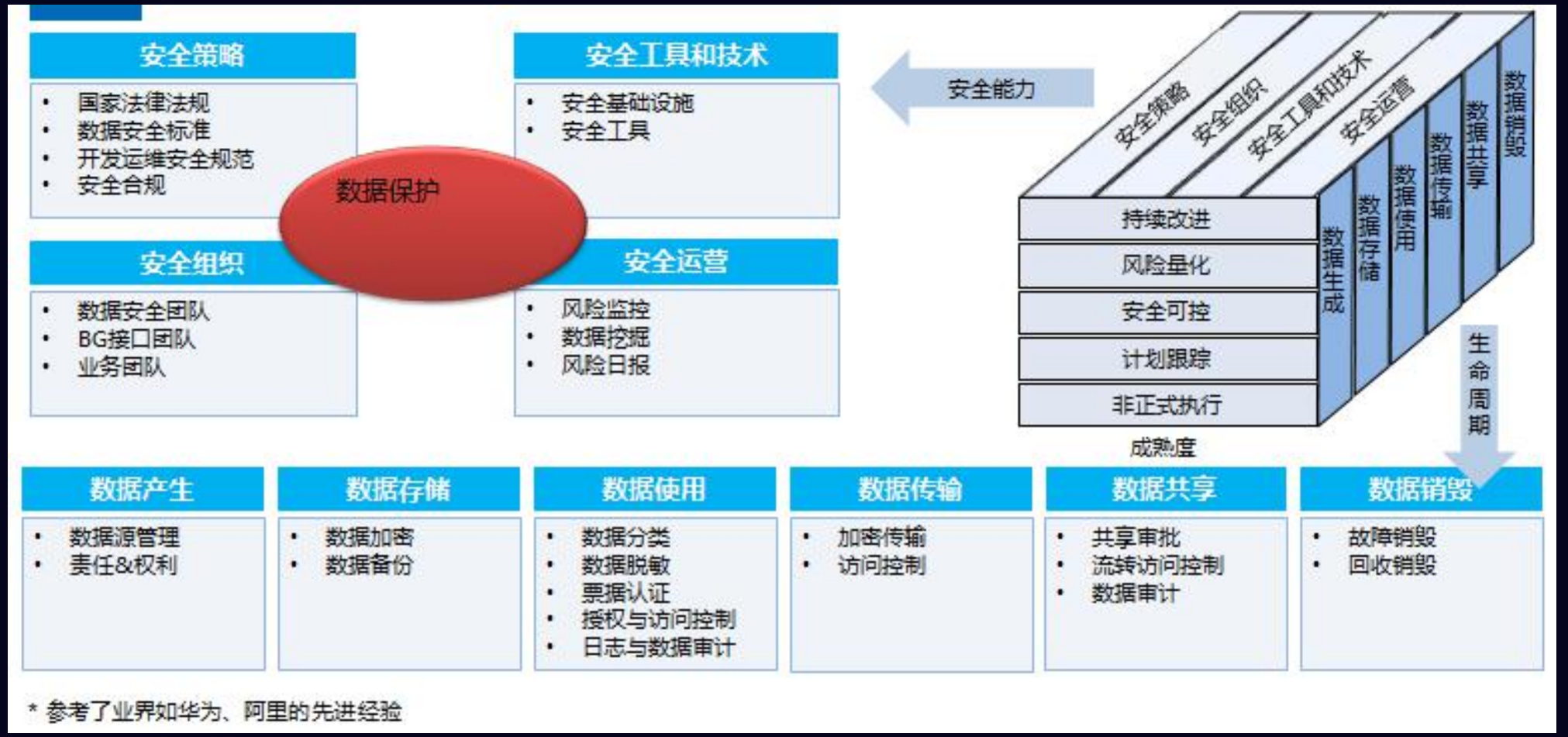
Anti-APT：办公环境安全



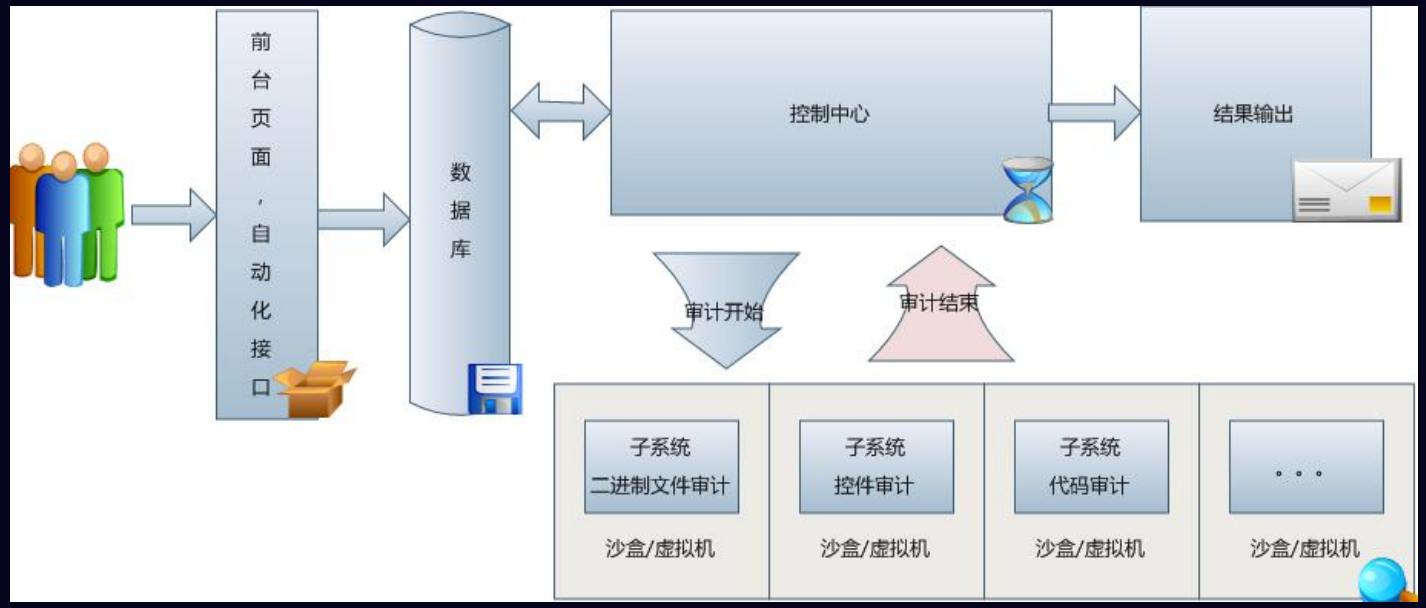
缩小攻击面：HTTP代理上网
划区治理：按网隔离
终端防御：PC/Mobile Agent
基线模型：异常检测
网络防御：流量分析

不要忘了BYOD和办公WiFi ！

数据安全

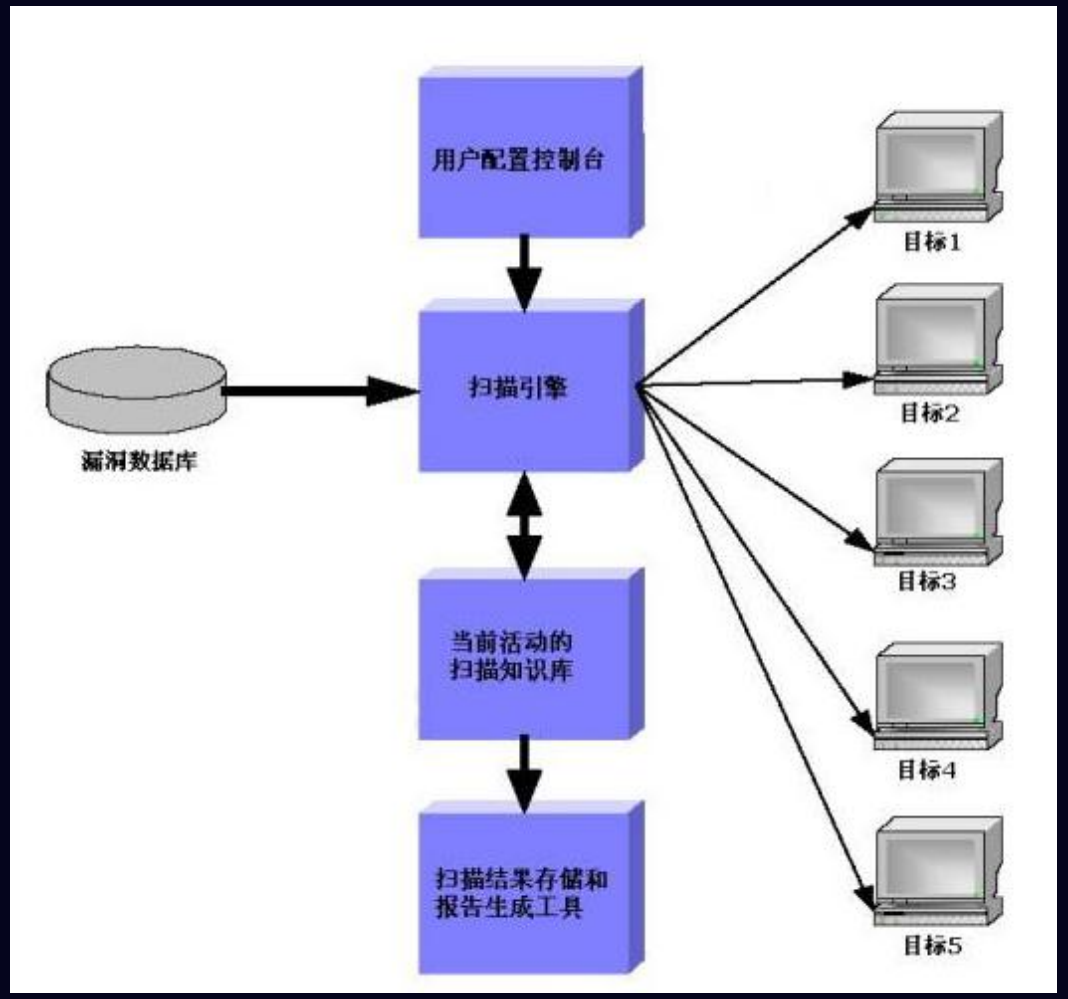

安全策略
国家法律法规
数据安全标准
开发运维安全规范
安全合规
安全工具和技术
安全基础设施
安全工具
数据保护
安全组织
数据安全团队
BG接口团队
业务团队
安全运营
风险监控
数据挖掘
风险日报
安全能力
安全策略
安全组织
安全工具和技术
安全运营
数据销毁
数据共享
数据传输
数据使用
数据存储
数据生成
持续改进
风险量化
安全可控
计划跟踪
非正式执行
成熟度
生命周期
数据产生
数据源管理
责任&权利
数据存储
数据加密
数据备份
数据使用
数据分类
数据脱敏
票据认证
授权与访问控制
日志与数据审计
数据传输
加密传输
访问控制
数据共享
共享审批
流转访问控制
数据审计
数据销毁
故障销毁
回收销毁
* 参考了业界如华为、阿里的先进经验

安全漏洞收敛：终端漏洞



支持PC（Win/Mac）、Mobile（iOS/Android）
静态 + 动态

安全漏洞收敛：服务端漏洞



自研爬虫
插件式
7*24h

红蓝军对抗

模拟黑客从攻击者视角对业务进行渗透，检验安全防护能力

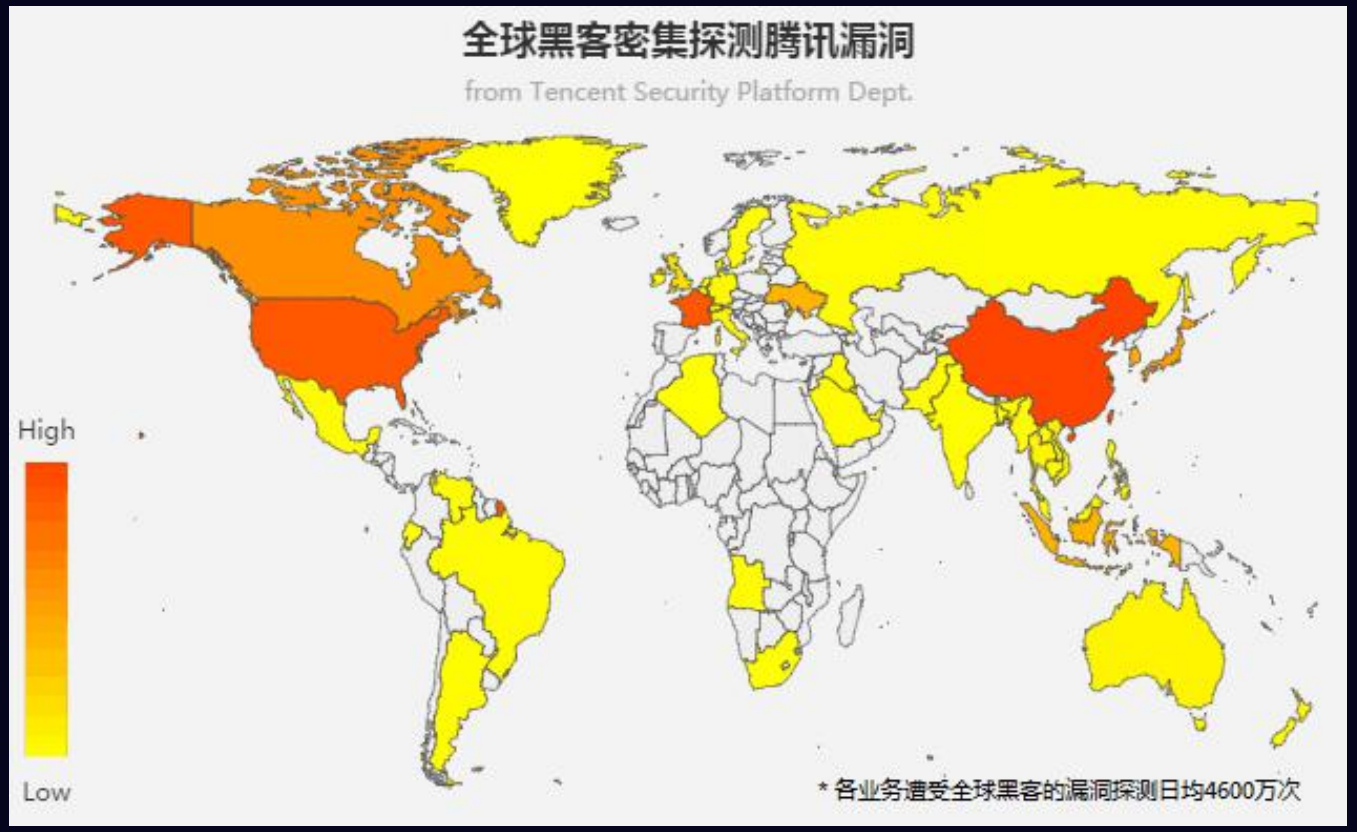
邮件 | 洋葱 区审计项结果表格).xls (15 KB) | 【洋葱 区效果审计】基础检查汇总(lak doc (84 KB) | 【洋葱 区审计】审计过程记录文档(doc

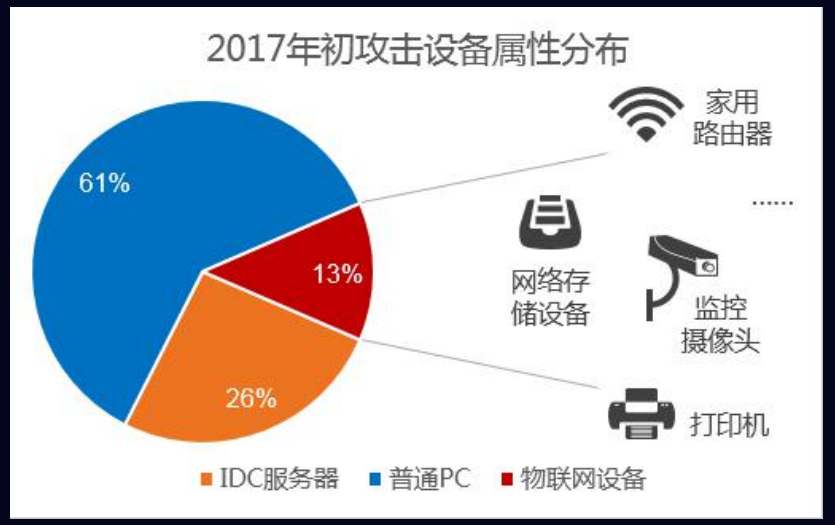
黑客入侵场景检测能力审计（ 实施）

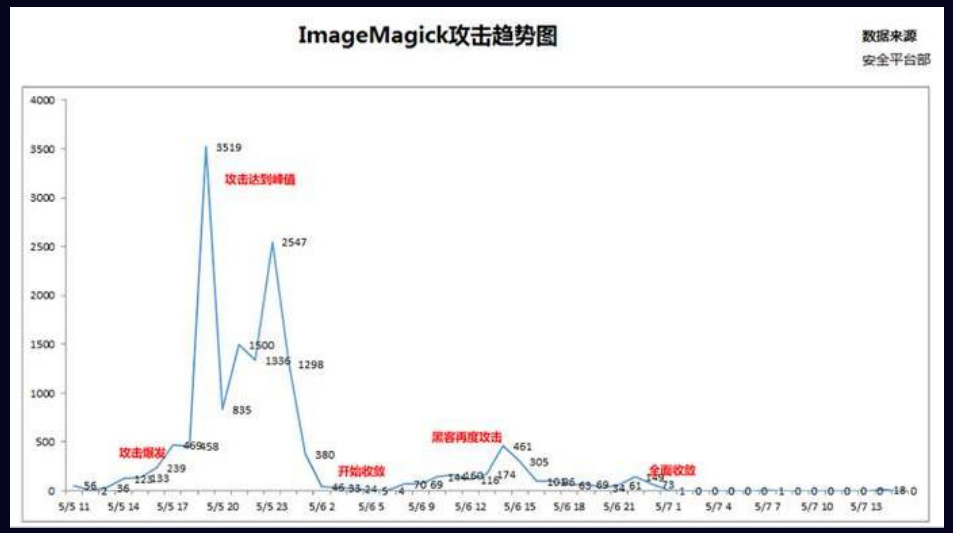
纵向为黑客场景，横向为规则。图例解释：√该项规则生效 ×该项规则无效 O该项规则不关注该行为

场景\规则	描述												结论
上 传		×	O	O	O	O	O	O	O	O	O	O	×	未发现的原因是 的
		O	O	O	O	O	×	O	O	O	O	O	O	非 的命
运行		O	√	O	O	O	O	√	√	O	O	O	√	良好
		O	×	O	O	O	O	×	×	O	O	O	×	
		O	O	O	O	O	O	O	O	O	O	O	×	
内网		O	√	O	O	O	O	O	O	√	O	O	√	良好
	描	O	O	O	×	O	O	O	O	O	O	O	×	不能发现

数据分析


全球黑客密集探测腾讯漏洞
from Tencent Security Platform Dept.
High
Low
* 各业务遭受全球黑客的漏洞探测日均4600万次


2017年初攻击设备属性分布
61%
13%
26%
家用
路由器
.....
网络存
储设备
监控
摄像头
打印机
IDC服务器
普通PC
物联网设备


ImageMagick攻击趋势图
数据来源
安全平台部
攻击爆发
攻击达到峰值
开始收敛
黑客再度攻击
全面收敛

漏洞奖励计划

腾讯安全应急响应中心
Tencent Security Response Center

众包众测，发现漏洞，检验安全防护能力

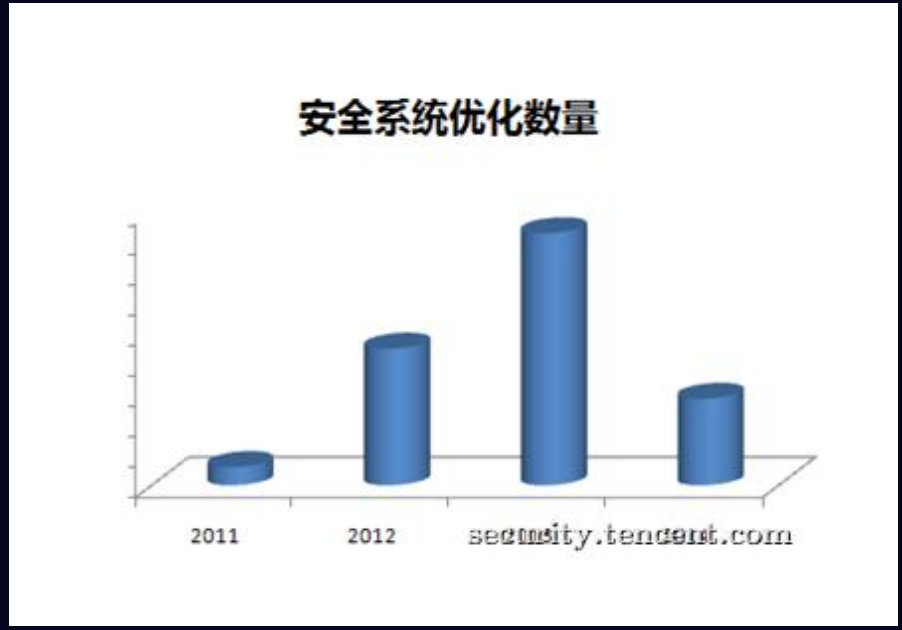
[TPSA15-20] 关于“威胁情报奖励计划（试行）”启动的安全公告

公告编号：TPSA15-20　公告来源：TSRC　发布日期：2015-10-15　分享

腾讯安全应急响应中心（简称TSRC）于2012年5月启动了，在三年多的不断试错和改进中，得到了业界广大安全专家的帮助和支持，大大提高了腾讯产品和业务的安全级别。但我们仍然觉得做得还不够，我们希望再来点改进。

自即日起，TSRC原有的“**安全漏洞奖励计划**”正式升级为“**威胁情报奖励计划**”——TSRC除原有的收集腾讯安全漏洞外，还收集与腾讯相关的任何安全威胁情报，一经确认，即按照威胁情报评分危害级别给予奖励。

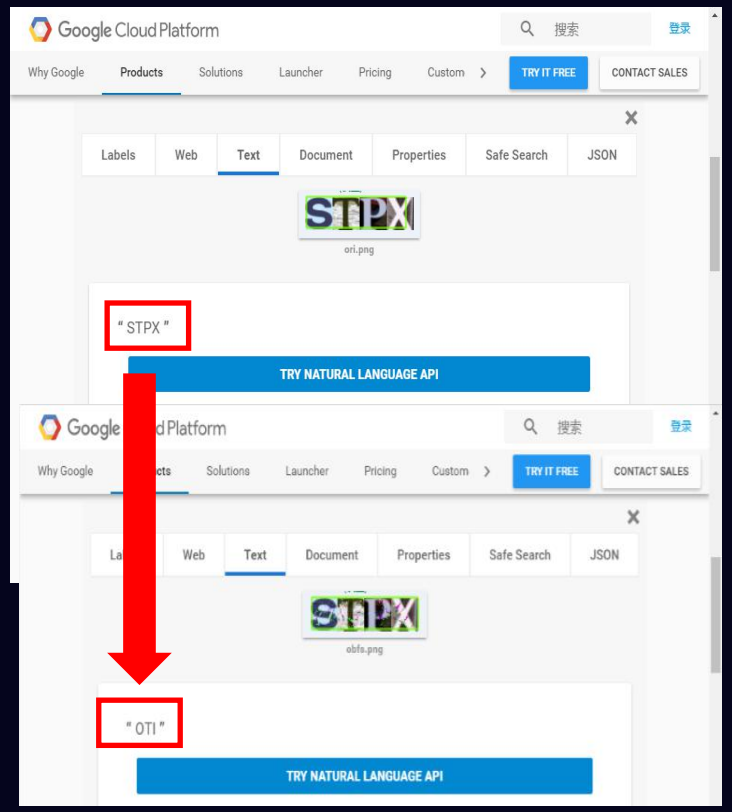
【适用条件】

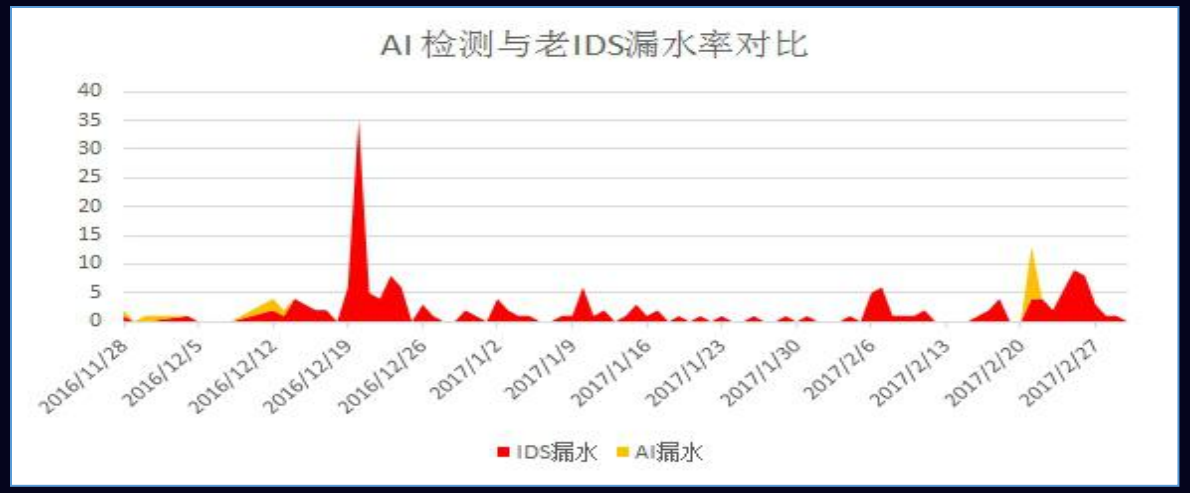


饿了么安全应急响应中心
Eleme Security Response Center

美好生活 共享安全

AI应用与对抗


Google Cloud Platform
搜索
登录
Why Google
Products
Solutions
Launcher
Pricing
Custom
TRY IT FREE
CONTACT SALES
Labels
Web
Text
Document
Properties
Safe Search
JSON
ori.png
" STPX "
TRY NATURAL LANGUAGE API
obfs.png
" OTI "
TRY NATURAL LANGUAGE API


AI 检测与老IDS漏水率对比
40
35
30
25
20
15
10
5
0
2016/11/28
2016/12/5
2016/12/12
2016/12/19
2016/12/26
2017/1/2
2017/1/9
2017/1/16
2017/1/23
2017/1/30
2017/2/6
2017/2/13
2017/2/20
2017/2/27
IDS漏水
AI漏水

饿了么安全应急响应中心
Eleme Security Response Center

腾讯安全应急响应中心
Tencent Security Response Center

THANKS

拉扎斯网络科技（上海）有限公司
Lajax Network & Tehnology Co