
Def 2013
第二届
全国网络与信息安全防护峰会
对话·交流·合作

互联网企业安全体系建设杂谈

宗泽
腾讯安全平台部

写在前面

- 抛砖引玉
- 真的只是“杂谈”

目录

我的企业安全观

安全是业务发展到一定阶段的刚需

做安全比做黑客困难N倍

技术是基础，运营是王道

互联网企业安全的特点

思路 1

安全部门的自身定位

孙子兵法：求其上，得其中；求其中，得其下；求其下，必败。

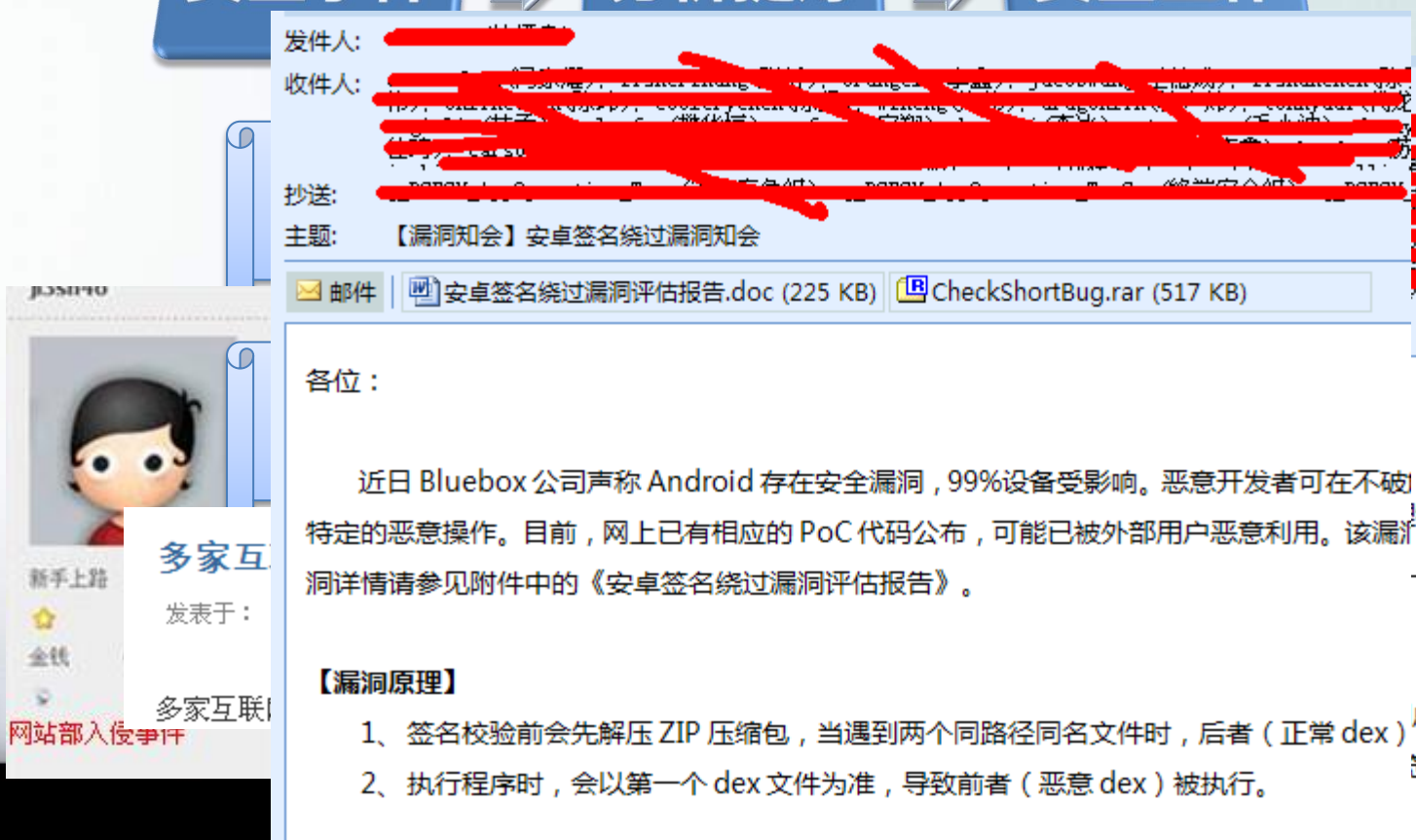
安全平台部

- 业务的核心竞争力
- 全面保障业务发展
- 应急响应

思路 2

事件驱动

安全事件 → 分析提炼 → 安全工作



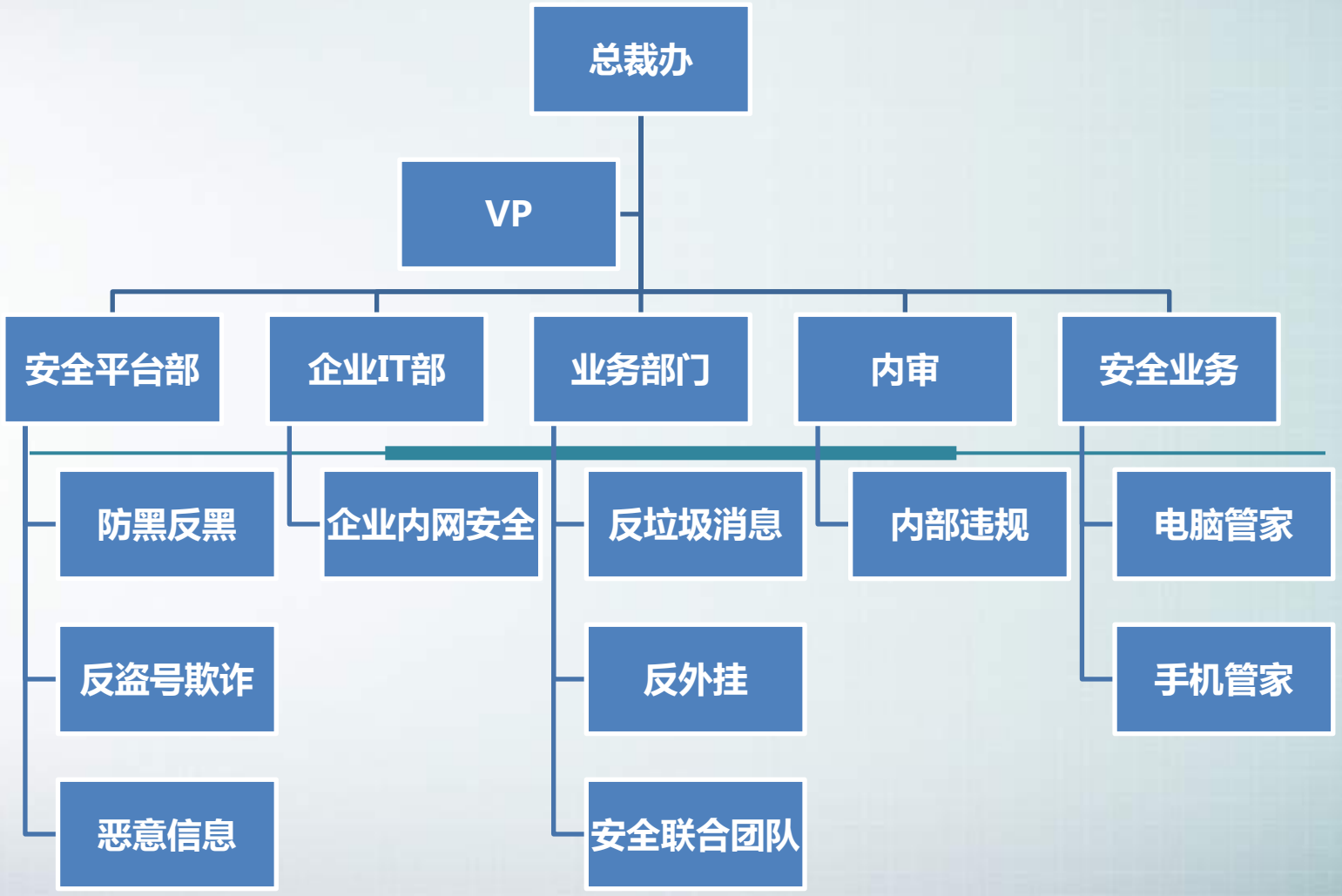
思路 3

抓大放小 解决主要矛盾

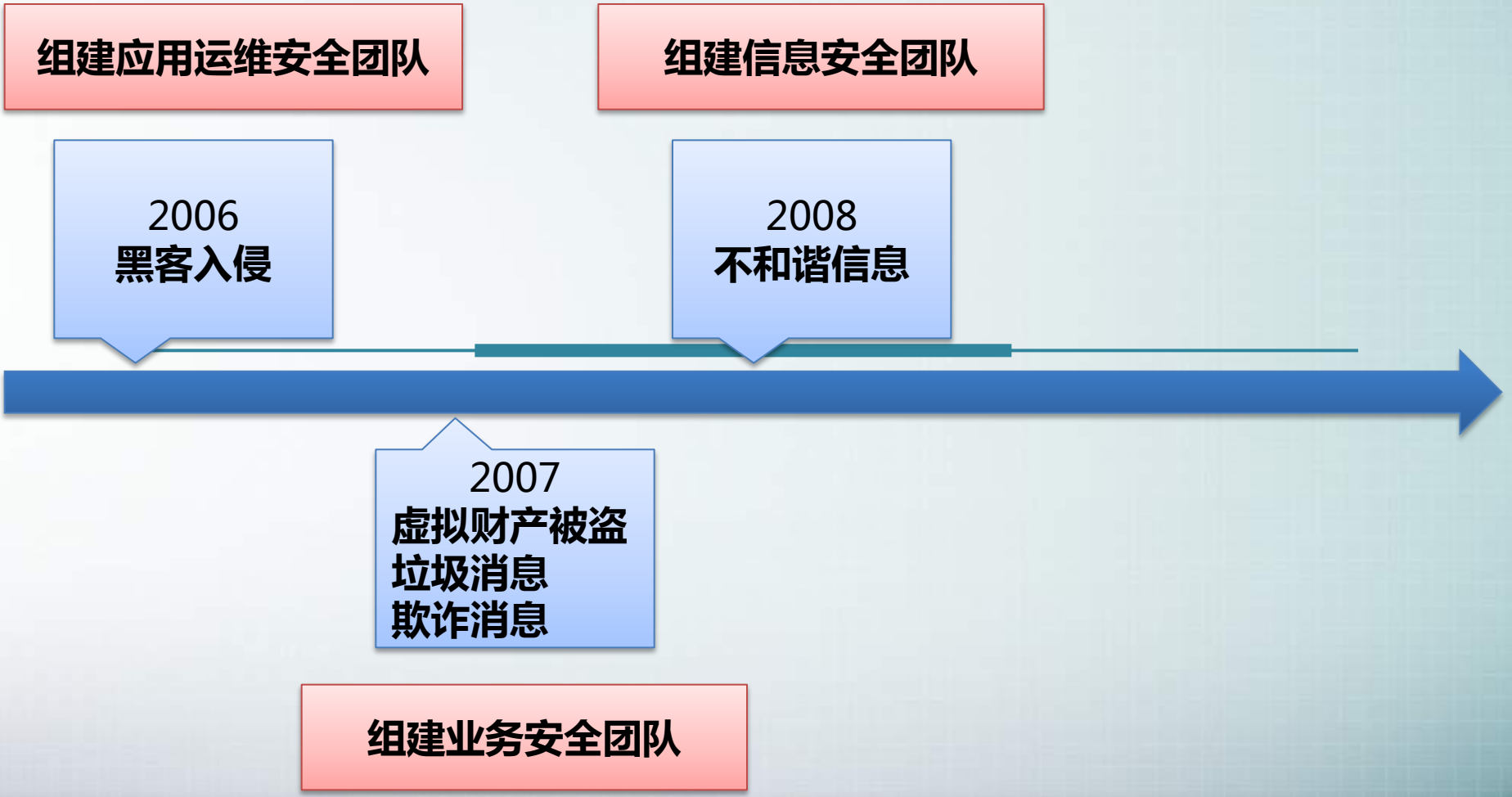
IDC入侵 → 内网入侵 → 客户端漏洞 → Web漏洞 → DDoS → 终端漏洞

IDC安全 | 内网安全 | 客户端安全 | 应用安全 | DDoS防御体系 | 终端安全审计

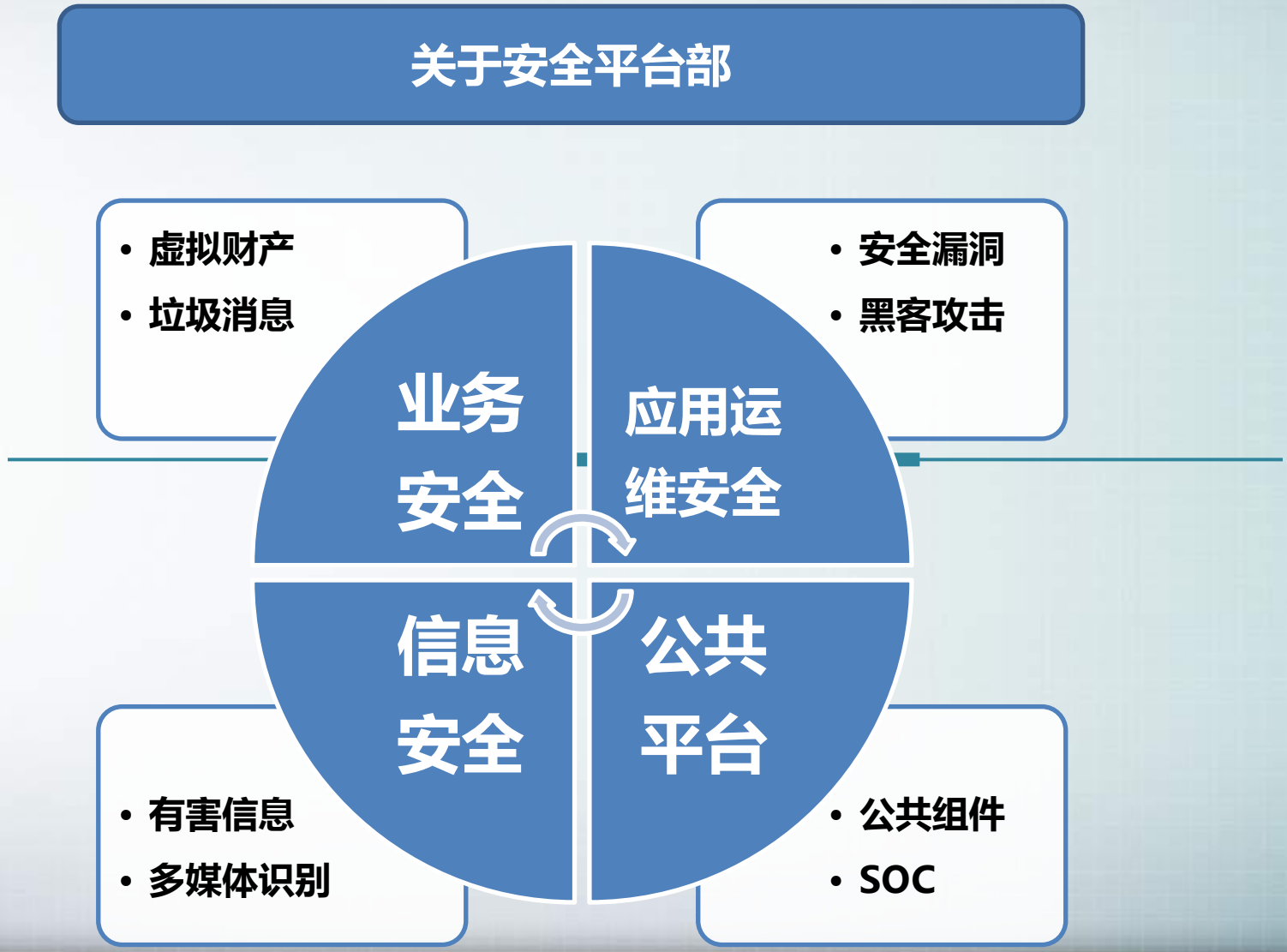
腾讯安全体系介绍


总裁办
VP
安全平台部
企业IT部
业务部门
内审
安全业务
防黑反黑
企业内网安全
反垃圾消息
内部违规
电脑管家
反盗号欺诈
反外挂
手机管家
恶意信息
安全联合团队

腾讯安全体系介绍


组建应用运维安全团队
组建信息安全团队
2006
黑客入侵
2008
不和谐信息
2007
虚拟财产被盗
垃圾消息
欺诈消息
组建业务安全团队

腾讯安全体系介绍


关于安全平台部
• 虚拟财产
• 垃圾消息
• 安全漏洞
• 黑客攻击
业务安全
应用运维安全
信息安全
公共平台
• 有害信息
• 多媒体识别
• 公共组件
• SOC

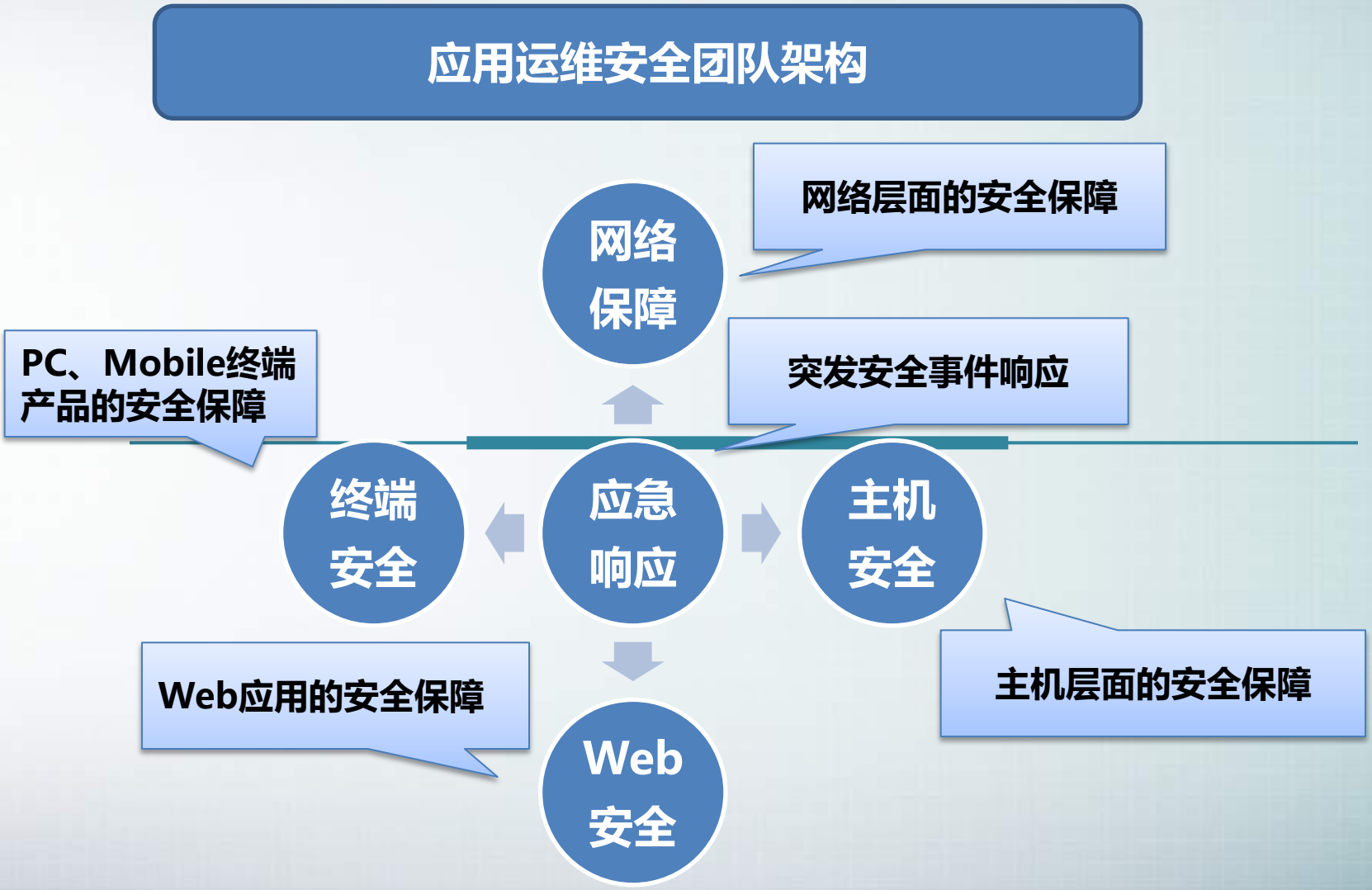
腾讯安全体系介绍

腾讯安全中心的几个发展阶段

腾讯安全体系介绍

TSDL思想

腾讯安全体系介绍


应用运维安全团队架构
网络保障
网络层面的安全保障
PC、Mobile终端产品的安全保障
突发安全事件响应
终端安全
应急响应
主机安全
Web应用的安全保障
主机层面的安全保障
Web安全

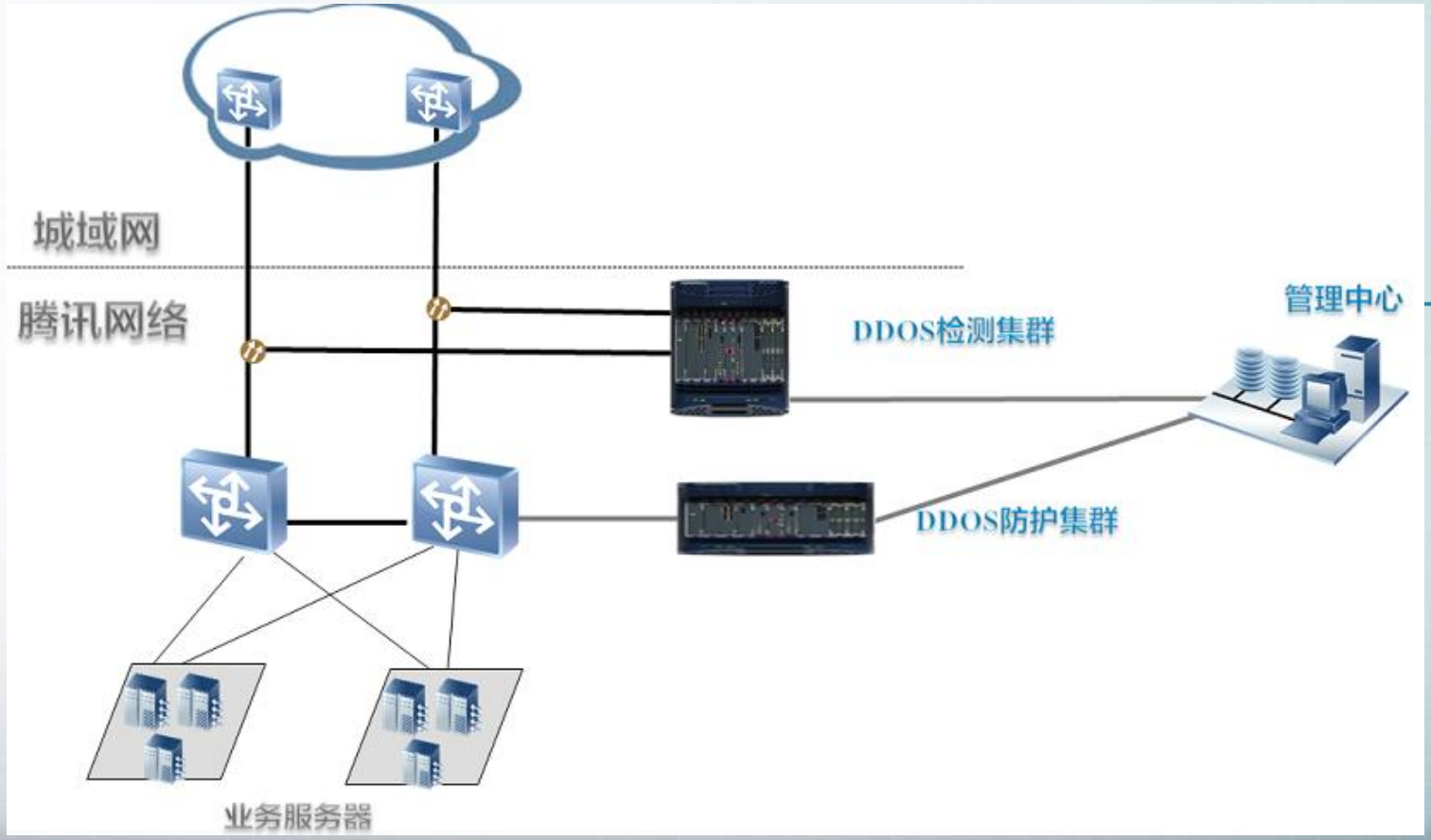
腾讯安全体系介绍

网络层威胁场景


```
C:\Python25\python.exe
WARNING: No route found for IPv6 destination :: (no default route?)
TCP Hijacking Delector by lake2
[+] Sniffing ....
74.125.128.199 has been hijacking !!!   debug info : 145  <-> 139
=>
74.125.128.199 has been hijacking !!!   debug info : 132  <-> 139
74.125.128.199 has been hijacking !!!   debug info : 134  <-> 139
74.125.128.199 has been hijacking !!!   debug info : 209  <-> 139
74.125.128.199 has been hijacking !!!   debug info : 211  <-> 139
=>
```

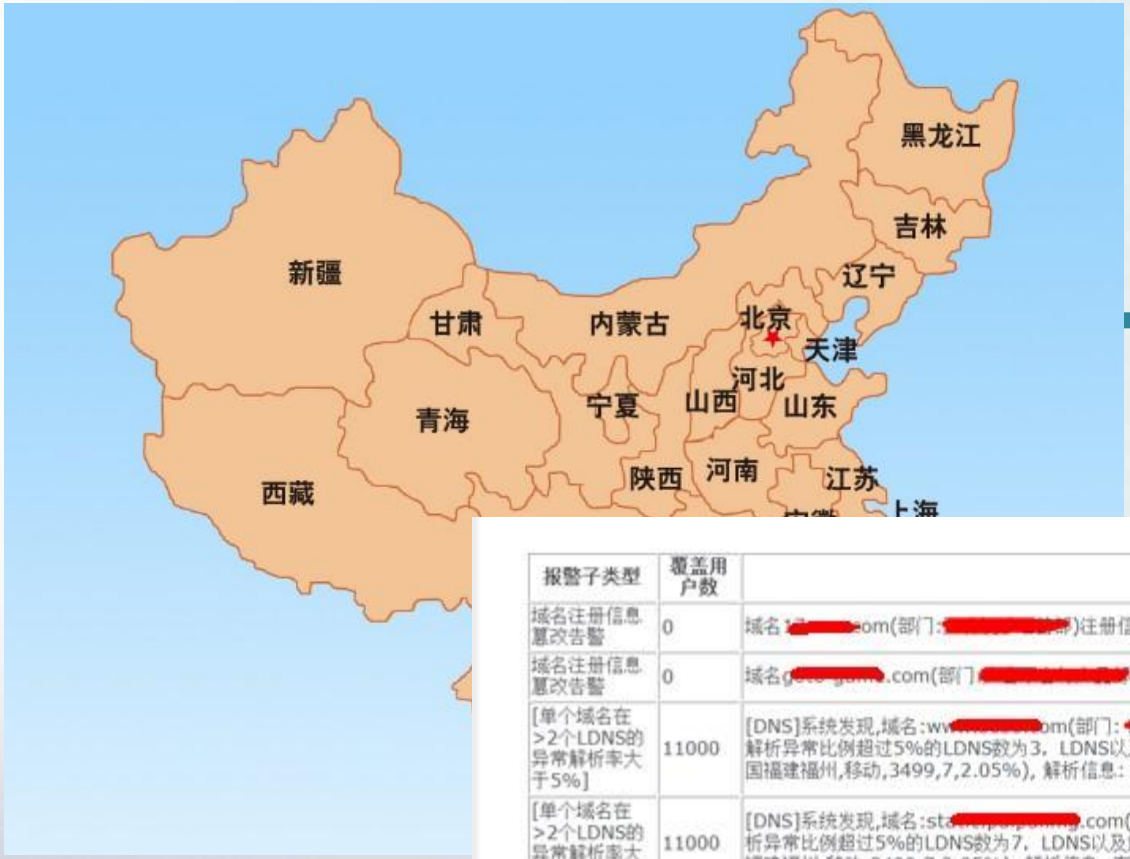
腾讯安全体系介绍

网络安全平台：DDoS检测与防护



腾讯安全体系介绍

网络安全平台：DNS解析监测



1）Local DNS劫持监测

覆盖全国各主要城市Local DNS

2）权威DNS篡改

权威DNS监测

报警子类型	覆盖用户数	细节
域名注册信息篡改告警	0	域名[redacted]注册信息发生变动，请关注(from:[redacted])
域名注册信息篡改告警	0	域名[redacted]注册信息发生变动，请关注(from:[redacted])
[单个域名在>2个LDNS的异常解析率大于5%]	11000	[DNS]系统发现,域名:[redacted]在2.5小时内，非故障类的解析异常比例超过5%的LDNS数为3，LDNS以及解析的详细信息为(TOP 2)，LDNS:[redacted](中国福建福州,移动,3499,7,2.05%)，解析信息：有风险：39%；
[单个域名在>2个LDNS的异常解析率大于5%]	11000	[DNS]系统发现,域名:[redacted]在2.5小时内，非故障类的解析异常比例超过5%的LDNS数为7，LDNS以及解析的详细信息为(TOP 2)，LDNS:[redacted](中国福建福州,移动,3499,7,2.05%)，解析信息：有风险：38.7%；

security.tencent.com

腾讯安全体系介绍

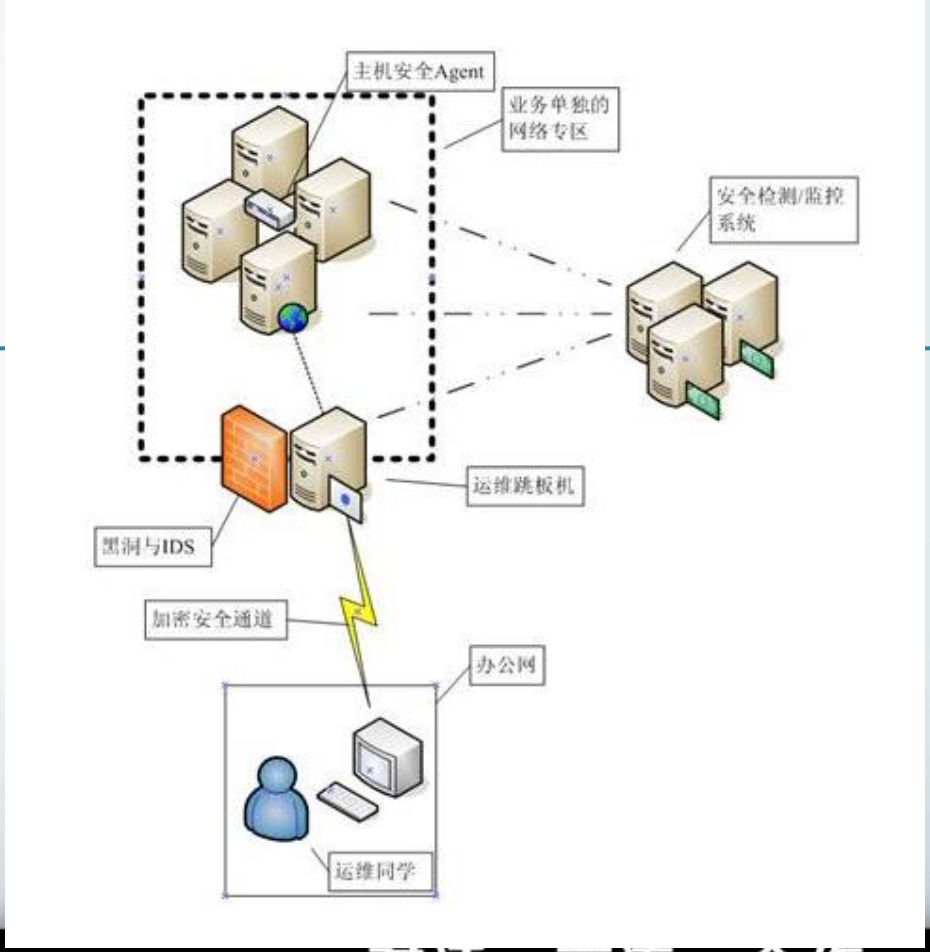
主机层威胁场景

2013-07-17	中国联通某分站struts命令执行
2013-07-17	易宝支付struts2命令执行漏洞！（已证明）
2013-07-17	京东某分站命令执行漏洞
2013-07-17	土豆网主站存在struts2命令执行漏洞！（已证明）
2013-07-17	51比购网命令执行
2013-07-17	京东商城分站存在struts2命令执行漏洞
2013-07-17	一号店旗下某网站，struts2命令执行漏洞（已证明读取到etc/passwd）
2013-07-17	京东商城某分站struts2命令执行漏洞
2013-07-17	百合网最新struts2任意命令执行漏洞大礼包集合（方便运维人员集中修复）
2013-07-17	京东商城旗下奢侈品360top,struts2命令执行漏洞（已证明读取到etc/passwd）
2013-07-18	金蝶主站struts2命令执行漏洞

struts2命令执行漏洞

腾讯安全体系介绍

主机安全平台：运维安全整体架构



腾讯安全体系介绍

主机安全平台：安全Agent

采集
- 服务器基础信息

分析
- 行为特征
- 数据挖掘

输出
- 安全风险
- 安全事件

处理
- 推动修复
- 应急响应

事件描述：

IP为[redacted]的Agent于2011-12-[redacted] 14:48:01发现webshell:
文件路径: [redacted]htdocs/tsrc/backdoor.php
分值: 85, 文件属主: [redacted], mtime: 2011-[redacted] 14:34:02, ctime: 2
部门: 安全中心, 机器负责人: [redacted]
匹配规则:
2002: eval(base64_decode("aWYoaXNzZXQo[redacted]9DT09LSUVbJ2N
0lFWydjbSddKS4nIDI+JjEnKTtzZXRjb29raV[redacted]9DT09LSUVbJ2N
Y29udGVudHMoKSkuJF9DT09LSUVbJ2N[redacted]2Vu
4001: eval(base64_decode("[redacted]9DT09LSUVbJ2N
0lFWydjbSddKS4nIDI+JjEnKTtzZXRjb29raV[redacted]9DT09LSUVbJ2N
Y29udGVudHMoKSkuJF9DT09LSUVbJ2NwJ10pO29[redacted]2Vu

时间
15:58:46
16:06:21
16:06:21
16:06:21
21:25:54
21:25:54

腾讯安全体系介绍

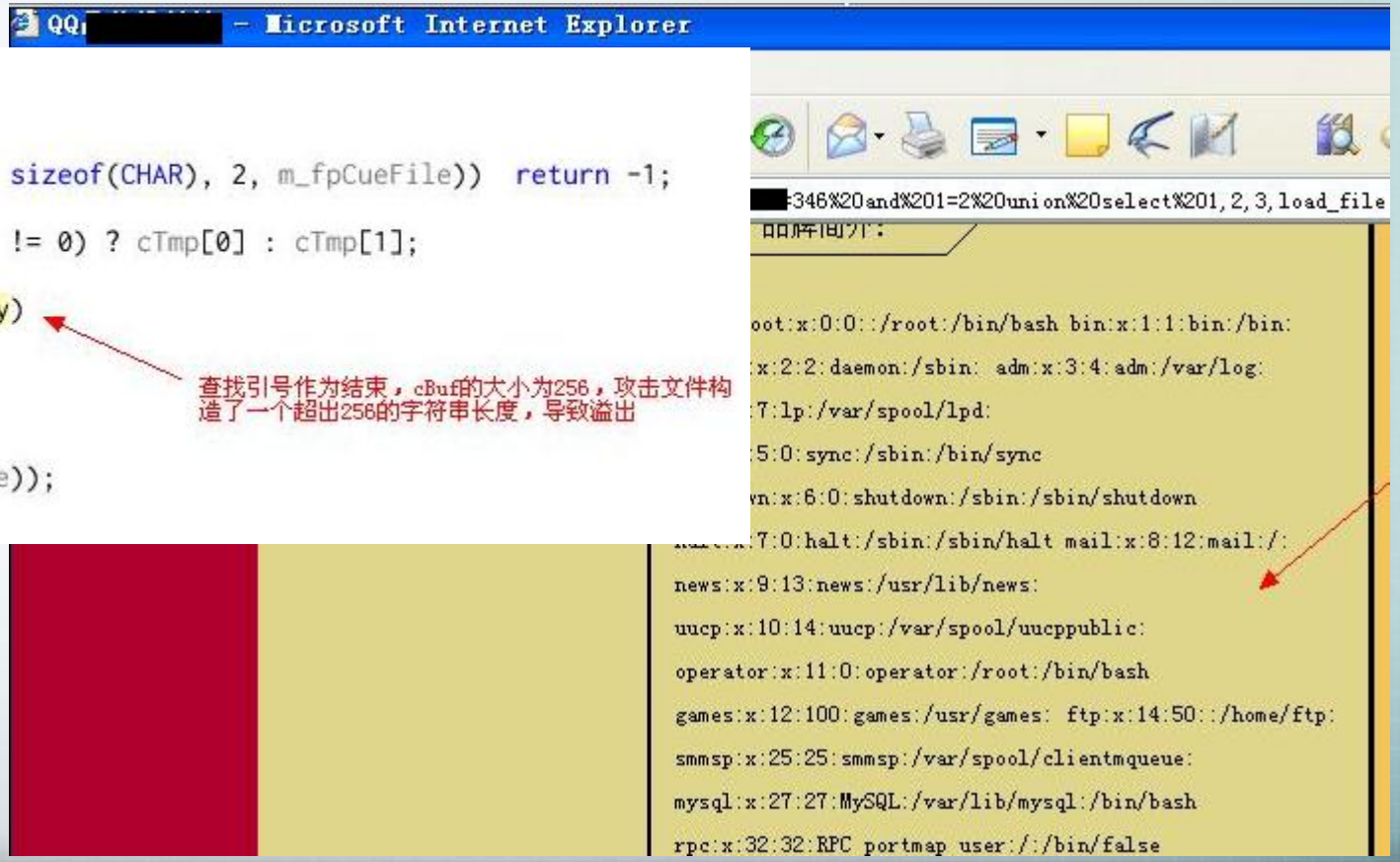
应用安全威胁场景

```
UINT nNum = 0;
do
{
    if (2 != fread(&cTmp, sizeof(CHAR), 2, m_fpCueFile))  return -1;

    cBuf[nNum] = (cTmp[0] != 0) ? cTmp[0] : cTmp[1];

    if (cBuf[nNum] == cKey)
    {
        break;
    }
    nNum++;
} while (!feof(m_fpCueFile));
```

查找引号作为结束，cBuf的大小为256，攻击文件构造了一个超出256的字符串长度，导致溢出



腾讯安全体系介绍

应用安全平台：Web/Server漏洞检测

SQL Injection
XSS
CSRF
JSON Hijacking
OS Injection
....

- 远程扫描
- 代码审计

Web

- 远程扫描
- 本地检测

Server

high-risk port
low version
remote overflow
danger config
weak pwd
....

腾讯安全体系介绍

应用安全平台：客户端漏洞审计

danger func
danger COM
DLL Hijacking
overflow
....

- 代码审计
- 动态分析
- 静态分析

PC

- 代码审计
- 动态分析
- 静态分析

Mobile

danger func
storage
transmission
组件权限
....

腾讯安全体系介绍

应用安全平台：WAF

No.	Time	Source	Destination	Protocol	Length	Info
190	9.75939700	10.26.234.31	113.108.12.60	TCP	66	58355 > http [SYN
197	9.76787600	113.108.12.60	10.26.234.31	TCP	66	http > 58355 [SYN
198	9.76793000	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK
238	10.0607890	10.26.234.31	113.108.12.60	HTTP	636	GET / HTTP/1.1
239	10.0630830	113.108.12.60	10.26.234.31	TCP	60	http > 58355 [ACK
240	10.0779570	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of a
241	10.0780740	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of a
242	10.0781050	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK
243	10.0810460	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of a
244	10.0811580	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of a
245	10.0811770	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK
246	10.0812800	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of a
247	10.0833940	113.108.12.60	10.26.234.31	HTTP	762	HTTP/1.1 200 OK
248	10.0834270	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK
432	15.0750180	113.108.12.60	10.26.234.31	TCP	60	http > 58355 [FIN

应急响应：struts 0day漏洞案例

总结&优化

如何快速解决安全风险？WAF

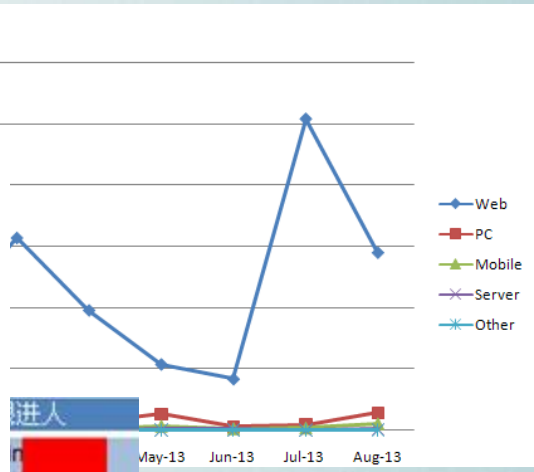
如何防御类似0day？主机agent新特性

腾讯安全体系介绍

应急响应：漏洞奖励计划

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

- 2013-09-04 因“腾讯漏洞奖励计划-用户兑换”获得1个“美心月
- 2013-09-01 因“腾讯漏洞奖励计划-用户兑换”获得1个“移动硬
- 2013-08-28 因“腾讯漏洞奖励计划-用户兑换”获得1个“手机 i
- 2013-08-12 因“感谢一直以来对TSRC的帮助和支持，赠送 TSRC 2(
- 2013-07-19 因“腾讯漏洞奖励计划-用户兑换”获得1个“Andro
- 2013-05-04 因“腾讯漏洞奖励计划-用户兑换”获得1个“三星G
- 2013-03-06 因“腾讯漏洞奖励计划-用户兑换”获得1个“雷蛇八
- 2013-03-06 因“腾讯漏洞奖励计划-用户兑换”获得1个“Q影”
- 2013-03-06 因“腾讯漏洞奖励计划-用户兑换”获得1个“New I
- 2013-02-05 因“提交高质量漏洞”获得1个“白
- 2013-01-14 因“2012年年度突出贡献-漏洞之王”
- 2013-01-07 因“2012年12月月度奖励-力拔头筹”
- 2012-12-06 因“2012年11月月度奖励-漏洞猎手”
- 2012-12-06 因“2012年11月月度奖励-力拔头筹”
- 2012-11-07 因“2012年10月月度奖励-漏洞猎手”
- 2012-11-07 因“2012年10月月度奖励-力拔头筹”
- 2012-11-07 因“2012年10月月度奖励-力拔头筹”
- 2012-11-07 因“2012年10月月度奖励-力拔头筹”



所属系统			
漏洞扫描			
	高危端口	务	
Web漏洞检测	Web目录扫	增加按目录缩包检测	Bin
信息泄漏检测	测试文件	优化扫描测试文件	Cat
Web漏洞检测	Tomcat漏扫	实现检测泄漏的功	Bin

未来的一些想法

整合内部平台，打造安全生态圈

安全服务1：防DDoS攻击

- 腾讯云安全提供专业的防DDoS攻击服务，能够帮您的云服务抵御CC、SYN flood、UDP flood等多种攻击。

安全服务2：漏洞扫描

- 腾讯云安全可以定期对您的云服务进行各种安全漏洞检测，并将检测结果及时反馈给您。

安全服务3：入侵检测

- 腾讯云安全可以定期对您的云服务进行木马、暗链检测，并将检测结果及时反馈给您。

Q&A

- 作为用人单位，你们对高校信息安全人才培养有哪些期待？（或你们觉得目前高校信息安全人才培养存在哪些不足？）

Q&A

- 在对外合作中，你们最核心的技术与资源优势是什么？

Q&A

- 在对外合作中，你们对合作方在技术与资源上有哪些要求或期待？

Thanks!