

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

内外兼修，保障业务安全

—— 腾讯安全运维实践

自我介绍

腾讯安全体系全局视图

内功修炼：安全平台建设与运营

外援支持：业界安全专家

Q&A

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计·自动化运维·云计算

演讲者

lake2

- 80SEC
- 9+ years security experience
- focus on Web Security



lakehu (胡珀)

- join Tencent Security Center in 2007
- work on Tencent Security Response Center
- System / Response / Assessment / Train

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

关于腾讯



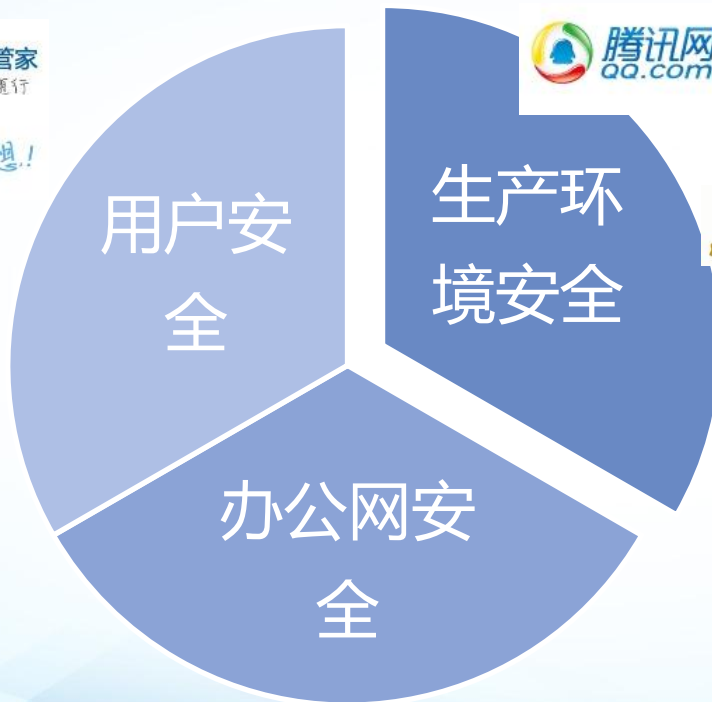
SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

腾讯安全体系



腾讯企业门户
OA让我们工作更轻松

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

关于腾讯安全中心

成立于2005

目前人数160+

负责腾讯整体安全

帐号安全体系

黑客攻击防御

危害信息打击

The update for Adobe Flash Player and Adobe AIR, Adobe Reader and Acrobat resolves a memory corruption vulnerability that could potentially lead to code execution (CVE-2009-1862).

lakehu of Tencent Security Center (CVE-2009-1862)

This update resolves a vulnerability that could lead to a cross-domain policy bypass (Internet Explorer-only) (CVE-2011-2458).

lakehu of Tencent Security Center (CVE-2011-2458)

Security Researcher Acknowledgments for Microsoft Online Services

- **Tencent Security Center**

Tencent

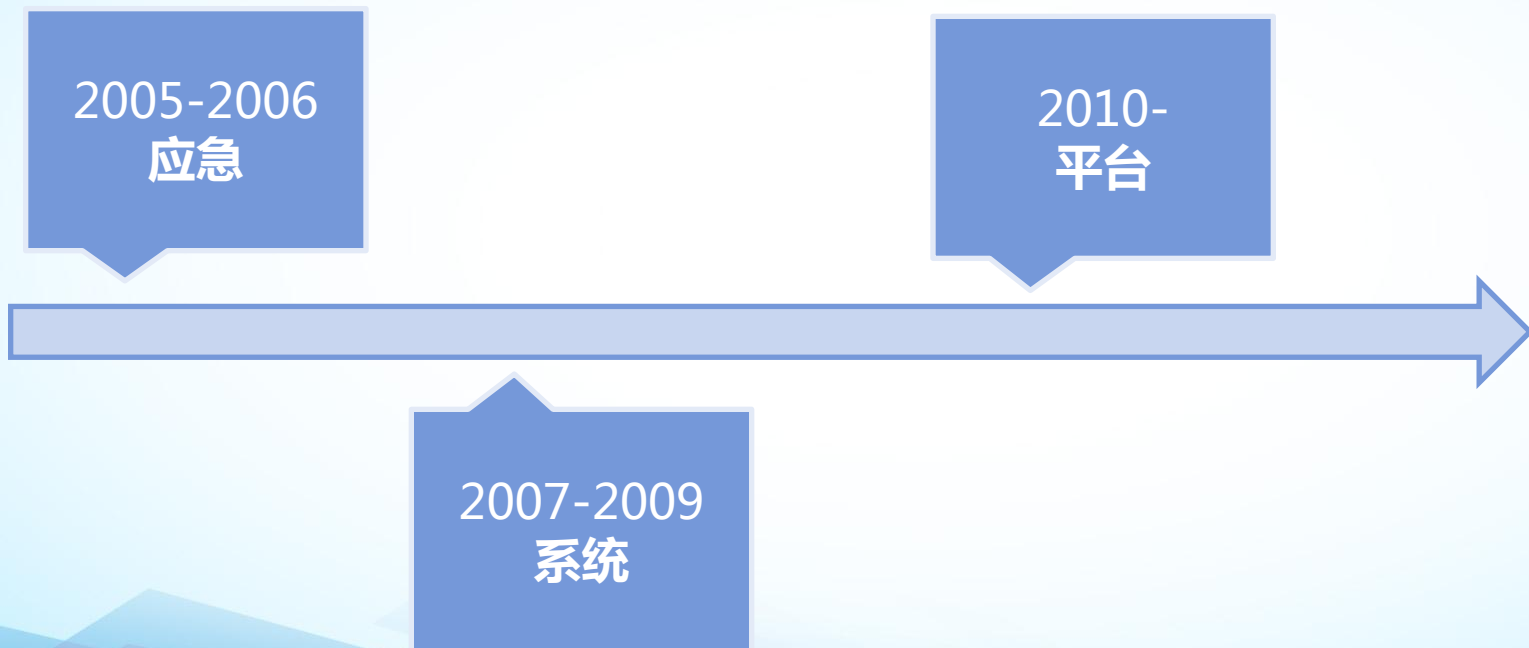
SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

安全建设思路与实践



T-SDL

Security Development Lifecycle



TSEC安全平台概述



Web漏洞扫描器

客户端审计系统

代码审计系统

主机安全Agent

运维操作审计

账号安全管理

DDoS防御

IDS / WAF

DNS监控系统

SACC

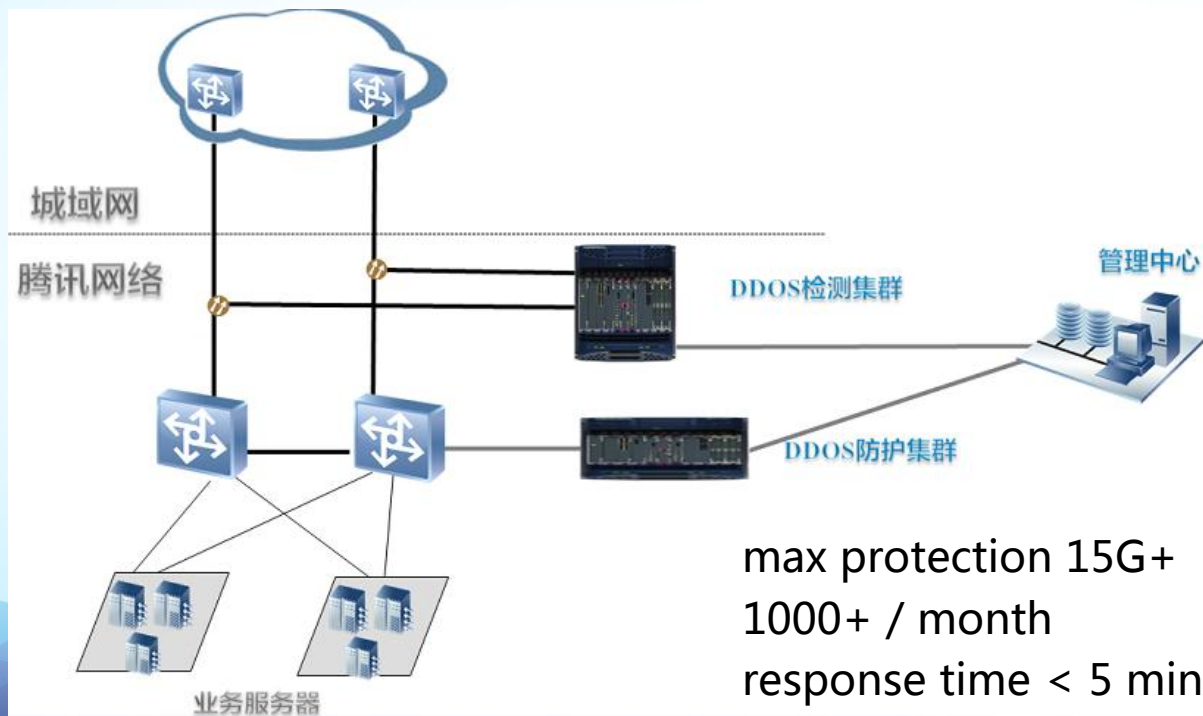
2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

网络安全平台：DDoS防御

Anti-DDoS



max protection 15G+
1000+ / month
response time < 5 min

SACC

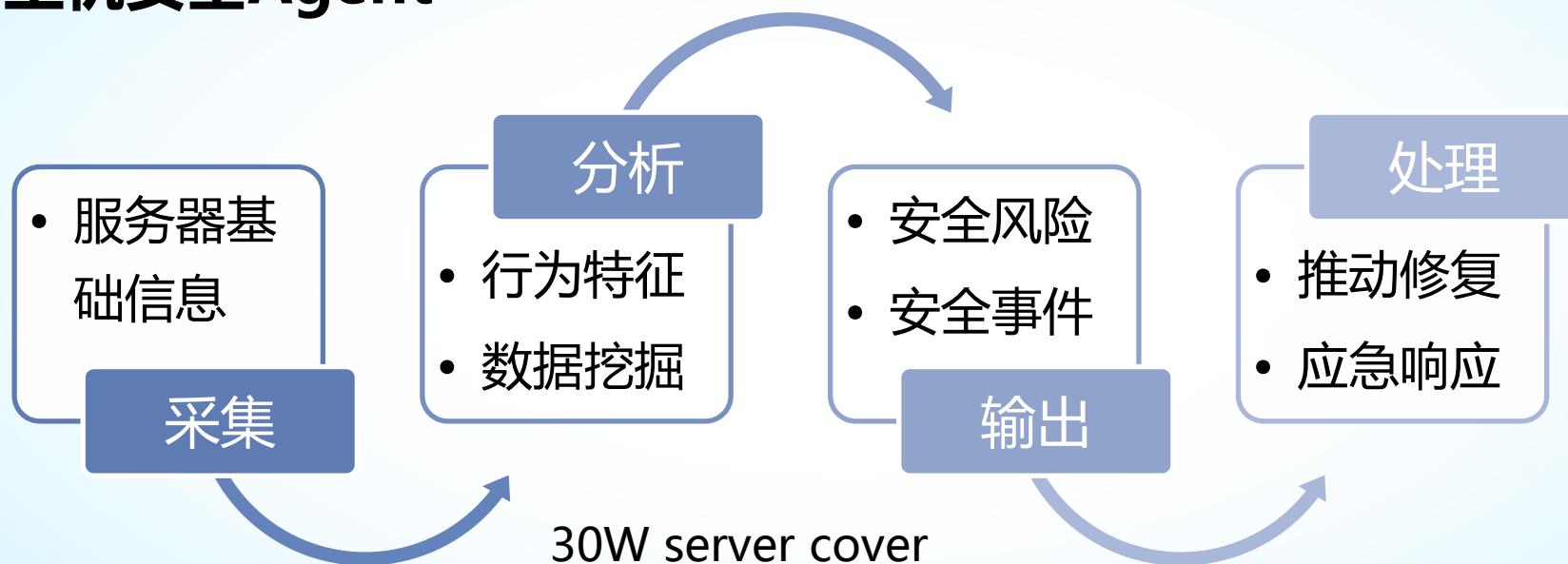
2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

主机安全平台：SecAgent

主机安全Agent



30W server cover
TB-Level data
200+ rule
response time < 5 min

应用安全平台：Web/Server漏洞检测

漏洞检测系统

SQL Injection
XSS
CSRF
JSON Hijacking
OS Injection
Etc..

• 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
unsecu config
weak pwd
Etc..

5W+ domain / 30W server cover
PHP / JSP / JAVA / C / C++ support
full scan time < 1 day

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

应用安全平台：客户端漏洞检测

漏洞检测系统

danger function
danger COM
overflow
DLL Hijacking
Etc..

- 代码审计
- 动态分析
- fuzz

PC



- 代码审计
- 动态分析
- 静态分析

Mobile

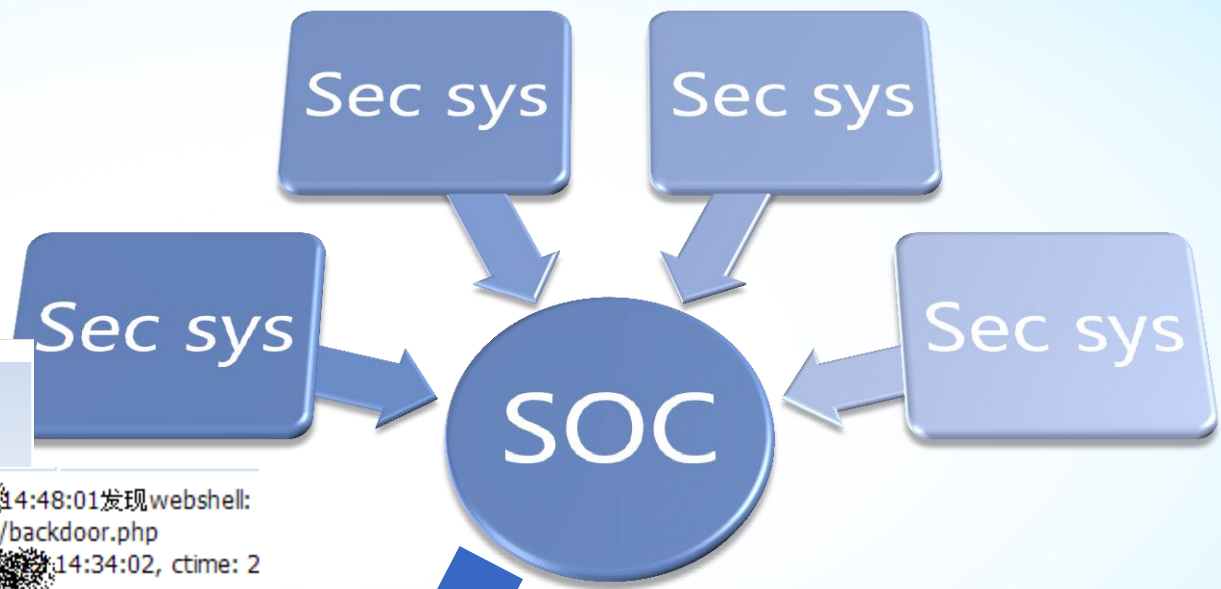


storage
password
transmission
malicious
Etc..

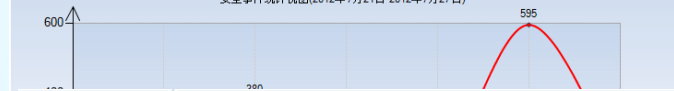


大脑：SOC

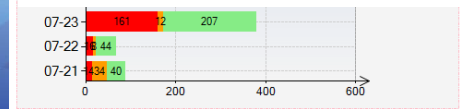
安全运营中心



截至目前，安全事件累计1000件，完成1000件，未完成0件，完成率98%；其中误报100件，误报率10%



事件描述：
 IP为163.8.1.1的Agent于2011-12-14 14:48:01发现webshell:
 文件路径: /var/www/html/htdocs/tsrc/backdoor.php
 分值: 85, 文件属主: root, mtime: 2011-12-14 14:34:02, ctime: 2
 部门: 安全中心, 机器负责人: hase@ha
 匹配规则:
 2002: eval(base64_decode("aWYoaXNzZXQ9Pj9DT09LSUVbJ2N
 0lFWyYdjBScddKS4nIDI+JjEnKTtzZXRjb29raVZlbnQ9LSUVbJ2N
 Y29udGVudHMokSkUJF9DT09LSUVbJ2NwJ10pO29lX2Vu
 4001: eval(base64_decode("aWYoaXNzZXQ9Pj9DT09LSUVbJ2N
 0lFWyYdjBScddKS4nIDI+JjEnKTtzZXRjb29raVZlbnQ9LSUVbJ2N
 Y29udGVudHMokSkUJF9DT09LSUVbJ2NwJ10pO29lX2Vu



入侵告警	20605	20580	25
DDOS	9629	9626	3
DNS告警	2242	2242	0
蠕虫	55	55	0

说明：以上数据均为历史累计总数。



SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

机动部队：应急响应

应急响应联合团队



SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

腾讯安全应急响应中心



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

官网 <http://security.tencent.com>

漏洞反馈平台与奖励

分享



当前，共有95位安全专家通过腾讯

以上安全专家长期关注腾讯安全，

全部 | 2012/08 | 2012/09 | 2012/1

SRC特向以下安全专家致谢：

排名	昵称
1	知道创宇-zjp
2	AIScanner

600+ v

30+ new features

20+ bug fixed



腾讯安全应急响应中心：【漏洞奖励计划-8月奖励】我们将为46位安全专家送出如图的奖品！由于8月收获颇丰，腾讯安全应急响应中心特别决定积分TOP3都获得NewPad！8月排名如下 <http://url.cn/85s5oe>。寄出的东西非常多，一线同事们辛苦了，请大家给他们一些掌声👏。老规矩，收到后拍照at我哦~

向左转 向右转 查看更多它的图片 查看原图

漏洞奖励计划 2012年8月奖励情况 by 腾讯安全应急响应中心

条件	名号	奖励物品
TOP 3 (3人)	力拔头筹	 (New Pad) 已纳入客户端漏洞第一名
第4至第13名 (10人)	无敌犀利	
第14名及之后 (33人)	再接再厉	
青铜企鹅勋章 得主额外获得	漏洞猎手	
幸运星 (3人)	最佳人品	100个Q币 (微博传播者、漏洞报告者、顾问群传播者)

青)。

分

SACC

中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算



与我同在

mrhupo@qq.com

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算