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

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

关于腾讯


腾讯产品战略布局 Product Strategies Map
即时通讯
电子商务
门户
游戏娱乐
美团
音视频
搜索
客户端
应用软件
优势领域
弱势领域
抢夺战中
难攻天险
领域分界
http://middle.blog.sohu.com

腾讯安全体系


电脑管家
GUANJIA.QQ.COM
腾讯手机管家
腾讯开放平台
open.qq.com
开放成就梦想!


用户安全
生产环境安全
办公网安全


腾讯网
QQ.com


手机QQ
mobile.qq.com


英雄联盟
LEAGUE OF LEGENDS


MySQL
DNS


腾讯企业门户
OA让我们工作更轻松

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)

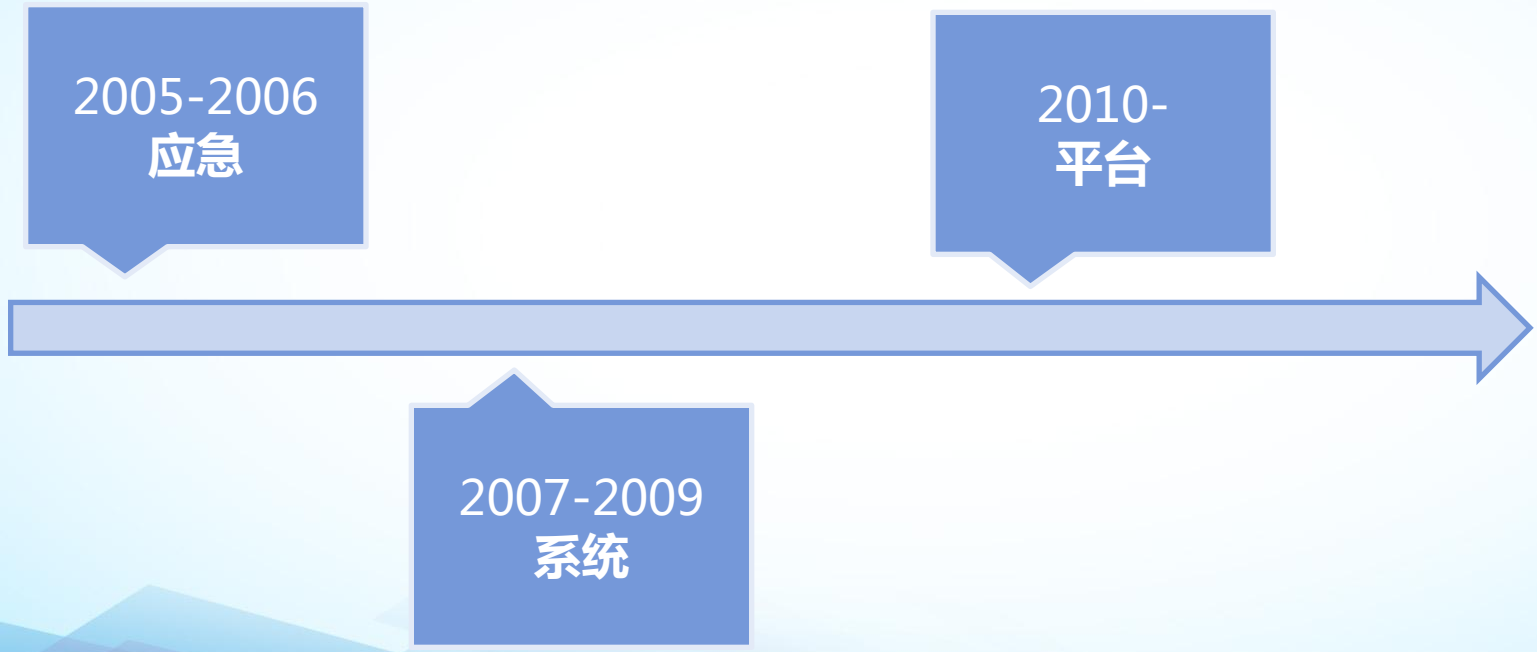
This update resolves a vulnerability that could lead to a cross-domain policy bypass (Internet Explorer-only) (CVE-2011-2458).

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

Security Researcher Acknowledgments for Microsoft Online Services

- **Tencent Security Center**
  Tencent

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

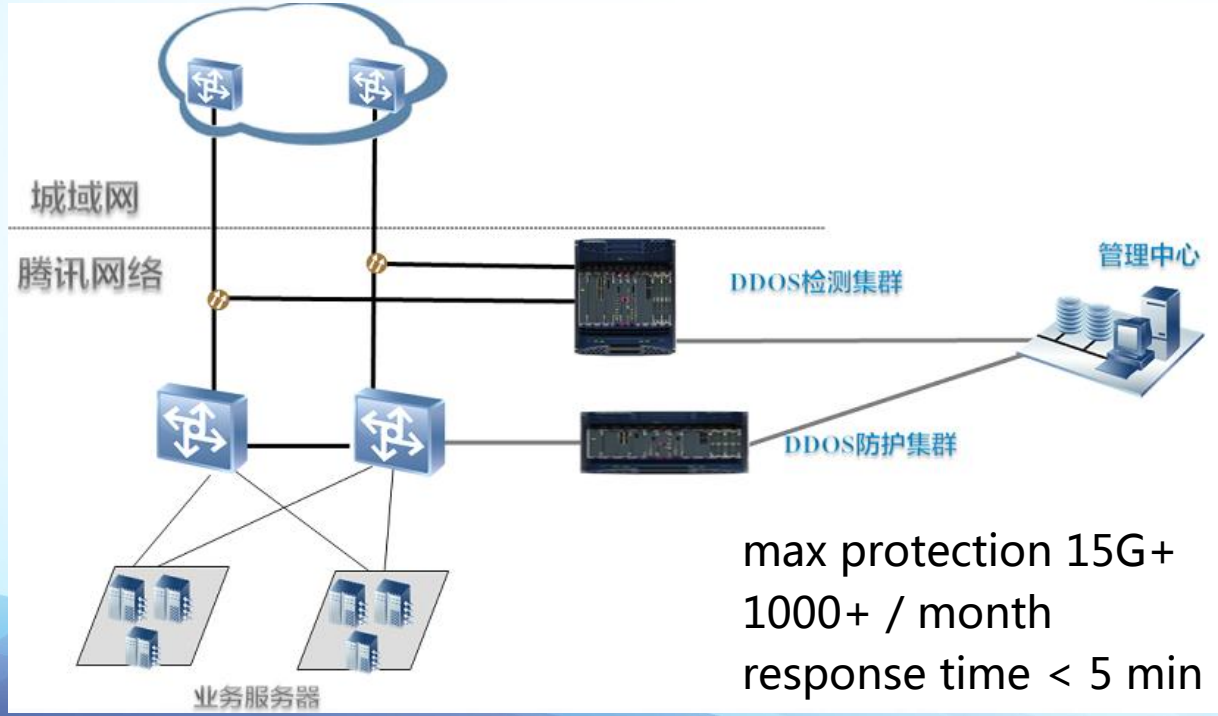
DDoS防御

IDS / WAF

DNS监控系统

网络安全平台：DDoS防御

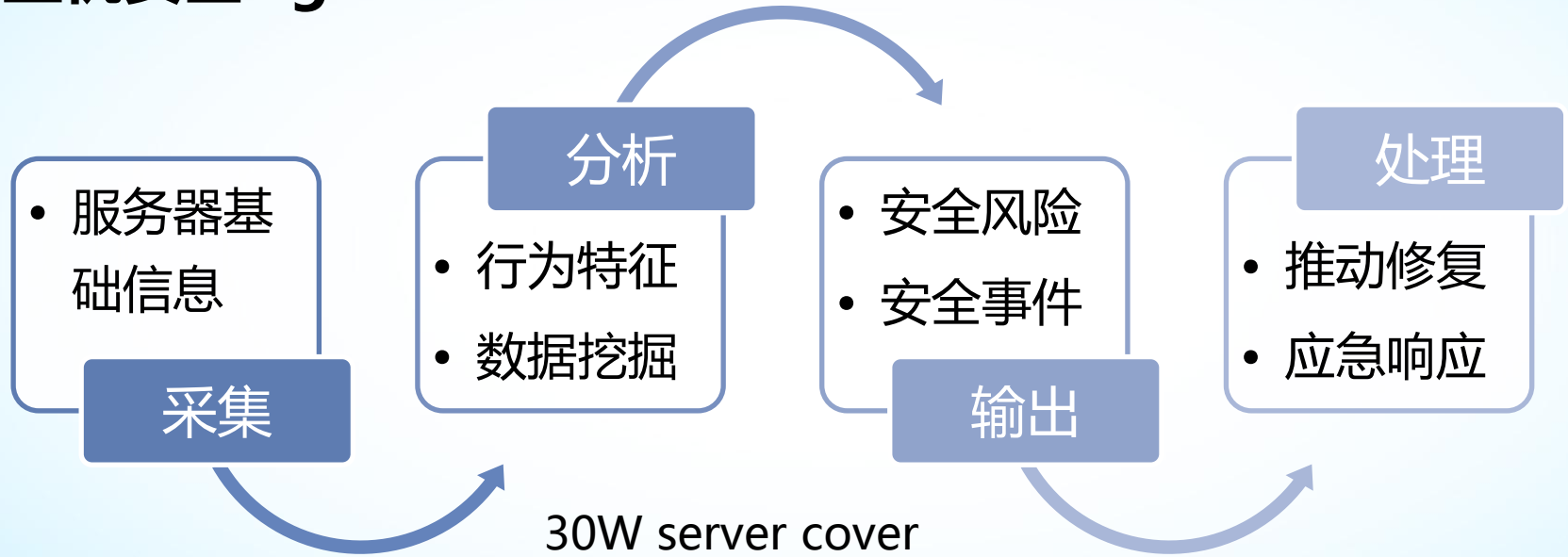
Anti-DDoS



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

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..

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

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

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

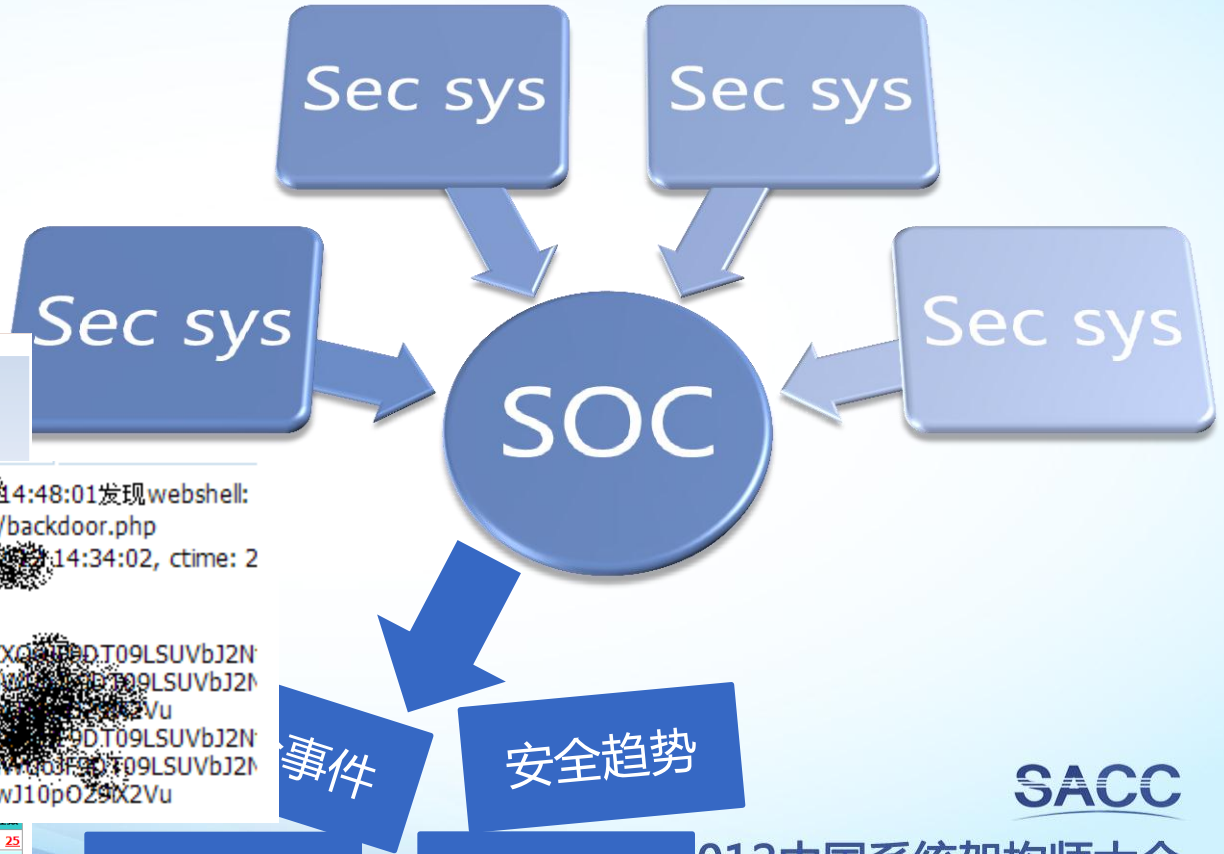
- 代码审计
- 动态分析
- 静态分析

Mobile

storage
password
transmission
malicious
Etc..

大脑：SOC

安全运营中心



机动部队：应急响应

应急响应联合团队

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

600+ v

30+ new features

20+ bug fixed

与我同在

mrhupo@qq.com