CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

新形势下的企业安全体系建设实践
（蓝军篇）

胡珀　　腾讯 技术工程事业群 安全平台部

CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

个人简介

胡珀　lakehu

- 腾讯 – 技术工程事业群 - 安全平台部　总监 / T4安全专家
- 2007年加入腾讯，一直在安全平台部从事基础安全体系建设工作

- 腾讯安全应急响应中心（TSRC）
- Tencent Blade Team
- 腾讯蓝军
- 漏洞检测平台、WAF
- 数据保护专项
- 主机入侵检测平台
- DDoS攻击防护平台
- 云安全

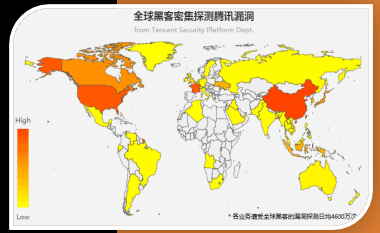
- 逾十五年网络安全经验，技术派，
  网名“lake2”

概况介绍

腾讯用户总量 **突破**

1, 000,000,000

概况介绍


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

应急响应中心 ->
全面保障业务发展 ->
业务的核心竞争力

安全相关部门架构

业务安全

- 安全平台
- 各业务部门

内容安全

- 信息安全
- 安全管理

基础设施安全

- 安全平台

产品安全

- 腾讯电脑管家
- 腾讯手机管家
- 腾讯安全、腾讯云安全
- 安全实验室（玄武、科恩等）

法务、政务、合规

安全生命周期

培训/training
- 安全技术培训
- 安全意识培训
- 安全规范

设计/design
- 安全技术培训
- 安全意识培训
- 安全规范

验证/verification
- 代码审计
- 渗透测试

响应/response
- 应急响应执行
- 人工巡查
- 漏洞扫描系统
- 安全情报系统

要求/requirements
- 安全需求建立
- 质量标准建立
- 风险识别

实施/implementation
- 提供安全开发工具
- 安全开发模范和最佳实践
- 安全API

发布/release
- 应急响应方案
- 上线前集成环境安全检查
- 安全运维规范

安全体系与安全产品构成

建立了安全团队，
建设了安全规范、安全系统、安全流程……

那么，现在足够**安全**了吗？

实战是检验防护能力的唯一标准

“Talk is Cheap，Show me the Shell”

实战：

完全仿真模拟黑客攻击
红蓝对抗是渗透测试的升级版本

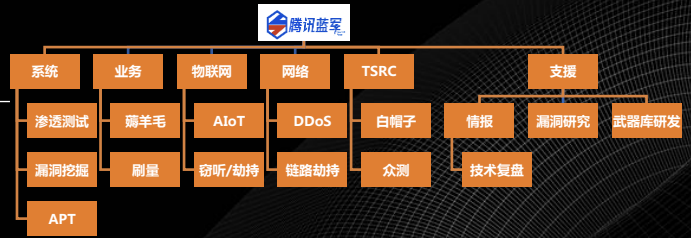
	渗透测试 Penetration Testing	红蓝对抗 Red Teaming
概念	攻击团队单方面进攻，关注最终目标渗透达成	攻防两支团队实战演练，关注检测、防护、应急处置等综合能力
能力	熟悉常见黑客攻击手法	精通各类场景的攻防技术，包括 APT、物联网、工业互联网等
工具	普通安全工具	定制化专业工具，包括定制后门、0day 漏洞等
团队	突击队	突击队、技术支援队

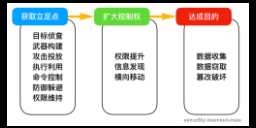
红蓝对抗实战：

关注安全风险
也关注防御体系的缺陷

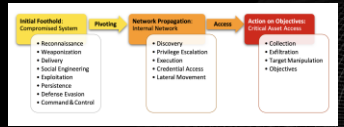
不局限于传统的系统蓝军，
腾讯蓝军的大蓝军建设之路：

- 独立团队
- 关注安全风险及防护能力
- 整合多个领域（系统、网络、业务）攻防能力
- 依托TSRC引入外部安全专家的视角和手法
- 提前布局新领域研究输出能力





传统的
红蓝军
网络攻防对抗



网络攻击蓝军

模拟各类流量型、资源消耗型DDoS攻击

检验DDoS防护能力

业务安全蓝军





BLADE


TSRC
腾讯安全应急响应中心

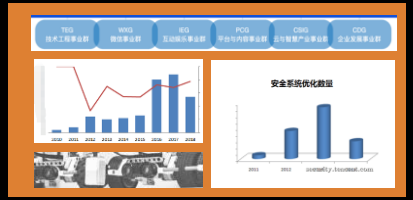
以局外人的视角帮助发现实际安全风险

新技术预研：Tencent Blade Team

夜半十二点
蓝军出动无人机挂载无线信号发射器
直飞36楼

- 漏洞研究团队发现智能设备协议漏洞，制作攻击测试工具
- 攻击分队制定攻击计划
- 攻击分队实施攻击计划
- 复盘 & 优化策略

内部安全防护能力检验与产品风险收敛



能力输出/产品输出

1. 支持腾讯云金融大客户HW行动
2. 支持腾讯云政企大客户红蓝对抗
3. 支持腾讯云电商大客户DDoS攻防演练
4. 区块链安全标准

相关传播和报道

推动国内企业自建SRC
重视安全研究者

* 来源：0xsafe.org

xSRC：
SaaS版本 / 开源版本

未来可能的合作机会

网络安全创新大会
Cyber Security Innovation Summit

THANKS