

**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

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)  | • 数据保护专项     |
| • Tencent Blade Team | • 主机入侵检测平台   |
| • 腾讯蓝军               | • DDoS攻击防护平台 |
| • 漏洞检测平台、WAF         | • 云安全        |
- 逾十五年网络安全经验，技术派，网名“lake2”

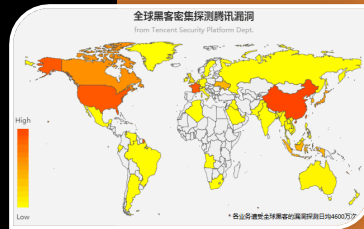


## 概况介绍



腾讯用户总量 **突破**  
**1,000,000,000**

## 概况 介绍



应急响应中心 ->  
全面保障业务发展 ->  
业务的核心竞争力

及时迅速应急响应

促进业务核心竞争力

全面保障业务发展

### 业务安全

- 安全平台
- 各业务部门



### 基础设施安全

- 安全平台



### 内容安全

- 信息安全
- 安全管理



### 产品安全

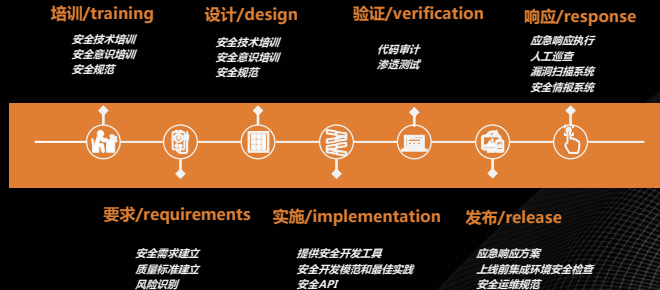
- 腾讯电脑管家
- 腾讯手机管家
- 腾讯安全、腾讯云安全
- 安全实验室（玄武、科恩等）

法务、政务、合规





## 安全生命周期



网络安全创新大会  
Cyber Security Innovation Summit





## 安全体系与安全产品构成



网络安全创新大会  
Cyber Security Innovation Summit



+ + + >\_ 一个问题

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

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"



## 渗透测试 & 红蓝对抗

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





## 蓝军建设之路

### 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引入外部安全专家视角和手法
- 提前布局新领域研究输出能力

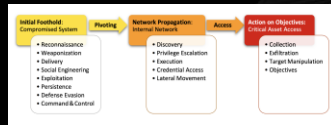




ATT&CK Matrix for Enterprise

Attack Type	Attack Vector	Attack Method	Attack Tool	Attack Result
Reconnaissance	Network	Port Scanning	Nmap	Discovery of open ports
Weaponization	Network	Malware Development	Metasploit	Creation of exploit code
Delivery	Network	Phishing	Phishing Kit	Delivery of malicious email
Exploitation	Network	Exploit Execution	Metasploit	Successful exploitation of vulnerability
Persistence	Network	Backdoor Installation	Metasploit	Installation of backdoor
Defense Evasion	Network	Antivirus Evasion	Antivirus Evasion Tool	Evasion of antivirus detection
Command & Control	Network	C&C Server Setup	C&C Server	Establishment of C&C channel

传统的  
红蓝军  
网络攻防对抗





模拟各类流量型、  
资源消耗型  
DDoS攻击  
检验DDoS防护能力



攻击类型	syn - flood
持续时间(秒)	syn - flood
	udp - flood
	udp - 自定义payload
	icmp - flood
包量	dns - flood
53.33 Kpps	fin - flood
53.33 Kpps	fin畸形 - flood
128.00 Kpps	ack - flood



业务安全蓝军





## 物联网&硬件设备蓝军



网络安全创新大会  
Cyber Security Innovation Summit





基于白帽子众测的**泛蓝军**： **TSRC**  
腾讯安全应急响应中心



**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



**网络安全创新大会**  
Cyber Security Innovation Summit





## 新技术预研：Tencent Blade Team



腾讯Blade Team发现云虚拟化平台QEMU-KVM逃逸漏洞 各大云厂或受影响

千变：绕过“木马通讯防线”，手机硬件解码器的“双守之道”

从攻破智能音箱到智能楼宇，我们和腾讯Blade Team聊聊物联网安全



New Flaws in Qualcomm Chips Expose Millions of Android Devices to Tracking

DEF CON 2018 Researchers Demonstrate Hackling Google Home for PCE

## + + + >\_ 蓝军行动一例：智能楼宇安全测试

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

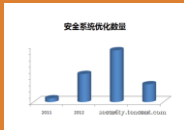




蓝军成果



### 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

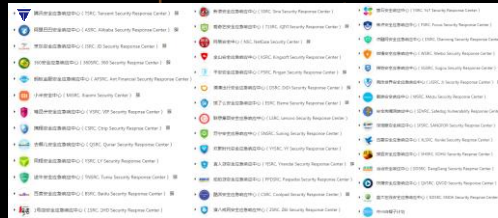


### 相关传播和报道





## 推动国内企业自建SRC 重视安全研究者



\* 来源: 0xsafe.org

+ + + >\_ 推动生态，合作共赢

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

xSRC :  
SaaS版本 / 开源版本





+ + + >\_ 推动生态，合作共赢

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

## 未来可能的合作机会



