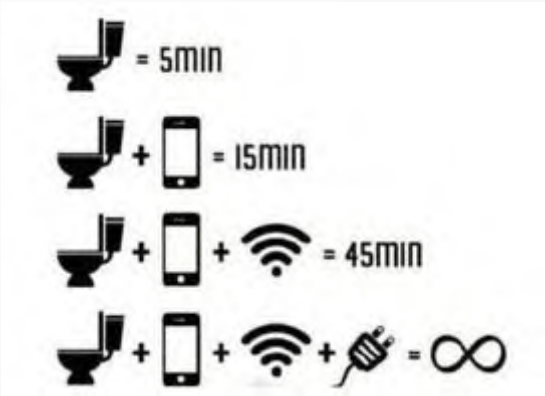
TiD 2017
质量竞争力大会

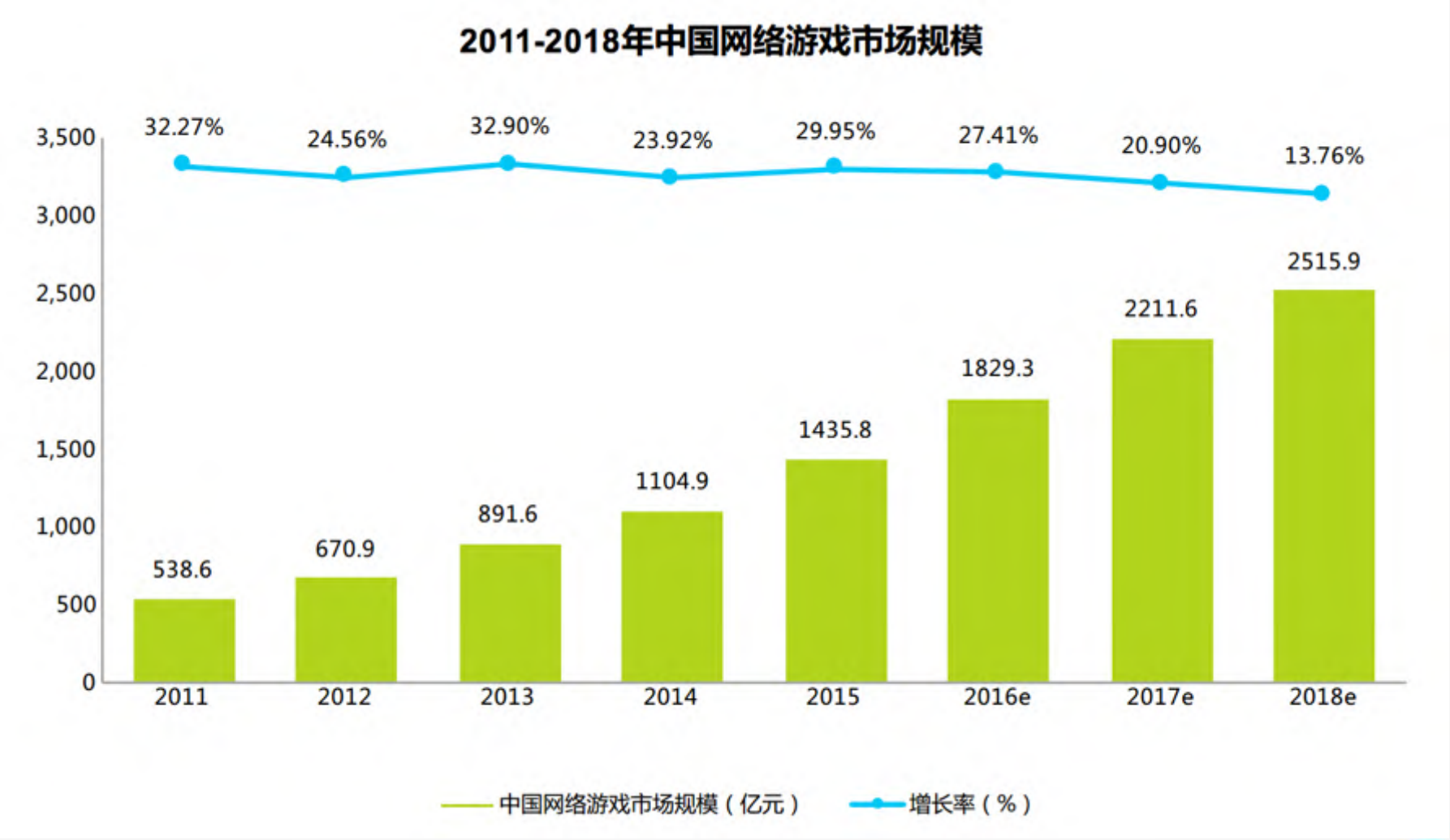
在线游戏企业安全建设之路

仲维国@竞技世界

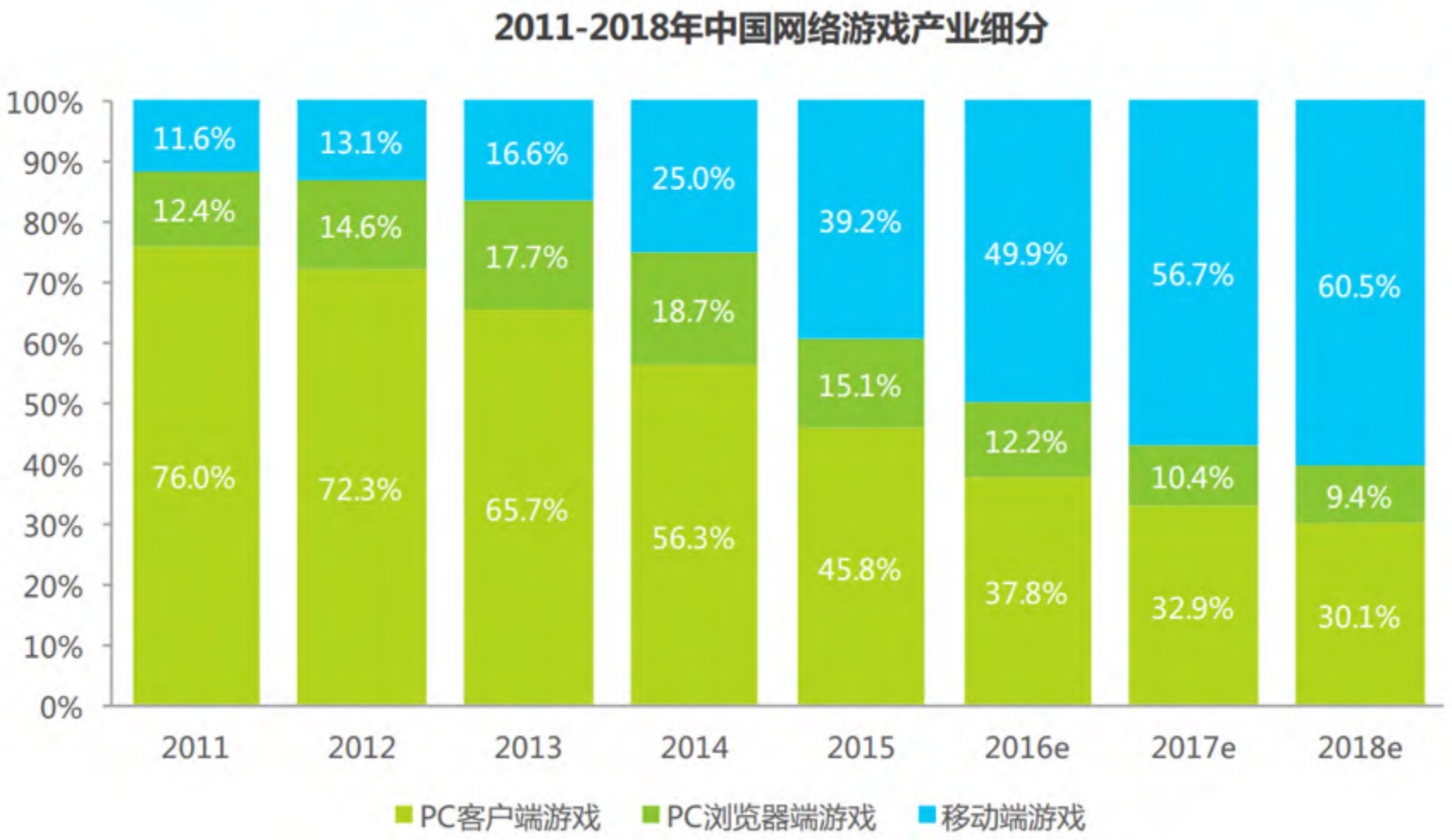

长江日报


成都全搜索
chengdu.cn


= 5MIN
= 15MIN
= 45MIN
= ∞


2011-2018年中国网络游戏市场规模
3,500
3,000
2,500
2,000
1,500
1,000
500
0
32.27%
24.56%
32.90%
23.92%
29.95%
27.41%
20.90%
13.76%
538.6
670.9
891.6
1104.9
1435.8
1829.3
2211.6
2515.9
2011
2012
2013
2014
2015
2016e
2017e
2018e
中国网络游戏市场规模（亿元）
增长率（%）

数据来源：艾瑞咨询

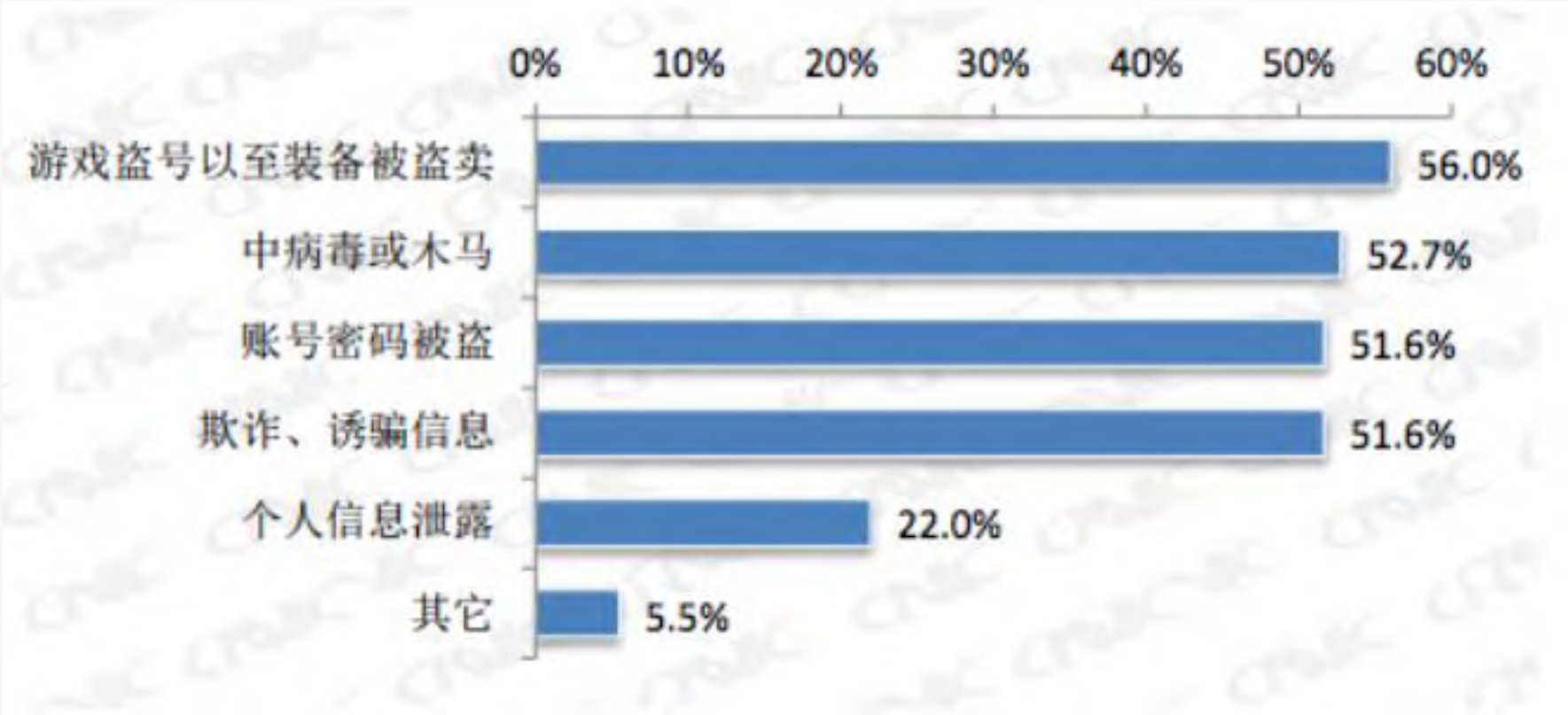

2011-2018年中国网络游戏产业细分
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
11.6%
12.4%
76.0%
13.1%
14.6%
72.3%
16.6%
17.7%
65.7%
25.0%
18.7%
56.3%
39.2%
15.1%
45.8%
49.9%
12.2%
37.8%
56.7%
10.4%
32.9%
60.5%
9.4%
30.1%
2011
2012
2013
2014
2015
2016e
2017e
2018e
PC客户端游戏
PC浏览器端游戏
移动端游戏

数据来源：艾瑞咨询

各种安全问题随之而来

那些年我们一起玩过的私服

你的装备被盗卖过吗？



数据来源：CNNIC 中国网民信息安全状况研究报告

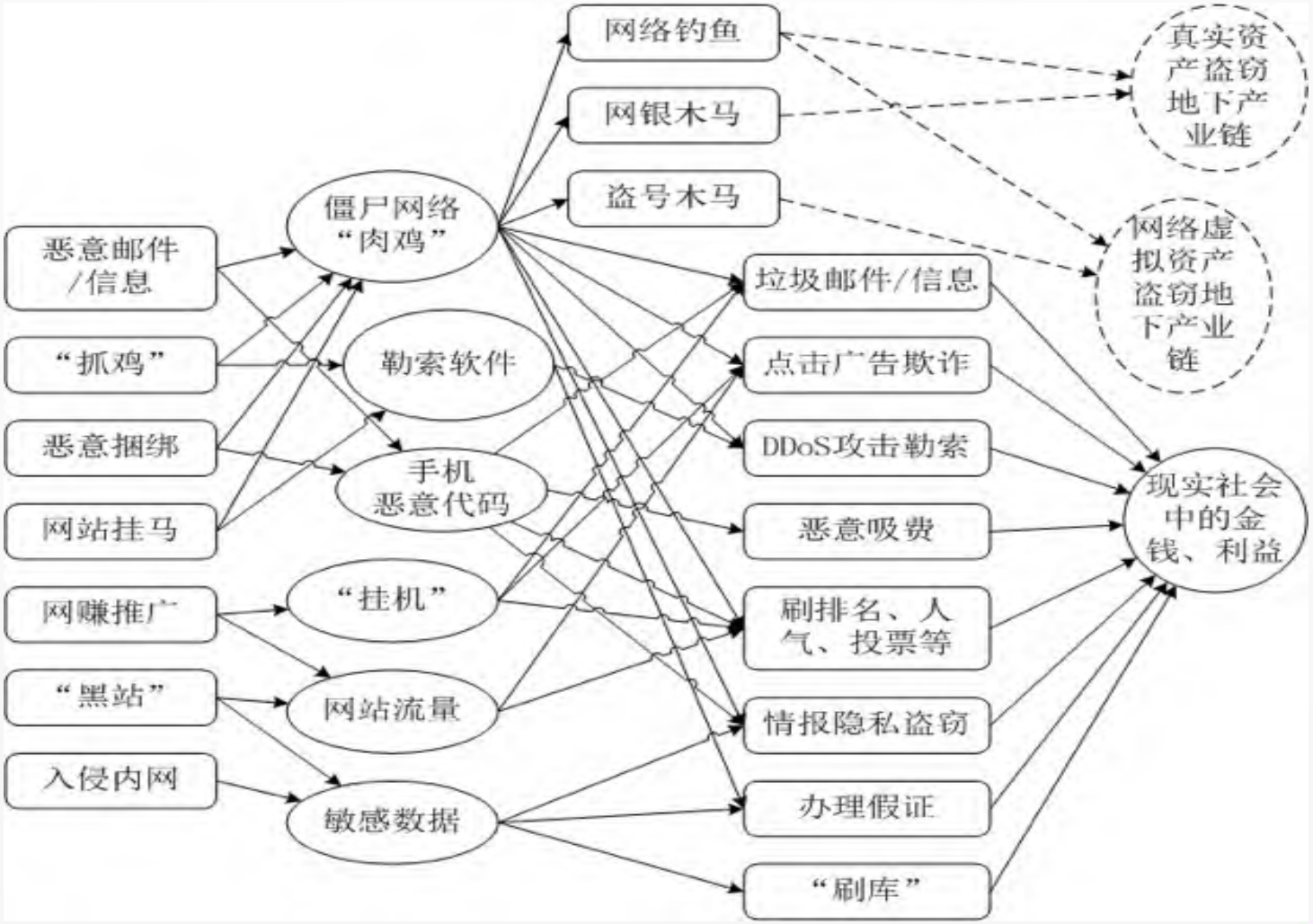

小海QQ盗号木马生成器
配置木马
收信账号:
等待
10000
毫秒后结束QQ
(1000毫秒为1秒)
木马模式:
防QQ2015登录界面
点击
3
次登录按钮后自动关闭木马
生成木马
使用教程
联系小海
测试收信


4399生死狙击小兮盗号器
对方账户
一键获取
目标正在准备！稍等
软件正在破译密码
破译80%

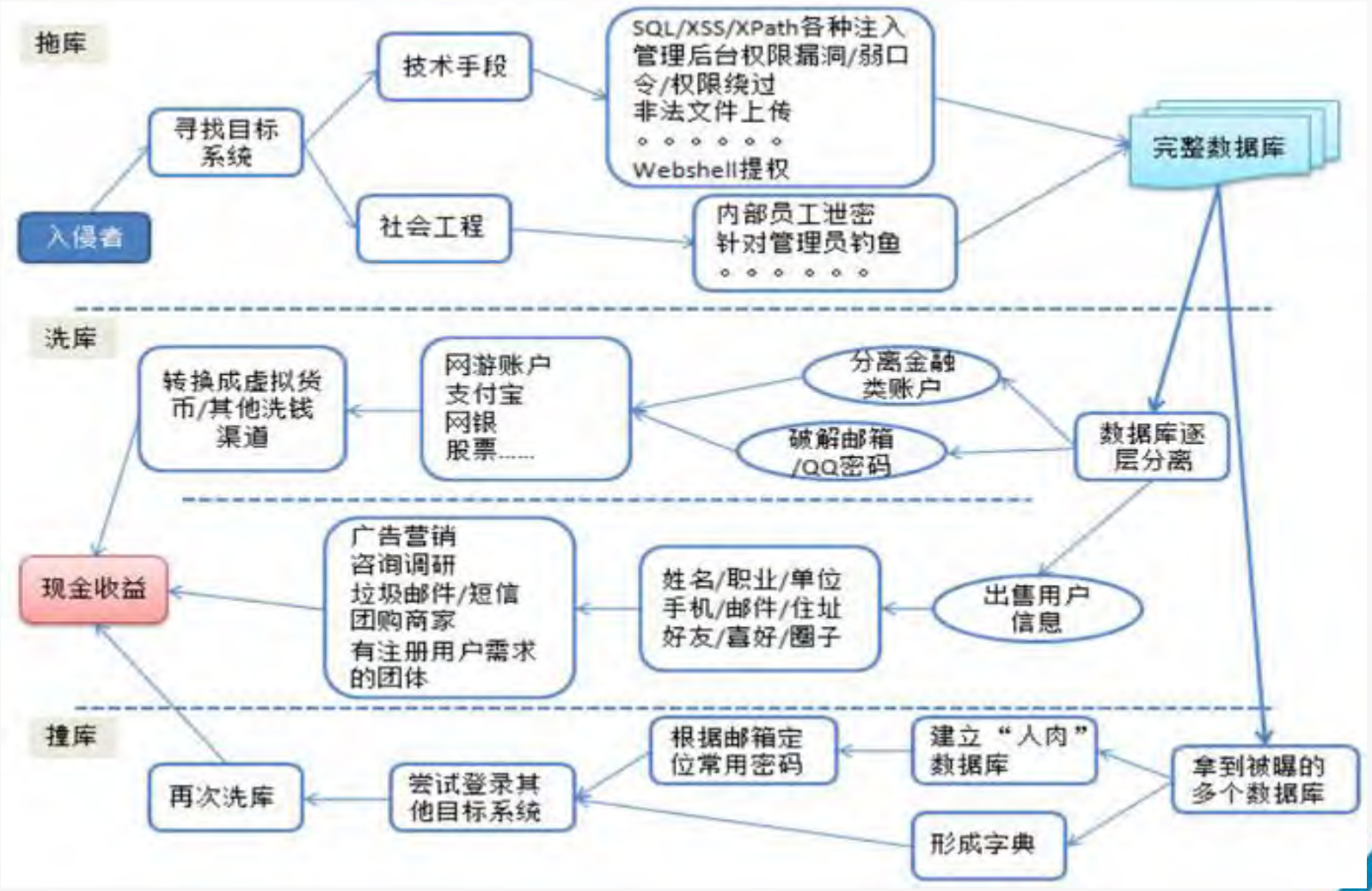
TiD2017

[illegible]	联系QQ	发布时间	地区/交易数量	类型	[illegible]	[illegible]	[illegible]
出售DNF黑信信封|剑灵	247088895	3月19日 16点发布	河南1000+	QQ信封黑信	支付宝交易	☆☆☆☆	查看
举报骗子	36810714	3月17日 22点发布	河北1000+	DNF黑信信封	支付宝交易	☆☆☆☆	查看
出售797k梯量	1373637988	3月15日 15点发布	广东其他	流量交易	支付宝交易	☆☆☆☆	查看
出售实力一手信	253919350	3月15日 15点发布	河北其他	DNF黑信箱子	支付宝交易	☆☆☆☆	查看
举报骗子	1600215585	3月14日 1点发布	辽宁1000+	DNF黑信箱子	支付宝交易	☆☆☆☆	查看
举报骗子	569316125	3月14日 1点发布	河北1000+	QQ信封黑信	支付宝交易	☆☆☆☆	查看
售网游信一手少量多次交易	3206370141	3月13日 17点发布	湖北1000+	DNF黑信信封	支付宝交易	☆☆☆☆	查看
制作刷信工具懂得来！	1009661955	3月13日 13点发布	北京100+	DNF黑信箱子	支付宝交易	☆☆☆☆	查看
实力一手dnf信箱三十折	253919350	3月12日 14点发布	吉林其他	DNF黑信箱子	支付宝交易	☆☆☆☆	查看
赵梦新	496095864	3月11日 2点发布	北京100+	DNF黑信箱子	支付宝交易	☆☆☆☆	查看
骗子QQ496095864	496095864	3月11日 2点发布	北京100+	QQ信封黑信	支付宝交易	☆☆☆☆	查看
【专业,安全,高效信封出售	2932472317	3月10日 11点发布	上海1000+	大话信封	支付宝交易	☆☆☆☆	查看
收魔兽数据	2375954887	3月10日 0点发布	北京其他	所有箱子	支付宝交易	☆☆☆☆	查看
举报骗子QQ	745832859	3月9日 18点发布	广东1000+	游戏箱子骗子	支付宝交易	☆☆☆☆	查看
247088895是骗子	3509641	3月8日 17点发布	河北其他	武林问道	网上银行交易	☆☆☆☆	查看
游戏信封|皇冠QQ信誉保障	529511314	3月8日 10点发布	湖北500+	DNF黑信箱子	支付宝交易	☆☆☆☆	查看
公布一个骗子QQ247088	52401520	3月7日 20点发布	北京100+	QQ信封黑信	支付宝交易	☆☆☆☆	查看
18.88永久话av群.	253919350最少每天更新50部	3月6日 15点发布	河北1000+	其它类别	支付宝交易	☆☆☆☆	查看
1万元押金担保卖家出信定	247088895	3月5日 22点发布	河南1000+	倩女幽魂	支付宝交易	☆☆☆☆	查看
✪押金2000卖家✪	253919350	3月2日 13点发布	河北1000+	DNF黑信箱子	支付宝交易	☆☆☆☆	查看

当黑客技术遭遇利益的诱惑

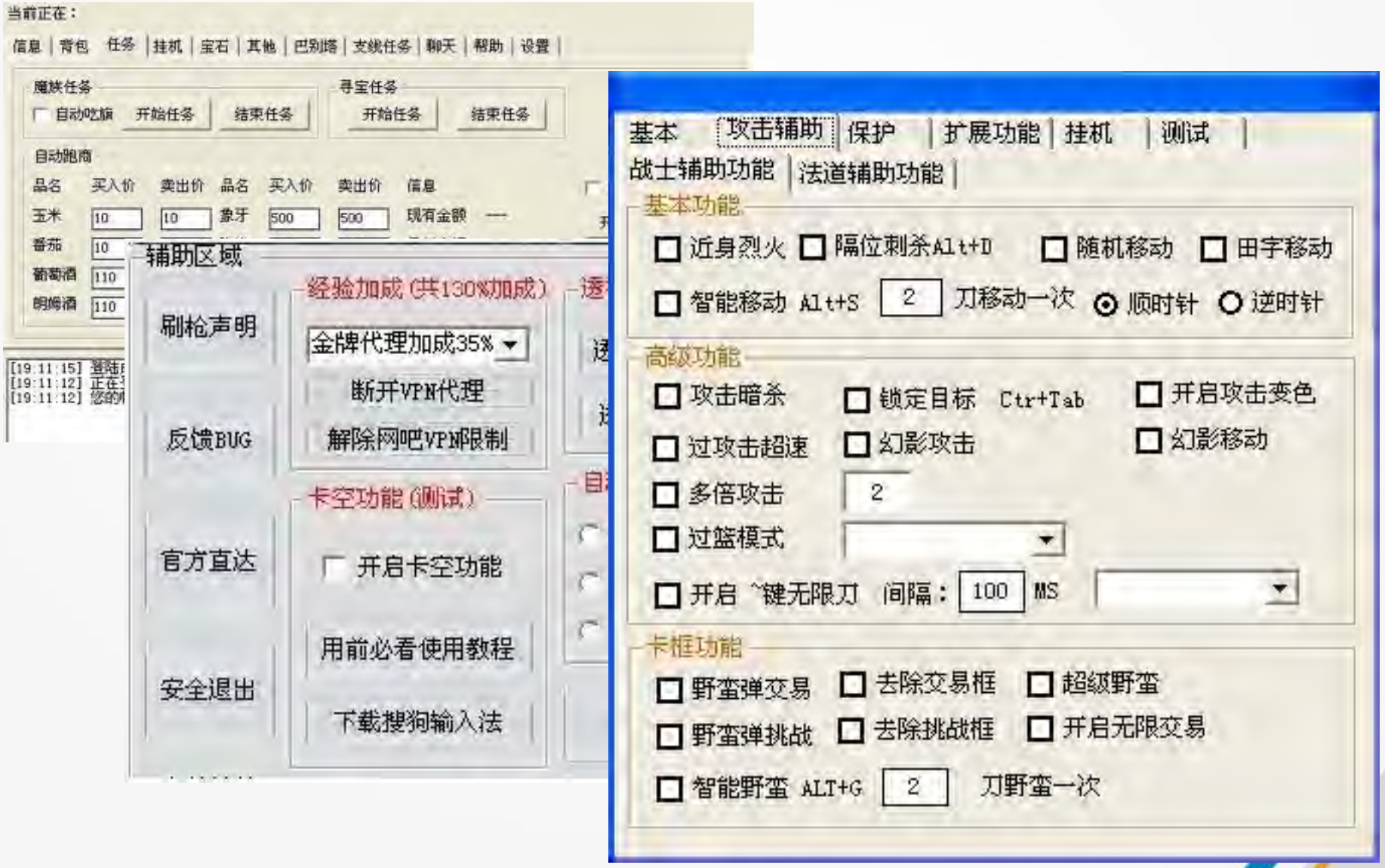


大数据时代，黑产可能比你自己还了解你



TiD2017

外挂——游戏平衡破坏者




郁金香...外挂技术
提供最专业游戏外挂相关资料
论坛 主页 外挂教程 免费教程 QQ咨询 相关工具下载 VIP学员办理 快速注册 获取金币 QQ群YY群 帮助 排行榜
热搜: 外挂教程 找CALL 找基址
论坛
郁金香 外挂开发(实战)
◆求市场玩家辅助销售代理权◆
最新主题
郁金香飞外挂科技公司
64位程序 输入16进制 printf f ...
游戏安全技术终极揭密教程--这个 ...
高稳定性高并发全平台社交聊天IM ...
2017版QQ密码窃取器免费版
可提现_手游_手机电玩城_手机捕 ...
可提现_手游_手机电玩城_手机捕 ...
有了它! 优酷、土豆、爱奇艺、乐 ...
无限制百度云盘下载神器，下载速 ...
翻墙神器蓝灯lantern 3.6.3破解 ...
高稳定性高并发全平台社交聊天IM ...
外挂视频教程相关(学员区)
001-C/C++语言教程
主题: 168, 帖数: 762
最后发表: 昨天 01:05
005-外挂制作(实战)
主题: 135, 帖数: 892
最后发表: 3 天前
手机游戏辅助软件
手机游戏辅助
玩游戏这档子事从来就不是规规矩矩的按游戏规则来的。相对来说，手机上的游戏在手机上运行更加的需要一些辅助工具来适应。小编整理的这个辅助大全是对游戏所有周边的一些用的着的工具进行了整理
资源不断补充中，欢迎提供建议
594个应用
合集列表
游戏蜂窝
小编推荐
掌上英雄联盟app
多玩我的世界盒子
最受欢迎
多玩饭盒(原多玩盒子)
叉叉助手
葫芦侠
版本: PC版 | 安卓版 | 苹果版

TiD2017

打金工作室——规模化

两男子出售DNF刷“金币”外挂 日入5万多元

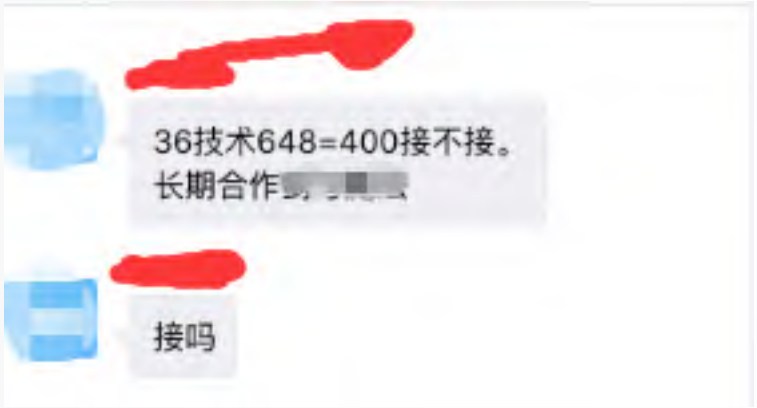
4月2日下午，网安支队在市公安局及铁人公安分局、让胡路公安分局、高新公安分局、龙凤公安分局的配合下，在萨尔图的某楼区和龙凤区的某小区，将正在使用外挂程序进行非法活动的辛某、张某等10名涉案成员抓获。当场缴获用于运行外挂程序的客户端简装计算机1.1万台，主控服务器120余台，扣押涉案车辆2台、现金7万余元、手机10余部及账本、银行卡若干，涉案财物总价值300余万元。

TiD2017

内容劫持——防不胜防

TiD2017

支付欺诈——无可奈何？



【传说】

专业教学60年。

带新人入行，包教包会，信誉保证，

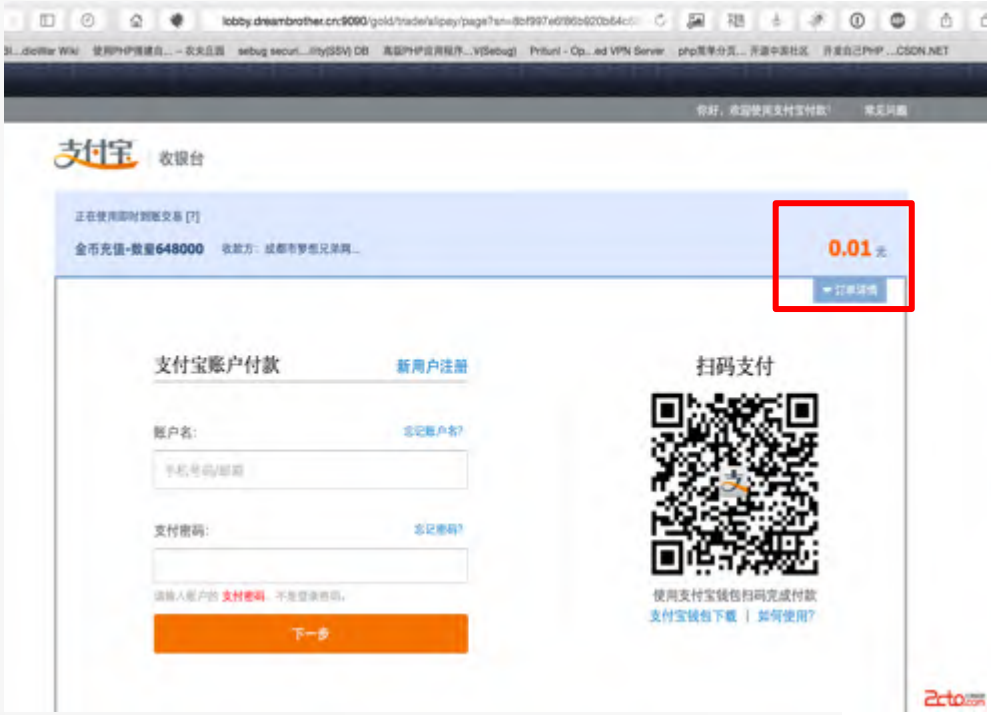
出苹果36技术，自撸自提app利润20 ➕

徒弟遍地是，欢迎加入

教苹果36 苹果648退款 软改硬改 八绑卡技术.支付宝技术，无限开支付宝技术。

破第三方

支付漏洞——坏人的提款机


支付宝 收银台
0.01 元
支付宝账户付款
新用户注册
账户名:
支付密码:
下一步
扫码支付
使用支付宝钱包扫码完成付款
支付宝钱包下载 | 如何使用?


Google
网游 支付漏洞
全部 新闻 图片 视频 地图 更多 设置 工具
找到约 4,210,000 条结果 (用时 0.74 秒)
百度网游存在支付漏洞| 安全脉搏
https://www.secpulse.com/archives/15527.html
利用网上支付系统漏洞获取不正当利益典型案例裁判规则 - 微博
weibo.com/ttarticle/p/show?id=2309404064926355331803
利用支付平台漏洞盗取网游点卡22岁青年获刑7年-中国法院网
www.chinacourt.org › 审判 › 刑事案件
网游防沉迷实名认证漏洞多移动端监管成空白|网络游戏|防沉迷系统_ ...
news.sina.com.cn/o/2016-10-31/doc-ifxxfuff7263691.shtml
利用支付平台漏洞盗取网游点卡青年获刑7年- 启东律师黄新宇 - 网站首页
www.hddls.net/case/510093.html
巨人被指诈骗洗钱安全支付漏洞还是刻意为之? _行业动态_投资界
news.pedaily.cn/201304/20130415346605.shtml
利用网游充值漏洞小伙下千万元订单-搜狐IT - 搜狐科技
it.sohu.com › 互联网 › 国内互联网

安全真是一个令人头疼的事.....

未知攻焉知防！

安全问题的根源

外因（威胁） VS 内因（脆弱性）

外因：小偷

内因：锁被绕过


网络黑产
56万人
1482亿元
26.5万元

外因：面临威胁


这些可以卖钱~
IP


不滿解雇 俄員工開怪手拆飛機洩恨


1010
0101
110

TiD2017

Apache

Java

Microsoft .NET Framework

OpenSSL

NGINX

php

glibc

Image magic

mongoDB

MySQL

hadoop

elasticsearch

cisco

H3C

DELL

Microsoft SQL Server

Windows Server 2012

cassandra

redis

CentOS

vmware

iOS

机房

拔错网线
拔错电源线
rm -fr /
错误配置
reboot ->halt
配错ip / 路由。。
误操作

密码明文文件
打包www.rar
xxx.log
不良习惯

无意泄漏
中木马
ftp登录（明文）
特权账号 / 用户

123456 password 12345678 123456789 qwerty 12345

内因：脆弱性

Office

EMAIL

办公场所

需要从不同视角进行威胁分析

宏观视角

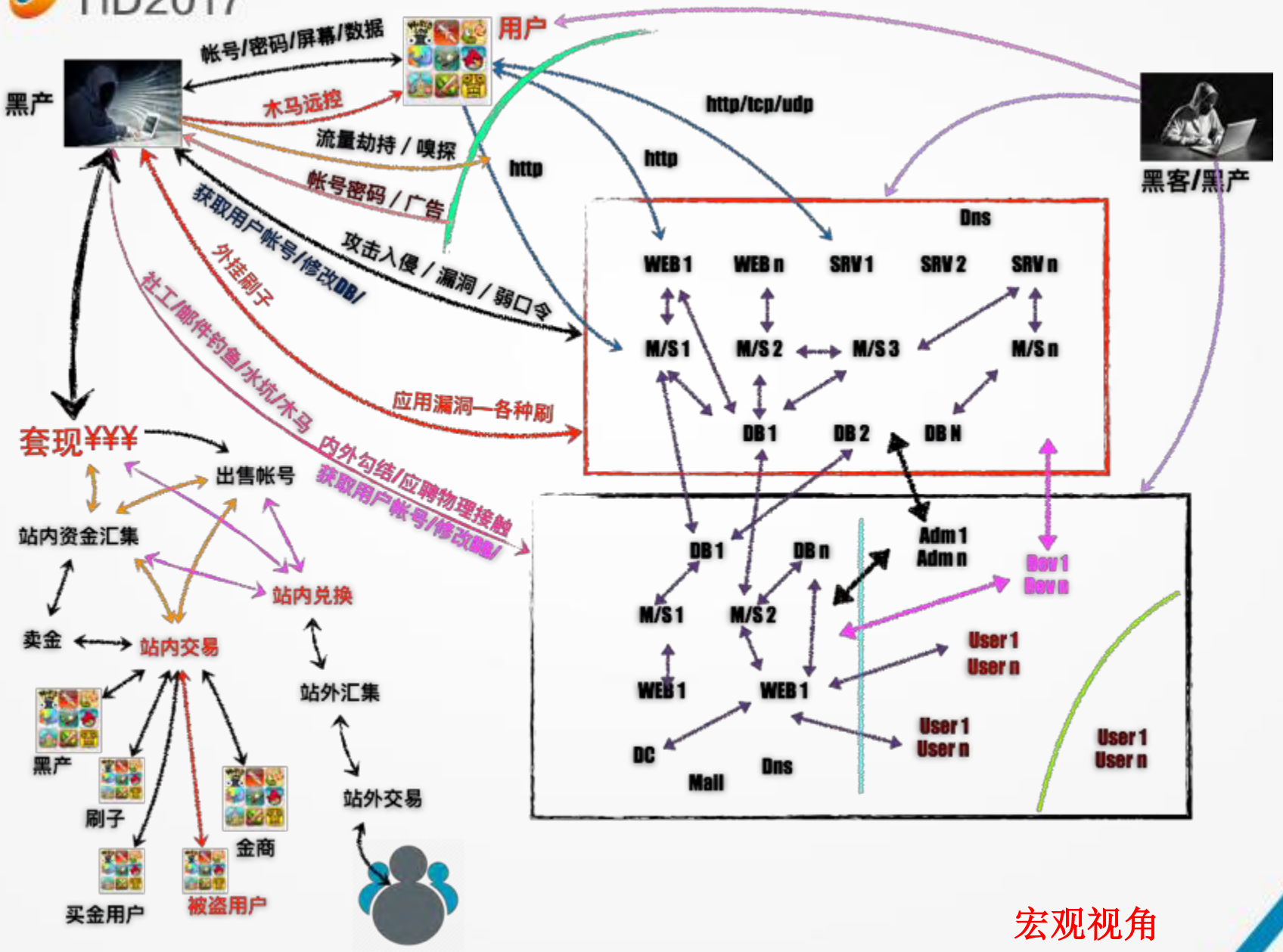
安全管理者视角：宏观掌控安全威胁，从宏观上规划设计技术控制、管理控制。

战略

微观视角

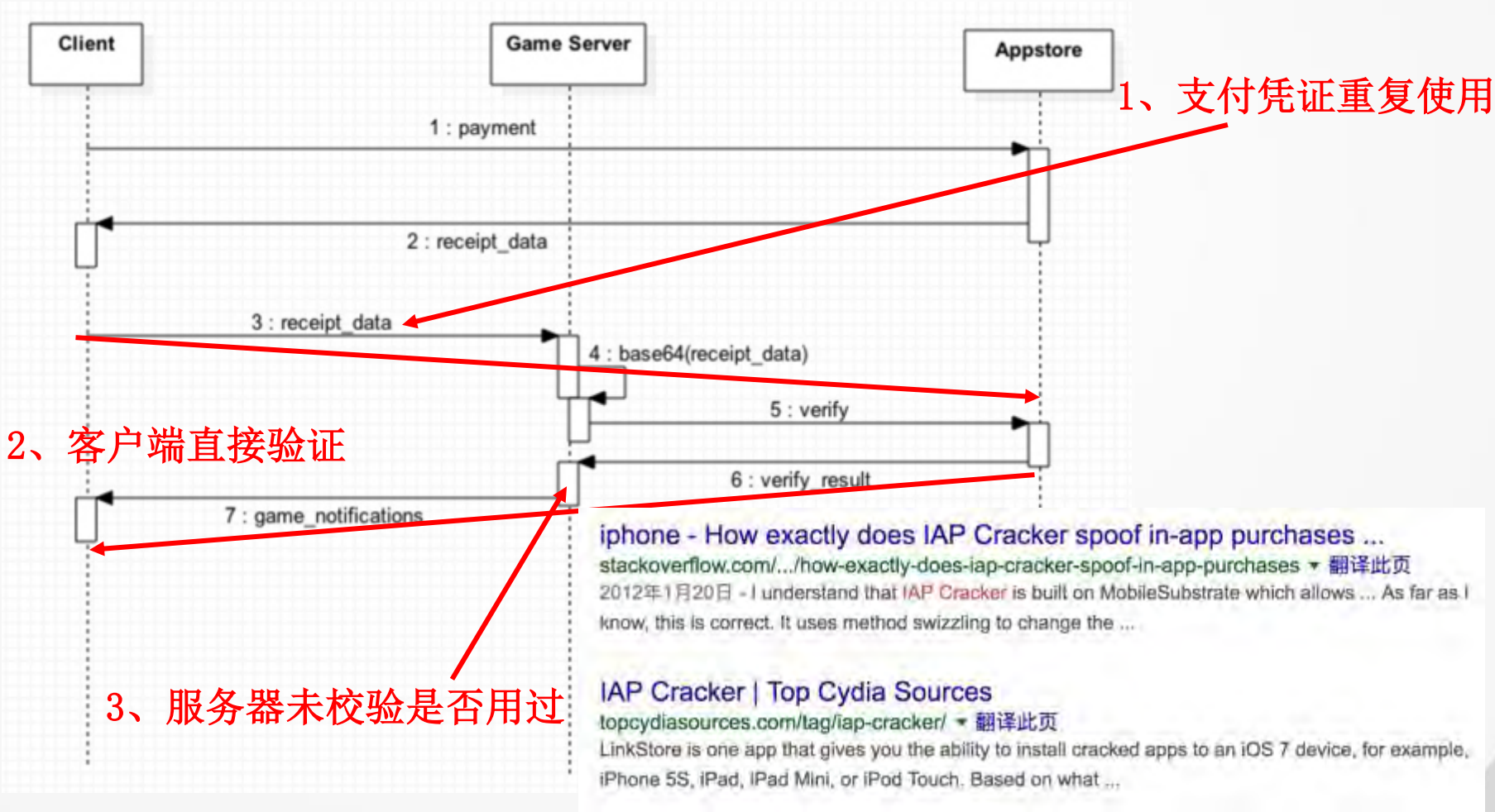
安全工程师视角：掌控具体的安全问题，技术控制细节，管理控制细节。

战术


用户
帐号/密码/屏幕/数据
黑产
木马远控
流量劫持 / 嗅探
帐号密码 / 广告
获取用户帐号/修改DB/
攻击入侵 / 漏洞 / 弱口令
外挂刷子
社工/邮件钓鱼/水坑/木马
应用漏洞—各种刷
内外勾结/应聘物理接触
获取用户帐号/修改DB/
http
http
http/tcp/udp
黑客/黑产
Dns
WEB 1
WEB n
SRV 1
SRV 2
SRV n
M/S 1
M/S 2
M/S 3
M/S n
DB 1
DB 2
DB N
套现¥¥¥
出售帐号
站内资金汇集
站内兑换
卖金
站内交易
站外汇集
站外交易
黑产
刷子
金商
买金用户
被盗用户
DB 1
DB n
Adm 1
Adm n
Dev 1
Dev n
M/S 1
M/S 2
User 1
User n
WEB 1
WEB 1
User 1
User n
DC
Dns
Mail
User 1
User n

宏观视角

支付威胁分析：苹果IAP威胁分析

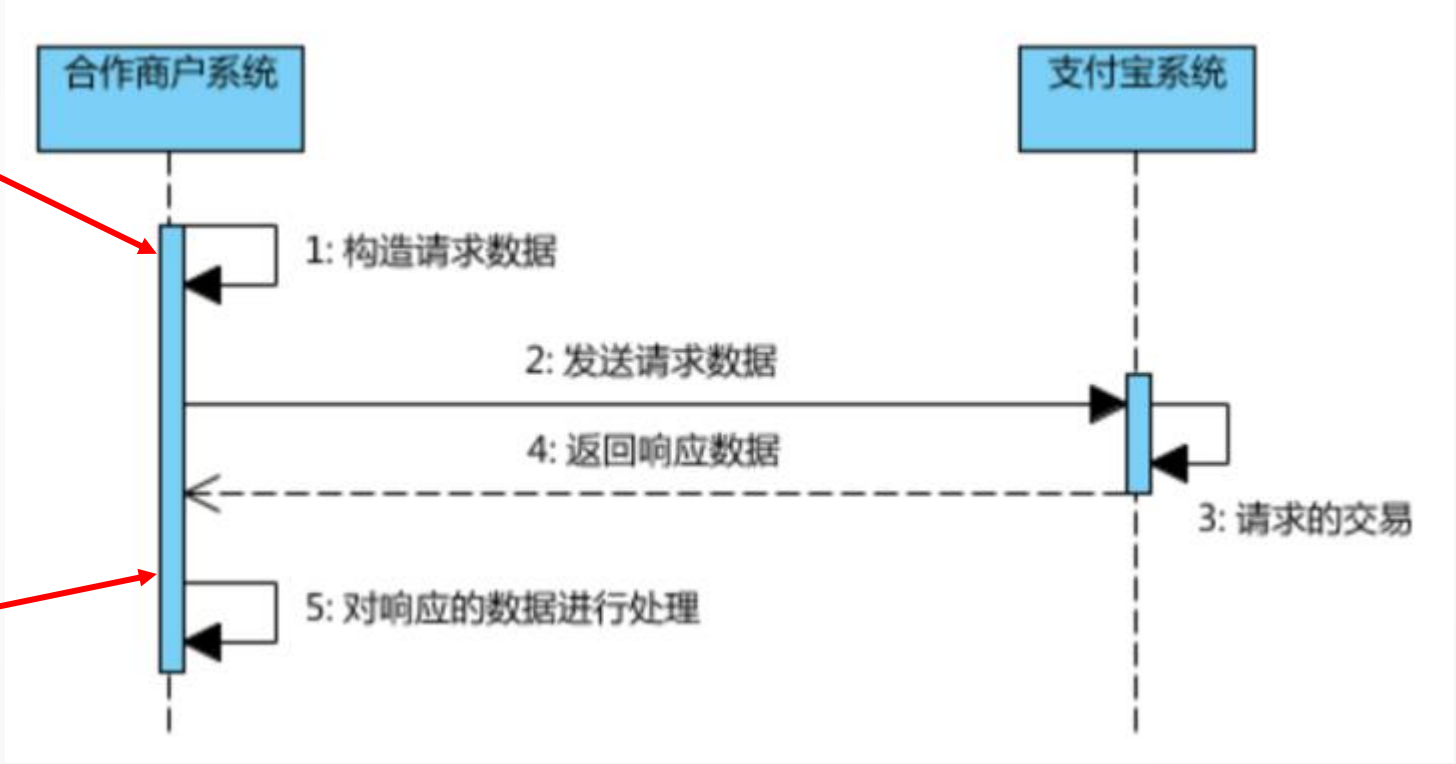


微观视角

支付威胁分析：第三方支付

使用客户端提交数据构造请求数据

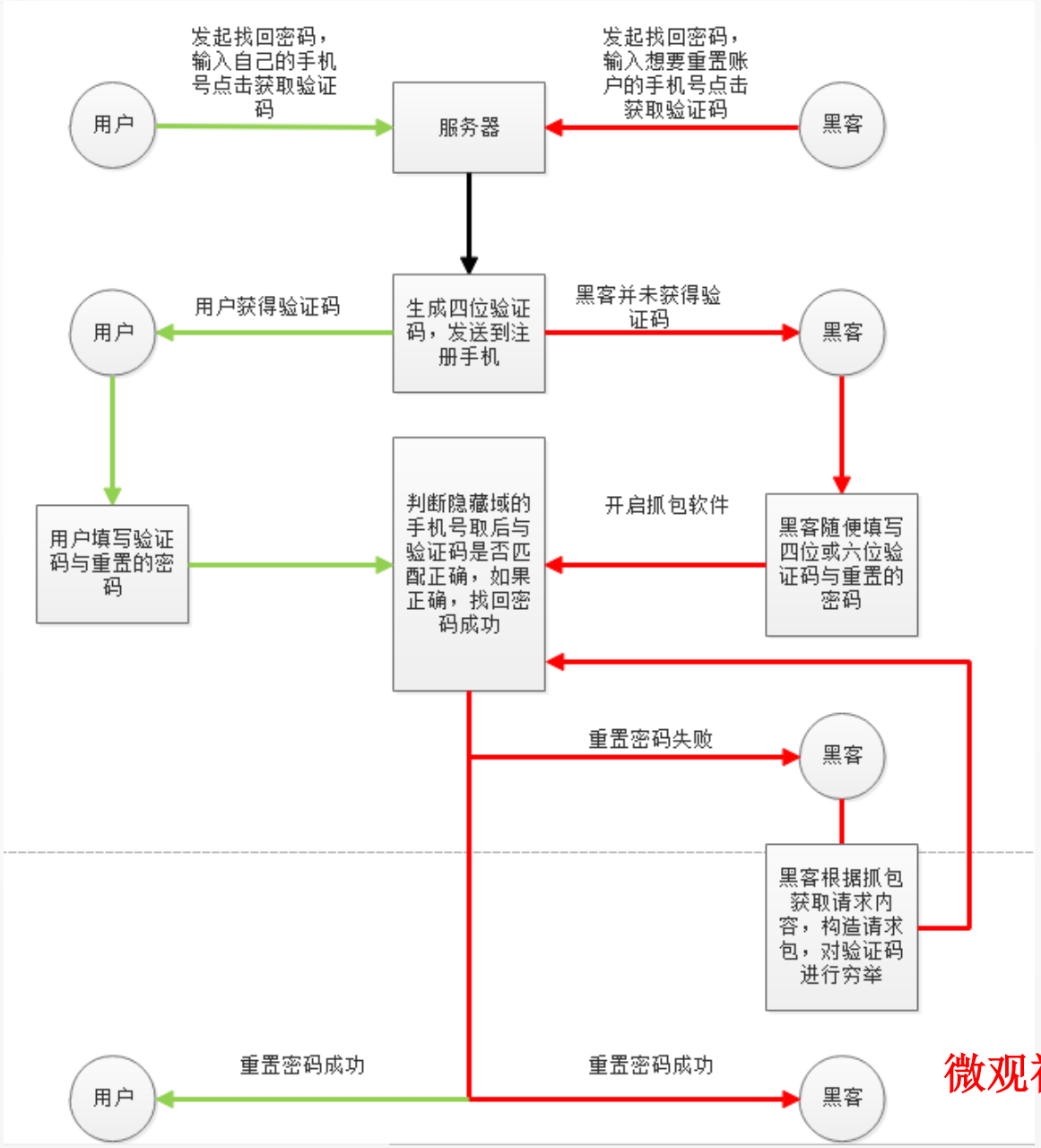
未进行有效性校验



微观视角

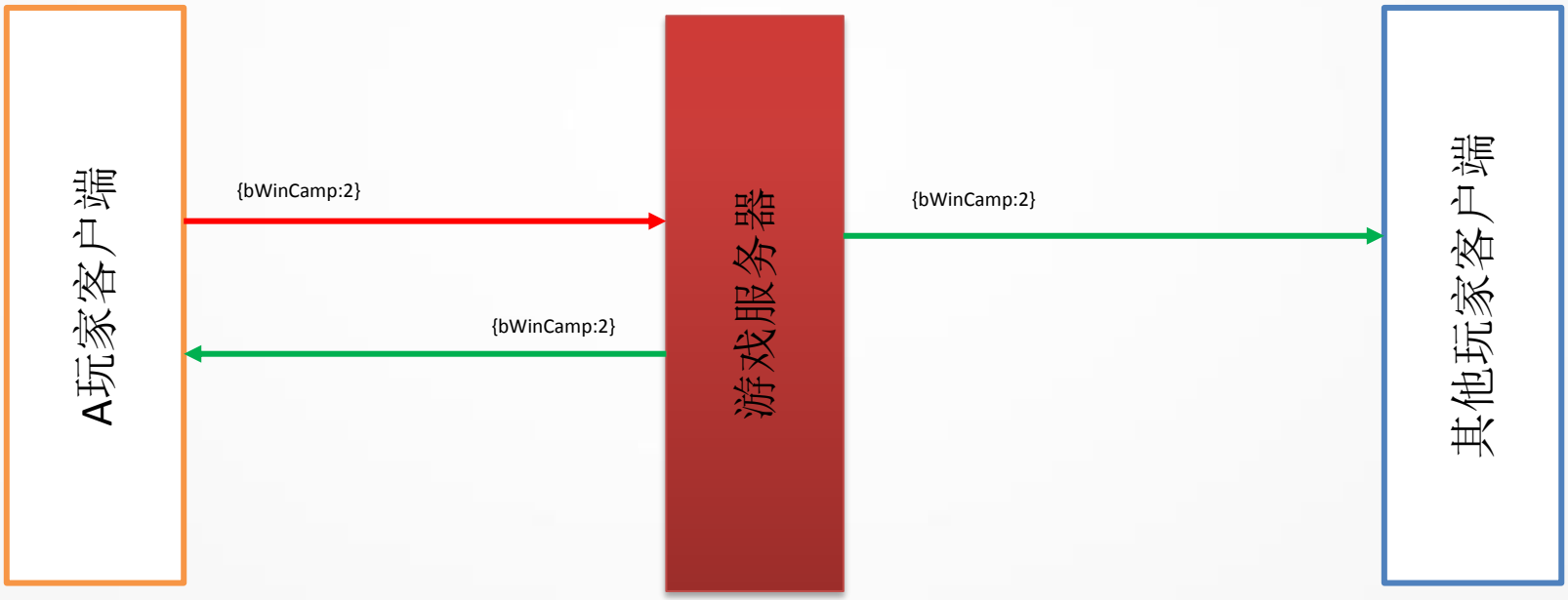
TiD2017

密码找回功能威胁分析



微观视角

游戏逻辑漏洞威胁分析: 协议漏洞



服务器信任客户端协议，广播该协议，对方阵营投降

又是宏观又是微观，到底咋干？

几个概念

未知攻，焉知防

安全最大化

适度防护

业务影响最小化

人是最薄弱环节

几个假设

漏洞一定存在

不是所有的漏洞都能补

已被入侵

内部威胁存在

防患未然

以**适当**的成本构建一系列**控制**措施（管理＋技术），将风险降低到可接受程度。

主动防御

+

亡羊补牢

以**适当**的成本构建一系列**监控**措施，及时监控脆弱性被利用情况，迅速响应，事后分析，持续改进。

检测响应

威胁源

黑客：攻击手段研究；特征检测；情报、线下打击

黑产：攻击手段研究、对抗；特征检测；线下打击

竞争对手：取证；法律；PR

玩家：游戏公平；PR

内部威胁：教育；权限；监控；审计

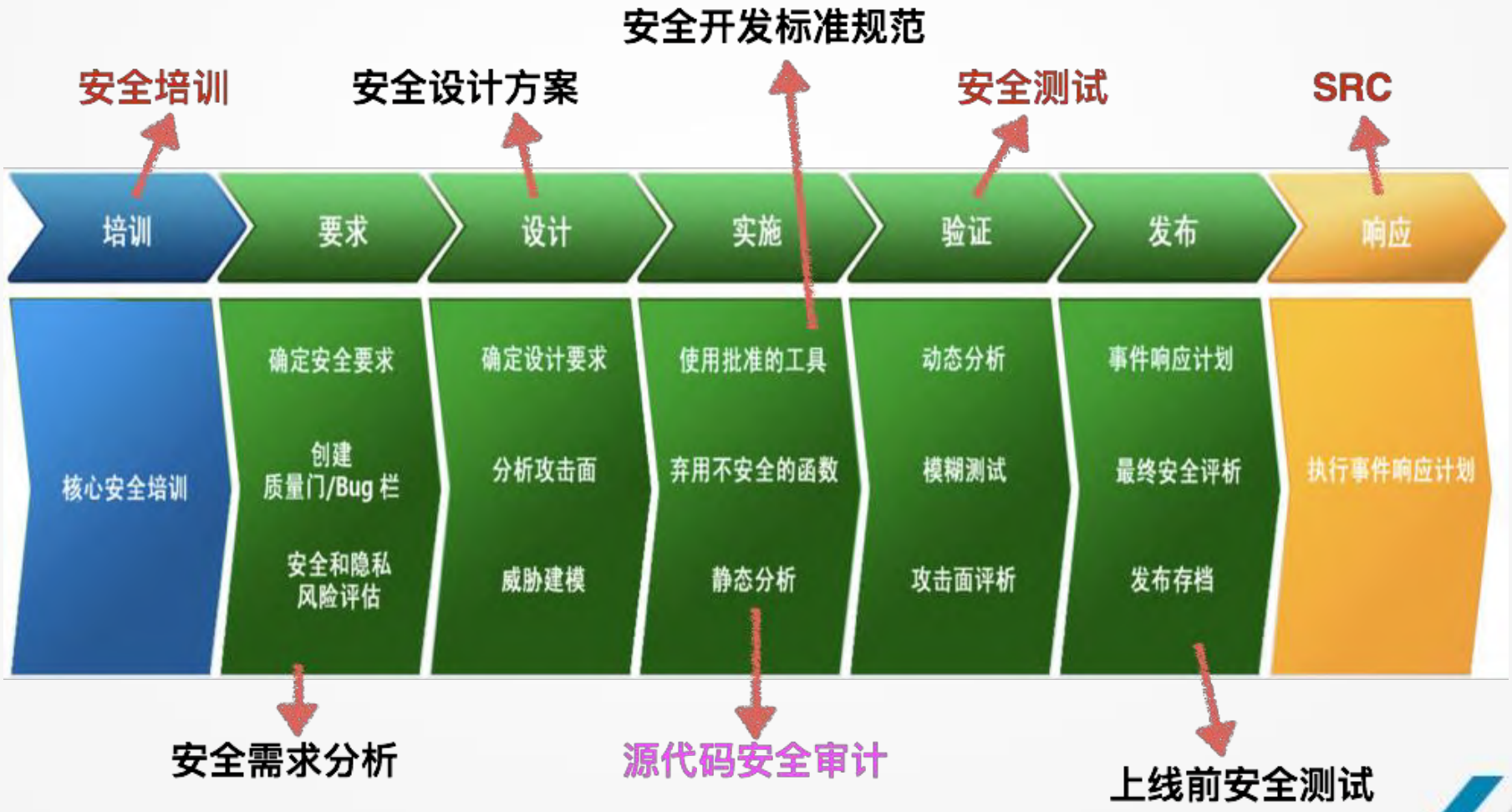
职业黑客：特征检测；内功；监控

自然灾害：应急预案；业务连续性计划；灾备


业务运营
系统运维
IT运维
业务系统
办公软件
基础软件
脆弱性
网络架构
系统架构
IT架构
硬件设备
物理环境
识别手段
缓解措施
预防措施
安全风险评估
安全测试
订阅漏洞信息
补丁更新
漏洞修复
架构调整
部署安全设备
安全加固
安全开发
安全开发标准规范
安全需求分析
安全培训
安全管理制度支持

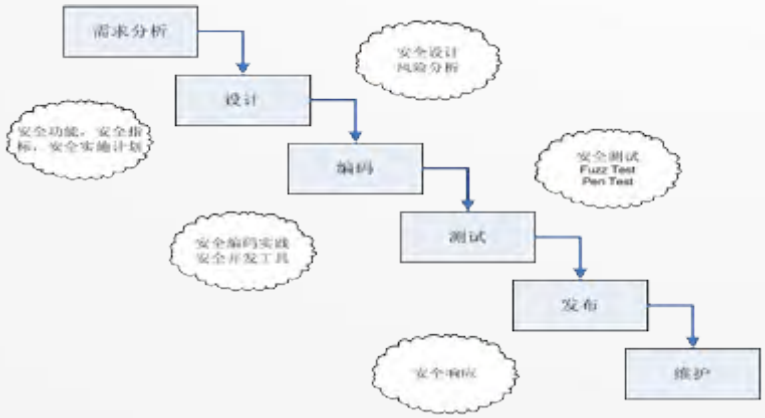

过程类
安全风险评估
权限控制
自动化运维
安全意识教育
安全培训
安全操作规范
安全管理制度
业务系统类
安全风险评估
安全测试
漏洞修复
安全设备
安全开发
安全开发标准规范
安全需求分析
安全培训
第三方软件类
安全风险评估
订阅漏洞信息
漏洞扫描
补丁更新
安全设备
安全加固
安全配置规范
安全意识教育
架构类
安全风险评估
架构调整
安全设备
访问控制
高可用性
安全需求分析
物理环境类
安全风险评估
访问控制
防火防盗
防水防潮
硬件生命周期管理
机房管理规范
大厦管理规定

Security Development Lifecycle



时间紧，任务重，BUG都修不完，还搞这么复杂？！

安全 VS 敏捷


需求分析
设计
编码
测试
发布
维护
安全设计
风险分析
安全测试
Fuzz Test
Pen Test


需求
测试
迭代1
开发
设计
发布
需求
测试
迭代1
开发
设计
发布
需求
测试
迭代1
开发
设计

游戏通讯协议被破解？

刷游戏币漏洞？

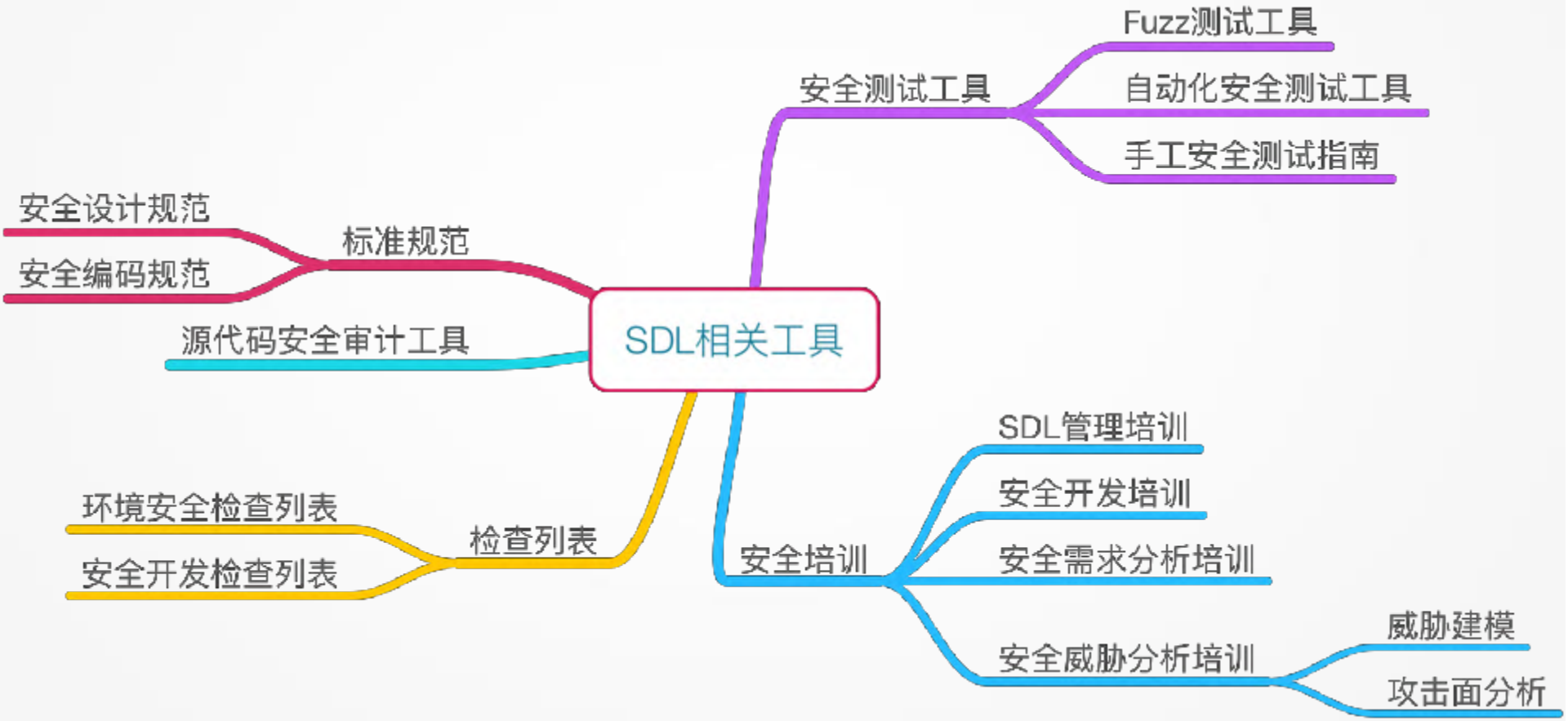
服务器漏洞导致入侵？

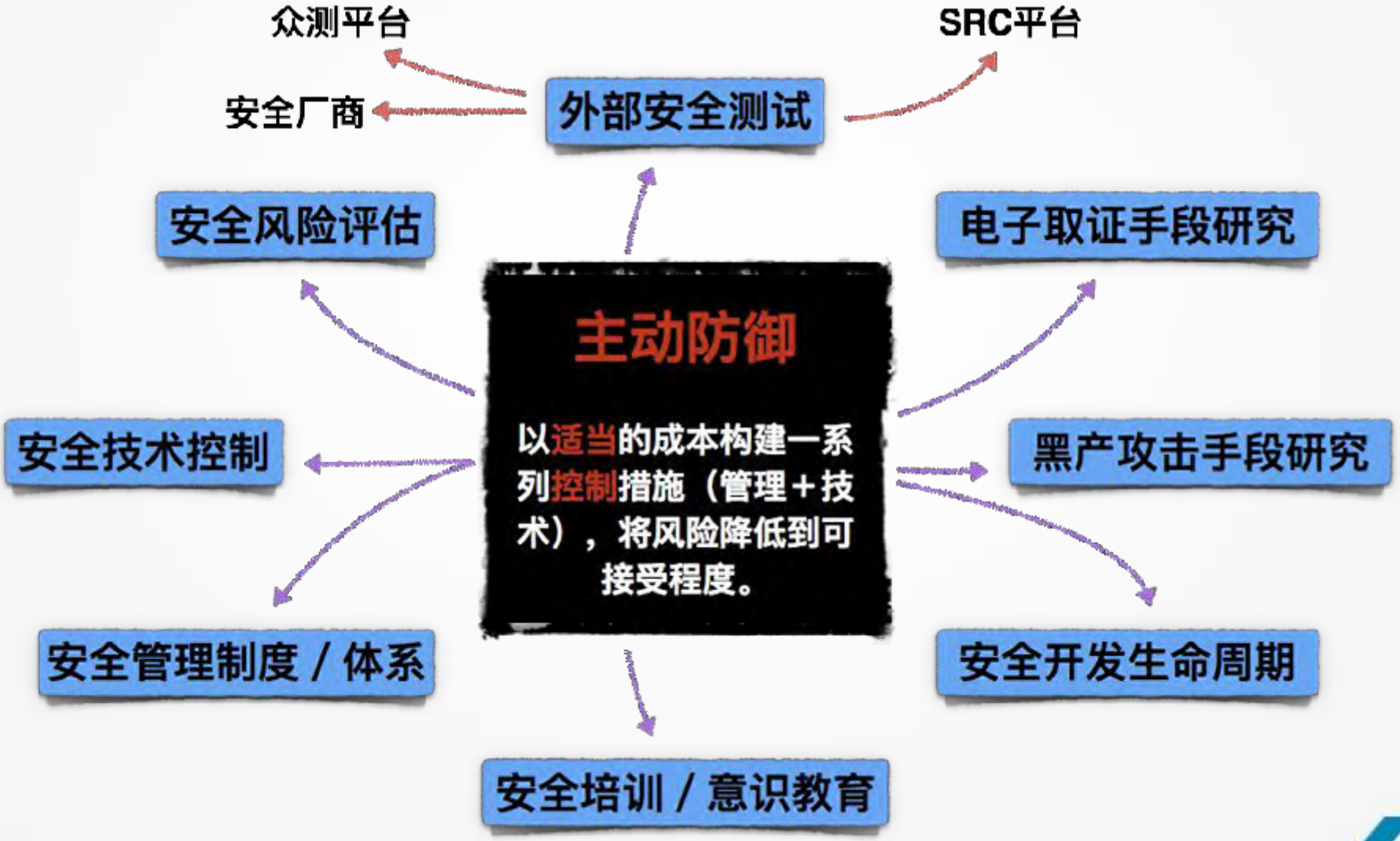
接口泄漏用户隐私？

越权操作别人账户？

很多时候损失惨重之后才会吸取教训！

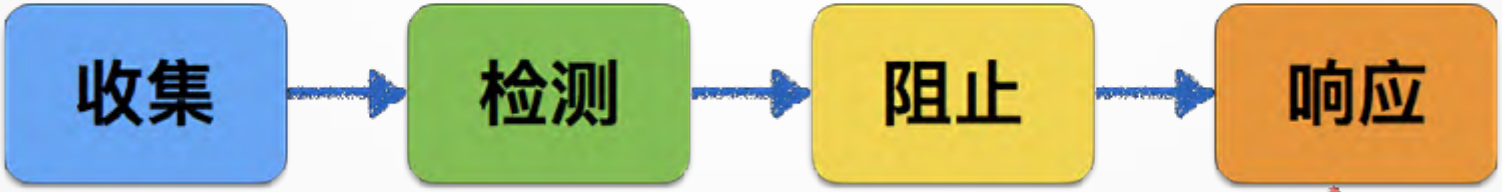
Security Development Lifecycle



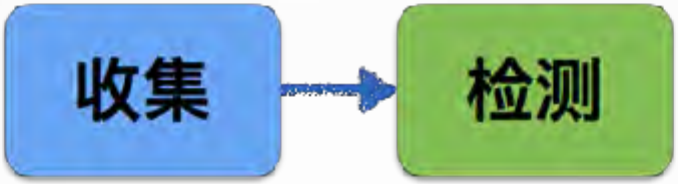

众测平台
SRC平台
外部安全测试
安全厂商
安全风险评估
电子取证手段研究
主动防御
以适当的成本构建一系列控制措施（管理＋技术），将风险降低到可接受程度。
安全技术控制
黑产攻击手段研究
安全管理制度／体系
安全开发生命周期
安全培训／意识教育

检测响应

以适当的成本构建一系列监控措施，及时监控脆弱性被利用情况，迅速响应，事后分析，持续改进。



主动防御



操作系统日志	网络设备日志	客服系统日志
数据库日志	DNS日志	后台系统日志
WEB服务器日志	域控日志	业务系统日志
办公客户端日志	邮件日志	游戏行为日志
操作系统进程信息	网络数据	游戏终端采集信息
操作系统账号信息	蜜罐捕获数据	交易数据

安全人员经验

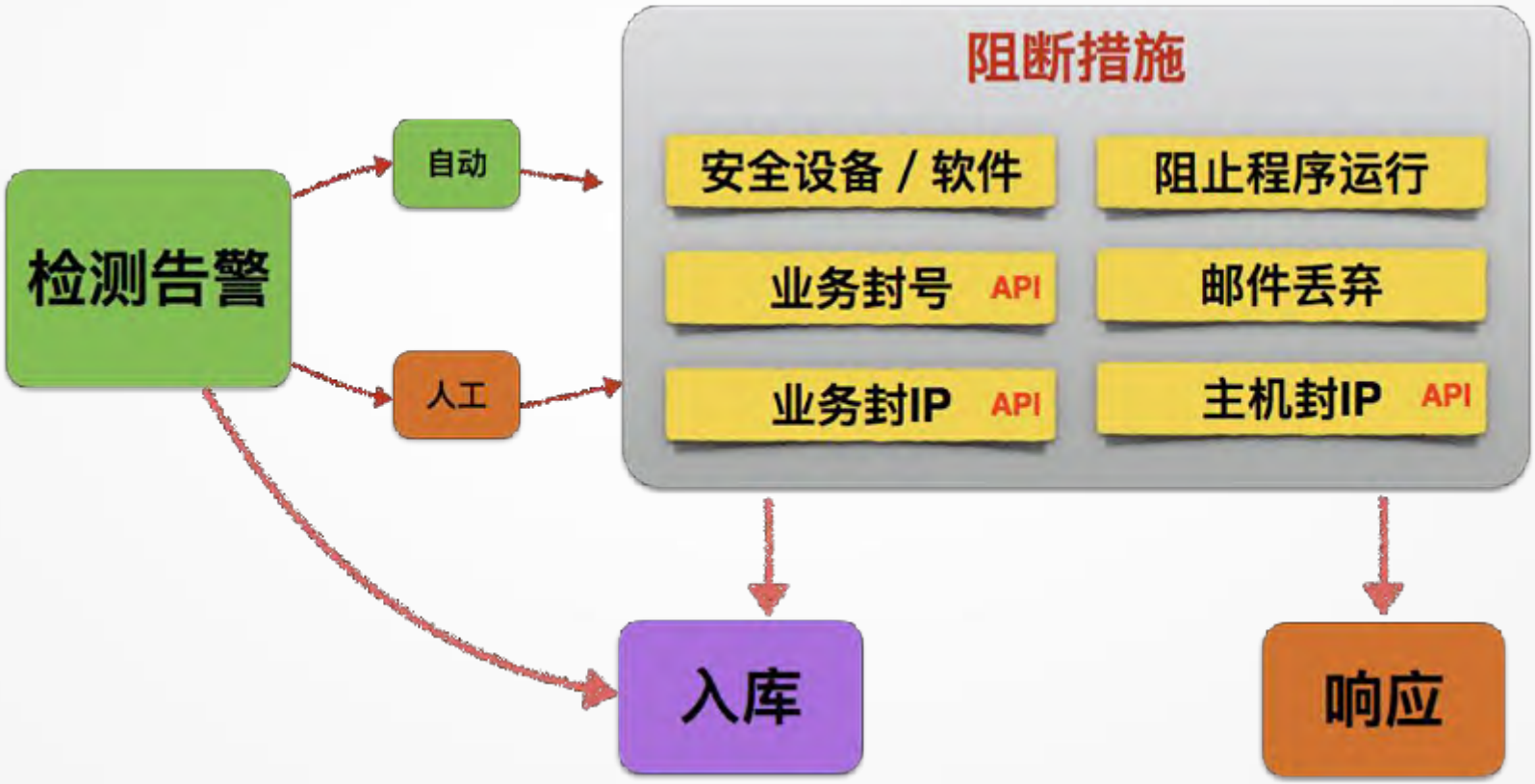
异常 / 统计模型

机器学习

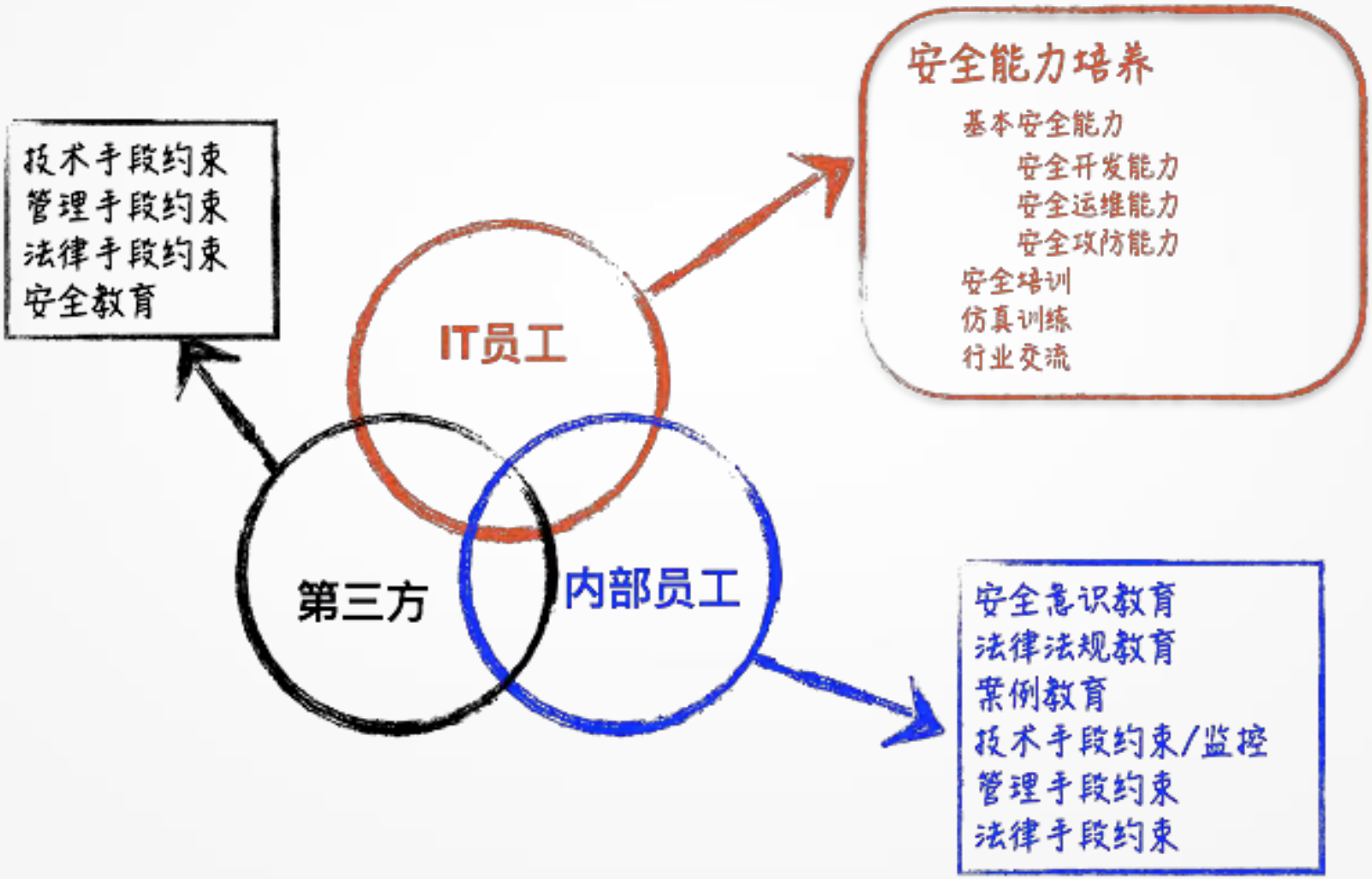
特征匹配

虚拟执行

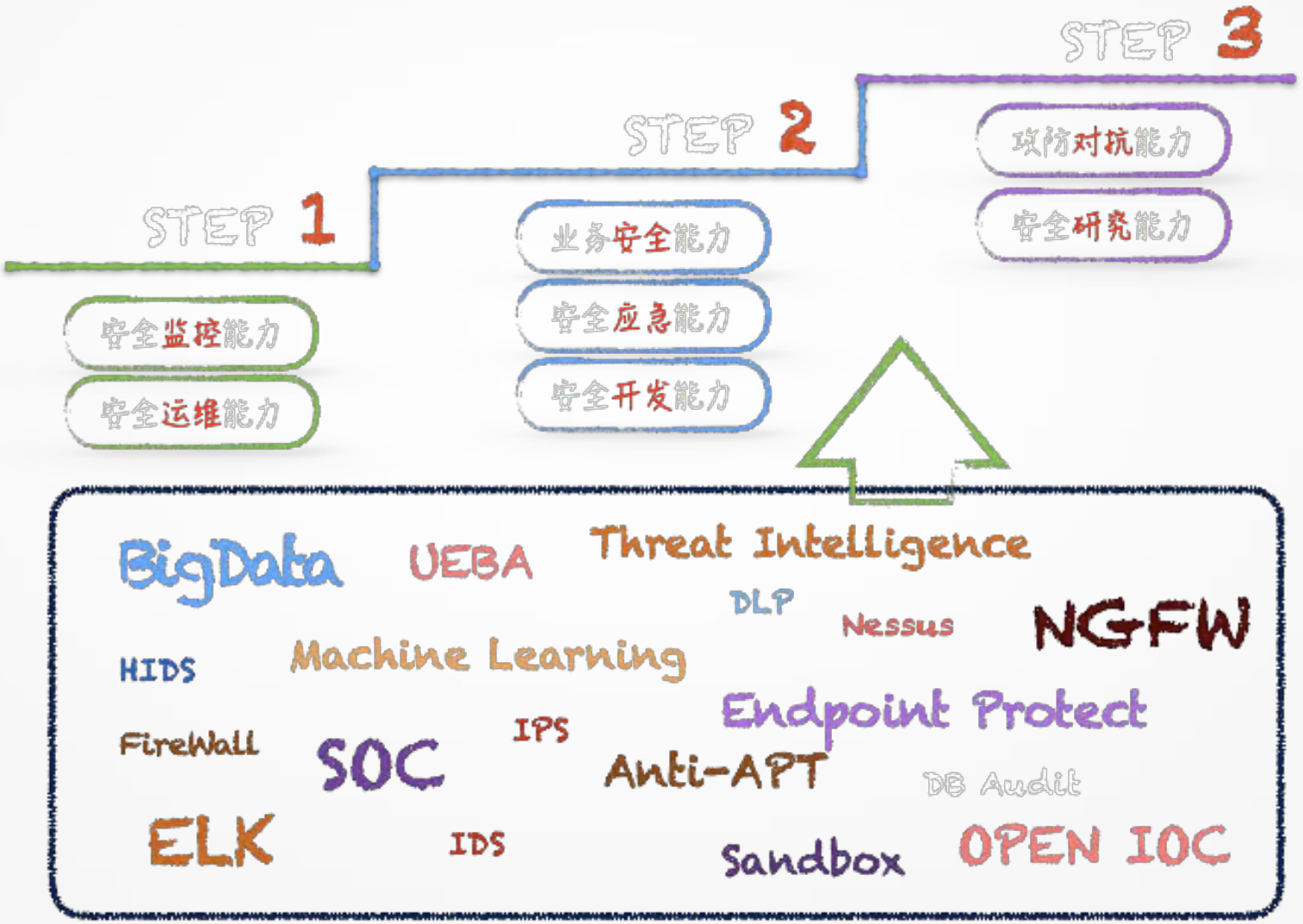
陷阱——蜜罐


检测告警
自动
人工
阻断措施
安全设备 / 软件
阻止程序运行
业务封号 API
邮件丢弃
业务封IP API
主机封IP API
入库
响应

人是“安全”中的关键要素


技术手段约束
管理手段约束
法律手段约束
安全教育
IT员工
第三方
内部员工
安全能力培养
基本安全能力
安全开发能力
安全运维能力
安全攻防能力
安全培训
仿真训练
行业交流
安全意识教育
法律法规教育
案例教育
技术手段约束/监控
管理手段约束
法律手段约束


攻防对抗能力
安全研究能力
业务安全能力
安全应急能力
安全开发能力
安全监控能力
安全运维能力
大数据、ML
恶意代码分析
威胁情报平台
蜜罐系统
渗透工具平台
入侵检测系统
源码审计工具
漏洞扫描工具
仿真演练环境
日志分析平台
漏洞挖掘
安全研究
安全监控
业务安全
安全培训


STEP 1
安全监控能力
安全运维能力
STEP 2
业务安全能力
安全应急能力
安全开发能力
STEP 3
攻防对抗能力
安全研究能力
BigData
UEBA
Threat Intelligence
DLP
Nessus
NGFW
HIDS
Machine Learning
Endpoint Protect
FireWall
SOC
IPS
Anti-APT
DB Audit
ELK
IDS
Sandbox
OPEN IOC

合作

共赢


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
merci
obrigado
dziękuję
bedankt
спасибо
go raibh maith agat
mochchakkeram
sukriya
kop khun krap
arigatô
dakujem
grazie
terima kasih
감사합니다
ありがとう
ευχαριστώ
мерси
рахмат
Баярлалаа
dank je
mersi
barka
welalin
tack
spas
kia ora
vinaka
спасибі
blagodaram
misaotra
matondo
paldies
faafetai lava
kiitos
dankie
mauruuru
hvala
köszönöm
akun dankon
chnorakaloutioun
gracies
sulpay
taiku
takk
trugarez
shukriya
dhanyavadagalu
diolch
xièxie
rahmet
tanemirt
najis tuke
kam sah hamnida
sagolun
dekuji
sobodi
mèsi
enkosi
bayarlalaa
gràcie
nandri
tapadh leat
хвала
asante
manana
murakoze
mamnun
дякую
djiere dieuf
tau
tenki
nanni
rahmet