


# 在线游戏企业 安全建设之路




仲维国@竞技世界

下一代  
软件研发  
SOFTWARE  
DEVELOPMENT



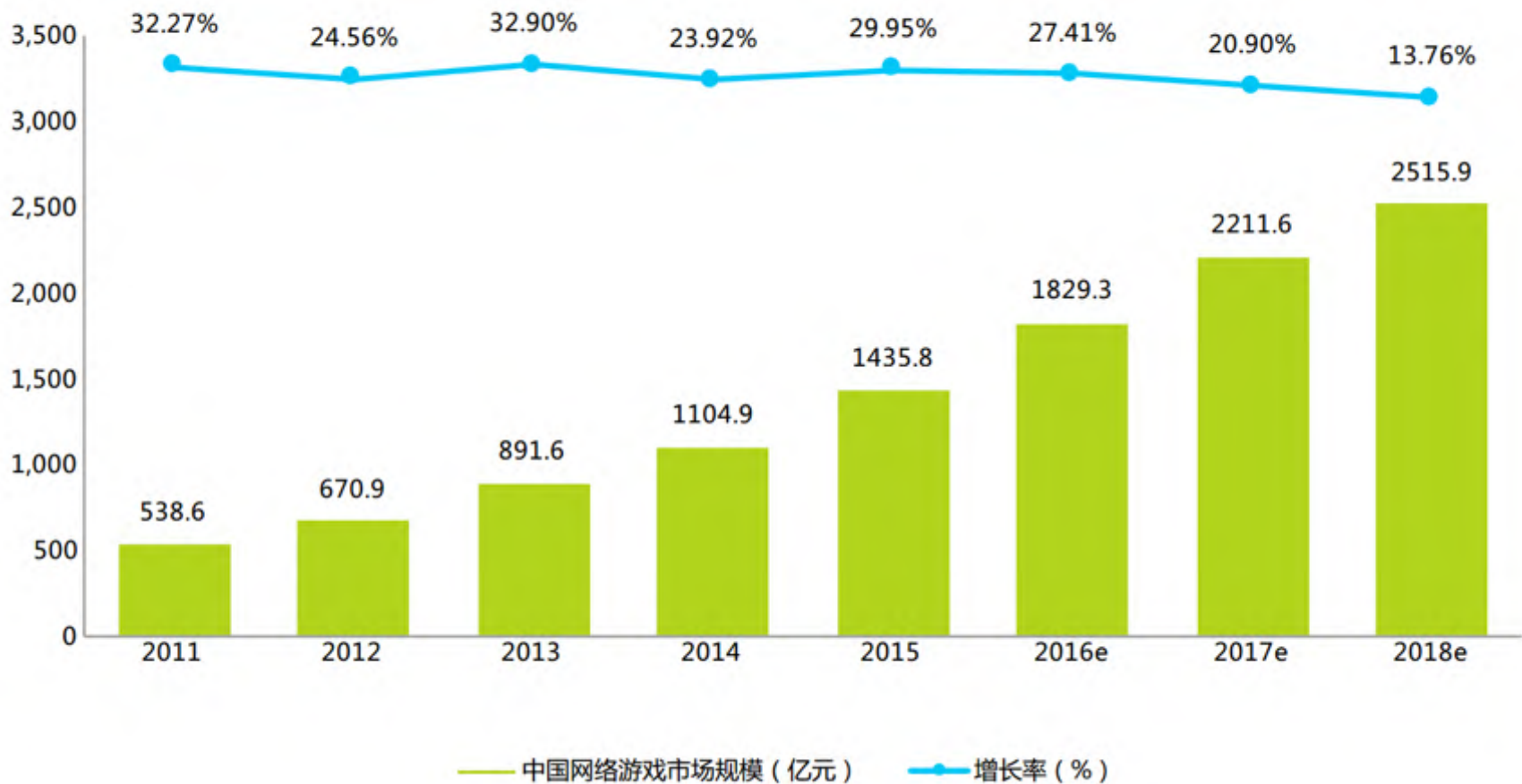
 = 5min

 +  = 15min

 +  +  = 45min

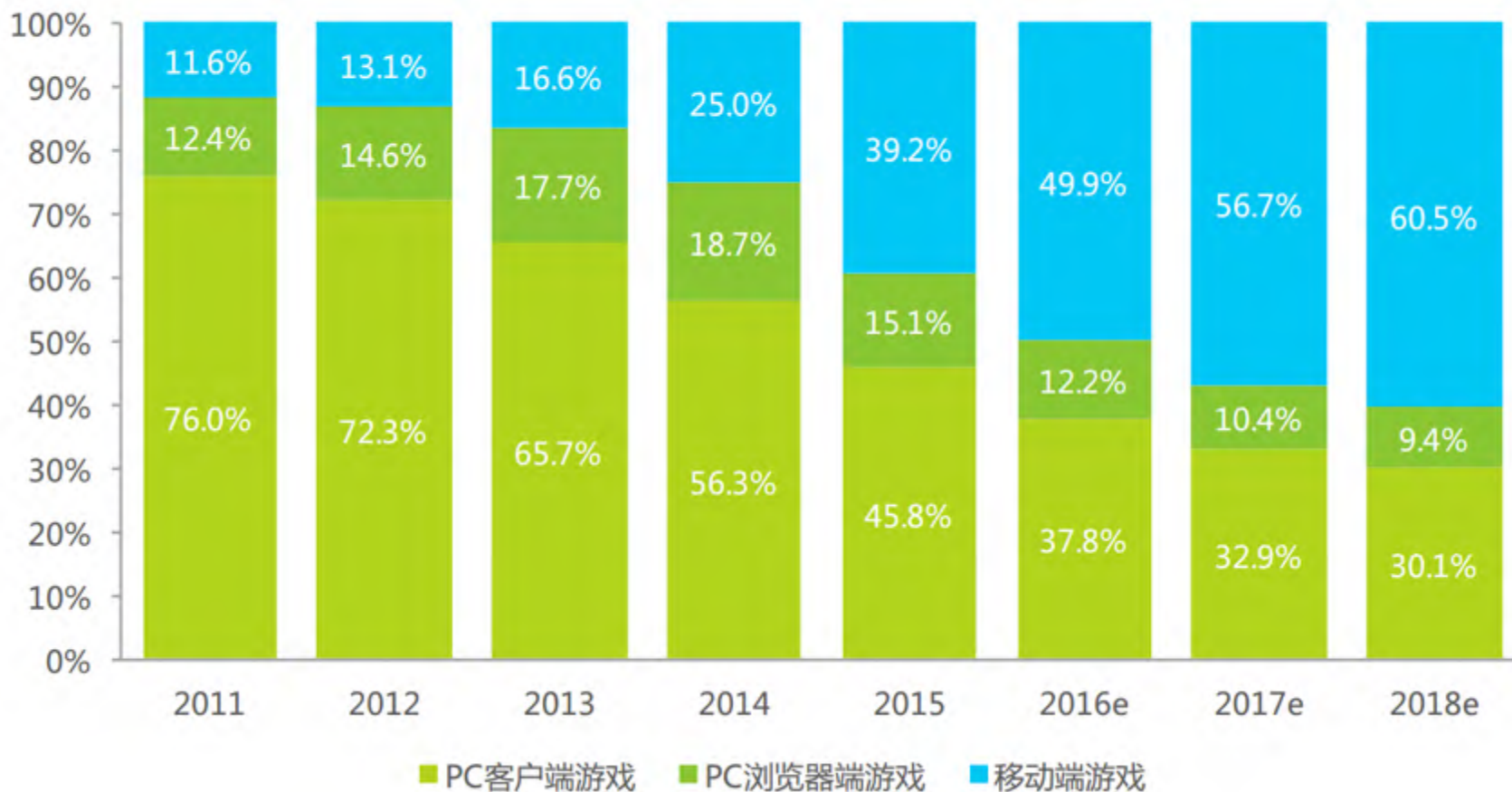
 +  +  +  = ∞

### 2011-2018年中国网络游戏市场规模



数据来源：艾瑞咨询

2011-2018年中国网络游戏产业细分



数据来源：艾瑞咨询

# 各种安全问题随之而来

A word cloud containing the following terms: 加速器 (Accelerator), HTTP劫持 (HTTP Hijacking), 钓鱼 (Phishing), 支付漏洞 (Payment Vulnerability), 外挂 (External Add-on), 羊毛党 (羊毛党 -羊毛党), DNS劫持 (DNS Hijacking), 私服 (Private Server), 打金工作 (Gold Farming Work), 漏洞 (Vulnerability), 黑 (Black), 羊 (Sheep), 金 (Gold), 工 (Work), 作 (Job).

# 那些年我们一起玩过的私服

www.188ty.com  
刀塔传奇 少年三国志

BT手游公益服  
BT手游公益服 安卓版+IOS下载  
注册福利, 进群有礼, 充值高返

不良人公益服

魅影传说 真实广告绝不坑爹  
公益服

全民挂机 128手游  
立即下载

狂人墨 八年老服 | 各種遊戲  
開服一條龍

梦幻西游

烈火战神 多款页游 完美仿官  
高比例 | 长久稳定

浴汗·得百兩

N多独家绝版的游戏, 赶紧来试玩

大话西游 真正的私服  
上线就送花式坐骑

手向华 一同加入我们 找回曾经的快乐回忆吧  
现在注册就送1000点

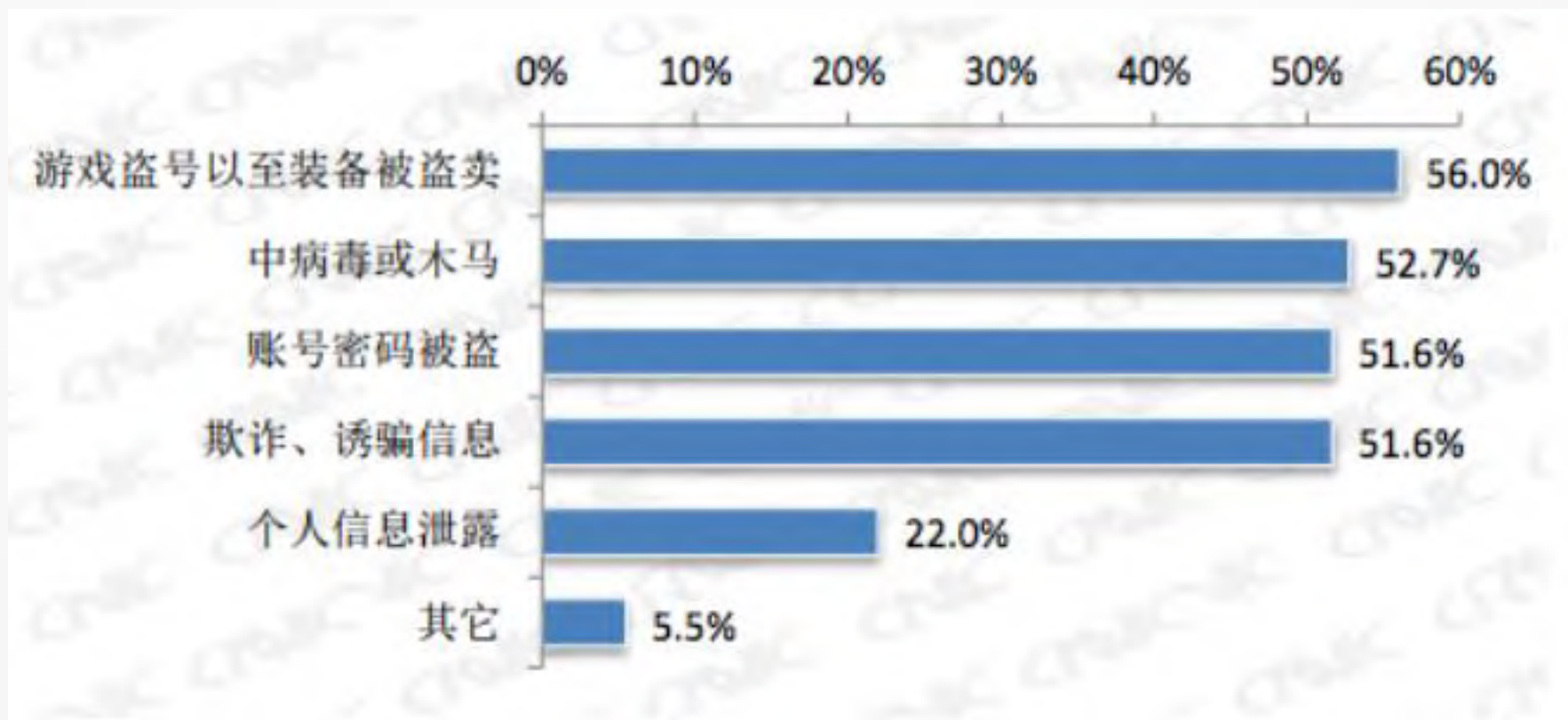
西西谷 懷舊楓之谷  
西西是你最佳好選擇~快加入!

少年三国志 更新同步官方 最新版本 家园天下 金将 金宠

亞曼尼天堂 6/29日 晚上八點 最新伺服器 寒霜冰界 正式開啟

无限元宝 + 顶级VIP = 免费领取

## 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  毫秒后结束QQ (1000毫秒为1秒)

木马模式:

点击  次登录按钮后自动关闭木马

### 4399生死狙击小号盗号器

对方账户

目标正在准备! 稍等

软件正在破译密码

破译80%

776	853	weng6	en855	222.217.117.20	广东省广州市 电信ADSL	2009-7-26	12:28:13
162	872	80863	366486238	61.54.75.2	河南省洛阳市 网通ADSL	2009-7-26	12:29:15
861	538	11111	1haoren	119.118.163.28	江苏省常州市 网通ADSL	2009-7-26	12:29:17
531	851	huang	1528528	222.288.62.83	四川省资阳市 电信	2009-7-26	12:29:42
354	915	an112	5	222.38.164.91	河北省沧州市 铁通	2009-7-26	12:30:04
148	398	15931	5888	121.19.124.24	河北省保定市 网通	2009-7-26	12:30:04
226	826	13846	1111	68.23.196.92	辽宁省营口市 网通	2009-7-26	12:30:05
775	191	aixiu	28	218.28.16.211	河南省郑州市 网通	2009-7-26	12:30:54
361	458	xiaox	394888	228.182.36.42	西藏 电信	2009-7-26	12:30:56
384	736	aifu	21.com	222.168.226.74	吉林省白城市 网通	2009-7-26	12:31:07
561	458	woa11	g2618886	115.49.217.135	河南省南阳市 网通	2009-7-26	12:31:07
514	157	13984	87790k	113.9.118.105	黑龙江省 联通	2009-7-26	12:31:21
344	527	myuu	ni1985228	117.48.252.5	江西省萍乡市 电信	2009-7-26	12:31:31
524	364	52131	78	125.211.114.172	黑龙江省哈尔滨市 网通	2009-7-26	12:31:48
893	847	zhang	i_love19	228.176.78.262	江西省萍乡市 城北网吧	2009-7-26	12:32:06
585	454	81652	827f	124.165.223.226	山西省吕梁市 网通	2009-7-26	12:32:12
785	153	980PT	7/+	116.116.137.139	内蒙古 网通	2009-7-26	12:32:16
267	399	88262	7aa	221.234.18.194	湖北省恩施州 电信	2009-7-26	12:32:16
365	277	13945	8688a	221.289.48.166	黑龙江省哈尔滨市 网通	2009-7-26	12:32:27
574	781	13512	9696	125.37.251.184	天津市 网通	2009-7-26	12:32:37
354	486	zhang	8711	221.232.22.11	湖北省武汉市 (汉口) 电信ADSL	2009-7-26	12:32:53
412	258	28816	08	228.164.193.243	四川省宜宾市 电信ADSL	2009-7-26	12:33:04
785	834	chen1	72881343	219.139.73.233	湖北省孝感市 电信	2009-7-26	12:33:09
735	974	12345	89	222.83.169.189	广西壮族自治区 电信	2009-7-26	12:33:19
784	122	wang7	86wux	123.191.187.251	辽宁省沈阳市 网通ADSL	2009-7-26	12:33:29
248	257	83188	ICEGE123	211.138.243.98	广西南宁市 移动	2009-7-26	12:33:38
593	946	cj666	1	123.139.239.94	陕西省西安市 网通	2009-7-26	12:34:03
833	578	uuv15	1821	124.225.158.148	海南省海口市 电信	2009-7-26	12:34:47
231	373	aaa22	3373	122.141.161.32	吉林省 网通	2009-7-26	12:34:48
281	563	suort	58	118.73.67.93	山西省临汾市 网通	2009-7-26	12:34:58
880	727	11nfa	x1985	125.37.184.174	天津市 网通	2009-7-26	12:35:13
865	841	13246	9798	114.241.159.161	北京市 网通ADSL	2009-7-26	12:35:15
391	841	78891	8	121.25.172.7	河北省张家口市 网通	2009-7-26	12:35:18
582	988	HU82	VCH	61.184.236.214	湖北省武汉市 电信	2009-7-26	12:35:24
515	388	Leag	48614	219.157.127.153	河南省漯河市临颖县 都市村网吧	2009-7-26	12:36:11





发布信息

首页| QQ信封黑信| DNF黑信箱子| DNF黑信信封| 剑灵箱子| 大话信封| 梦幻西游信封| 传奇江湖| 武林问道| 征途屠城| 流量交易| 其它类别| QQ华夏QQ三国| 天龙八部2| QQ三

国| 龙之谷| 大唐无双| 神魔大陆| 倩女幽魂| 梦幻西游| 伊莎在天| 所有箱子| 剑灵信封| 剑灵箱子| 剑灵| 剑灵信封| 剑灵| 发布信 | 举报 | 广告价格表



小心骗子! 直接打款被骗别怪我管理, 自己举报!

域名注册

QQ: 5www.xiangzi5.com 私人兼职推广! 有任何

标题	账号QQ	发布时间	地区/卖家数量	类型	交易渠道	等级	介绍
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797棋牌屋	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信箱三十拆	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 皇报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永久进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

红茶工作室  
QQ: 33685214

QQ营销信专用信封 问道梦幻

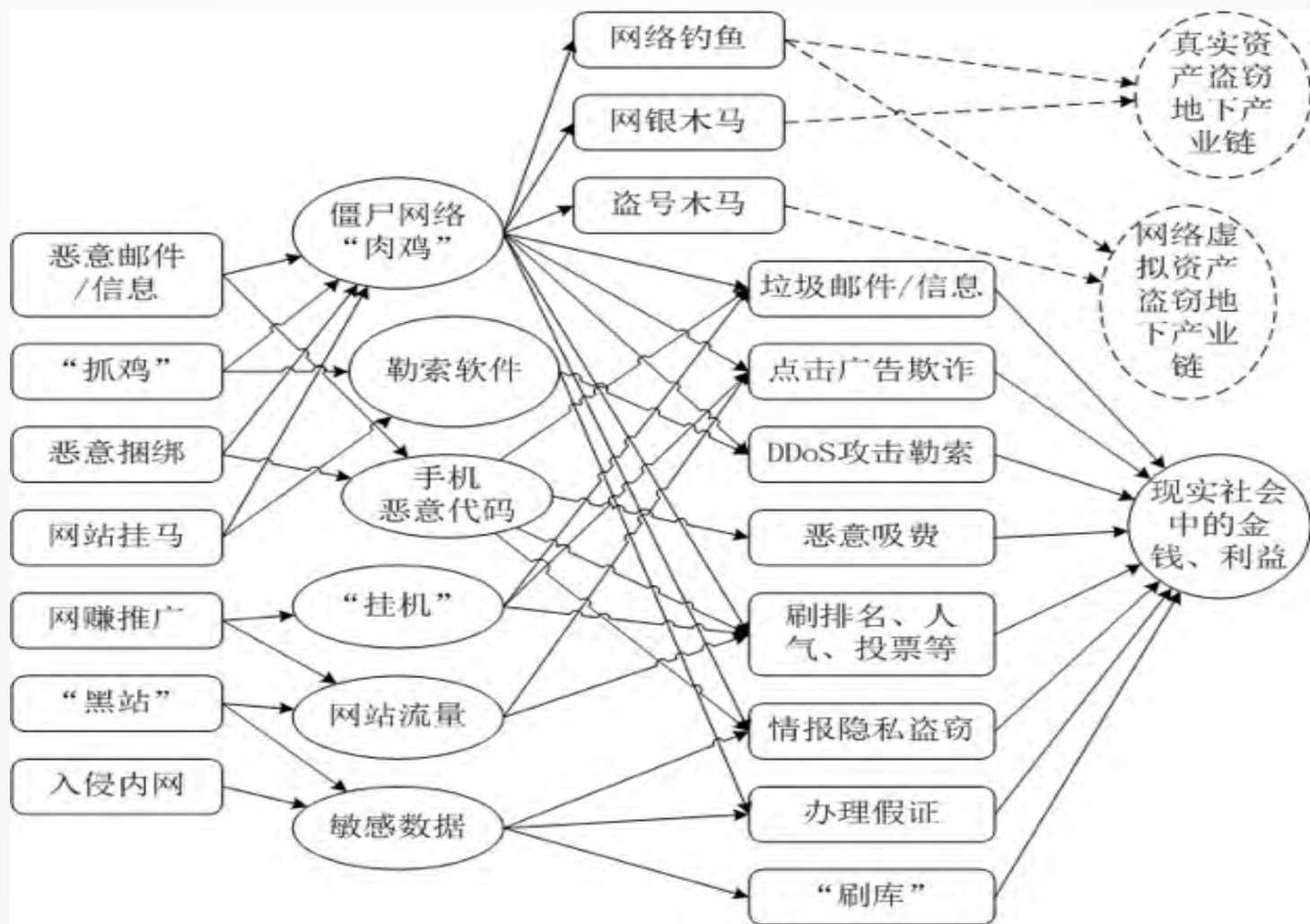
一手货源 上家已跑路

上家抢走 抢回还还还大快的!

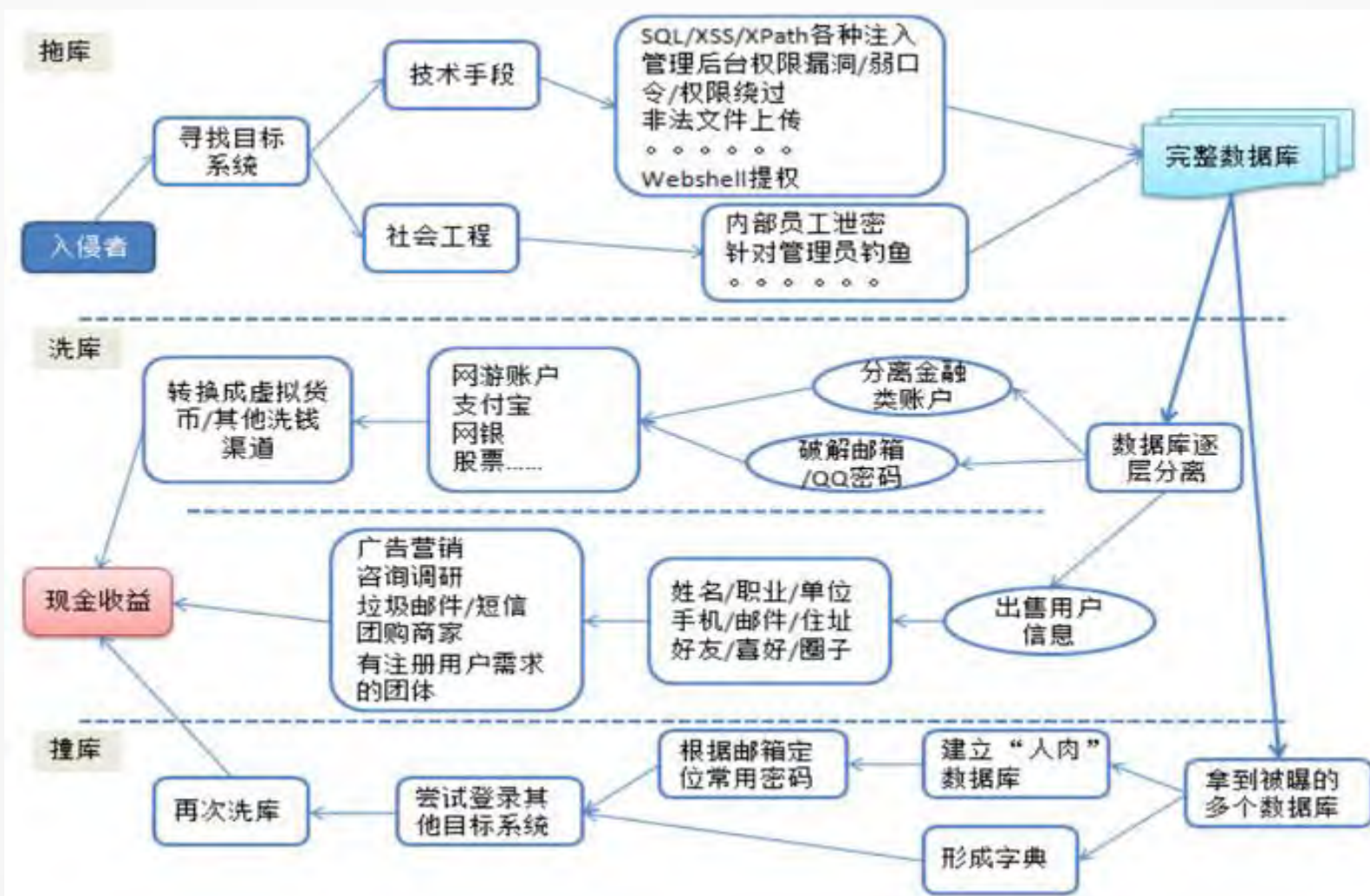
找不到货源别家 别家别家!

这个号容易吗叫我

# 当黑客技术遭遇利益的诱惑



# 大数据时代，黑产可能比你自已还了解你



# 外挂——游戏平衡破坏者

当前正在：

信息 | 背包 | 任务 | 挂机 | 宝石 | 其他 | 巴别塔 | 支线任务 | 聊天 | 帮助 | 设置

**魔族任务**

自动吃旗   开始任务   结束任务

**寻宝任务**

开始任务   结束任务

**自动跑商**

品名	买入价	卖出价	品名	买入价	卖出价	信息
玉米	10	10	象牙	500	500	现有金额
番茄	10					
葡萄酒	110					
朗姆酒	110					

**辅助区域**

刷枪声明

反馈BUG

官方直达

安全退出

经验加成 (共130%加成)

金牌代理加成35%

断开VPN代理

解除网吧VPN限制

卡空功能 (测试)

开启卡空功能

用前必看使用教程

下载搜狗输入法

基本 | **攻击辅助** | 保护 | 扩展功能 | 挂机 | 测试

战士辅助功能 | 法道辅助功能

**基本功能**

近身烈火    隔位刺杀 Alt+D    随机移动    田字移动

智能移动 Alt+S    刀移动一次    顺时针    逆时针

**高级功能**

攻击暗杀    锁定目标 Ctr+Tab    开启攻击变色

过攻击超速    幻影攻击    幻影移动

多倍攻击  

过篮模式  

开启 ^键无限刀   间隔:  MS  

**卡框功能**

野蛮弹交易    去除交易框    超级野蛮

野蛮弹挑战    去除挑战框    开启无限交易

智能野蛮 ALT+G    刀野蛮一次

[19:11:15] 登陆

[19:11:12] 正在

[19:11:12] 您的

请输入搜索内容

帖子 -

搜索: 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 ◆

今日: 1 | 昨日: 6 | 帖子: 69984 | 会员: 20807 | 收藏夹

最新主题

鑫郁飞外挂科技公司

- 64位程序 输入16进制 printf f ...
- 游戏安全技术终极解密教程-这个 ...
- 高稳定性高并发安全平台社交聊天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 ...
- 高稳定性高并发安全平台社交聊天IM ...

外挂视频教程相关(学员区)

**视频** 001-C/C++语言教程  
主题: 168, 帖数: 762  
最后发表: 昨天 01:05

**视频** 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

玩游戏这件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

<p><b>游戏蜂窝</b> 2017-02-23 / 22.5M ★★★★★ 下载</p> <p><b>推荐理由:</b> 游戏蜂窝可以说是最全的手机游戏辅助脚本分享平台, 游戏蜂窝辅助器里面的大神也会在第一时间来给你提供帮助</p> <p>版本: PC版   安卓版   苹果版</p>	<p><b>掌上英雄联盟app</b> 2017-03-01 / 24.3M ★★★★★ 下载</p> <p><b>推荐理由:</b> 掌上英雄联盟app提供游戏资讯和战绩数据更新为LOL官方助手功能, 更加准确和及时, 掌上英雄联盟app是腾讯</p> <p>版本: PC版   安卓版   苹果版</p>	<p><b>多玩我的世界盒子</b> 2017-03-10 / 21.8M ★★★★★ 下载</p> <p><b>推荐理由:</b> 多玩我的世界盒子是对我的世界手机版的一个非常扩展的辅助应用, 制造大家最关注的我的世界皮肤, 我的世界</p> <p>版本: PC版   安卓版   苹果版</p>
<p><b>多玩饭盒(原多玩盒子)</b> 2017-02-23 / 35.5M ★★★★★ 下载</p> <p><b>推荐理由:</b> 多玩饭盒是多玩盒子手机版改名而来, 多玩饭盒主要是专注高德地图这个游戏, 需要帮助的玩家应该还是很多</p> <p>版本: PC版   安卓版   苹果版</p>	<p><b>叉叉助手</b> 2017-03-11 / 20.0M ★★★★★ 下载</p> <p><b>推荐理由:</b> 叉叉助手是一款安卓游戏辅助系统软件, 可以帮助玩家在玩游戏迅速取得想要的东西和目的, 让你不在为神</p> <p>版本: PC版   安卓版   苹果版</p>	<p><b>葫芦侠</b> 2016-12-16 / 13.1M ★★★★★ 下载</p> <p><b>推荐理由:</b> 葫芦侠修改器是一款游戏辅助软件, 无论安卓还是IOS用户, 玩游戏的朋友和比想和葫芦侠修改器, 和葫芦</p> <p>版本: 安卓版   苹果版</p>

# 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



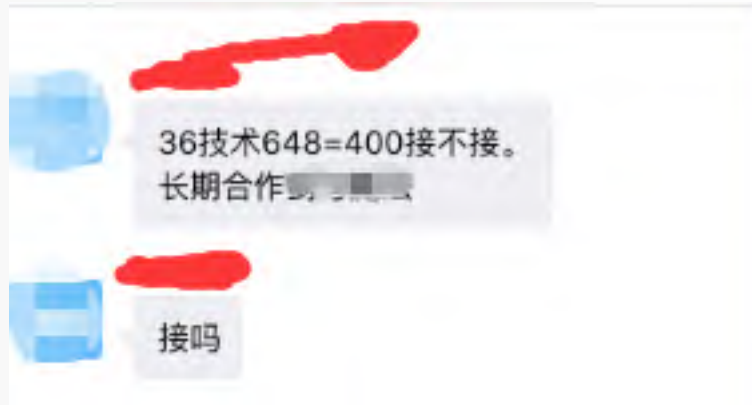
4月2日下午，网安支队在市公安局及铁人公安分局、让胡路公安分局、高新公安分局、龙凤公安分局的配合下，在萨尔图的某楼区和龙凤区的某小区，将正在使用外挂程序进行非法活动的辛某、张某等10名涉案成员抓获。当场缴获用于运行外挂程序的客户端简装计算机1.1万台，主控服务器120余台，扣押涉案车辆2台、现金7万余元、手机10余部及账本、银行卡若干，涉案财物总价值300余万元。

# 内容劫持——防不胜防





# 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

正在使用即时到账交易 [?]

金币充值-数量648000 收款方: 成都市梦想兄弟网...

0.01元

打印凭证

支付宝账户付款

新用户注册

账户名:

忘记密码?

手机号码/邮箱

支付密码:

忘记密码?

请输入账户的支付密码, 不是登录密码。

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

找到的 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>

2015年5月17日 - 漏洞标题: 百度网游存在支付漏洞, 相关厂商: 百度, 漏洞作者: darkremor, 提交时间: 2013-06-14 23:25, 公开时间: 2013-06-17 10:06, 漏洞类型: 设计 ...

## 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/tarticle/p/show?id=2309404064926355331803](http://weibo.com/tarticle/p/show?id=2309404064926355331803)

2017年1月17日 - 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 ... 利用网游第三方支付系统漏洞, 明知银行账户余额不足仍恶意充值, 造成支付平台支付 ...

## 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](http://www.chinacourt.org), 审判、刑事案件

2008年7月25日 - 中国法院网讯 (常州) 22岁江苏青年李东生与他人合谋, 利用黑客手段登入网络支付平台, 用先付款购买网游点卡再将已付款项退回的方式窃取各类 ...

## 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/oi/2016-10-31/doc-ifyxuff7263691.shtml](http://news.sina.com.cn/oi/2016-10-31/doc-ifyxuff7263691.shtml)

2016年10月31日 - 尽管漏洞百出, 电脑端网络游戏还好还有一个实名认证防沉迷系统, 而移动 ... 现在一些移动端支付平台已经可以进行面部识别作为支付的辅助密码。

## 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](http://www.hddls.net/case/510093.html)

案情回顾: 22岁江苏青年李某与他人合谋, 利用黑客手段登入网络支付平台, 用先付款购买网游点卡再将已付款项退回的方式窃取各类游戏点卡2073张, 价值 ...

## 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](http://news.pedaily.cn/201304/20130415346605.shtml)

2013年4月16日 - 巨人被指诈骗洗钱安全支付漏洞还是刻意为之? ... 曾供职于盛大网络的网商业内人士黄海明(化名)向《IT时报》记者透露, 事实上大多数网游公司都 ...

## 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](http://it.sohu.com), 互联网, 国内互联网

2010年12月2日 - 两年前, 一次偶然发现让网游迷邓某心跳加速手发抖: 通过第三方支付平台给网络游戏购买点数, 即使输错卡号密码也能充值成功。兴奋之余, 邓某借 ...

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

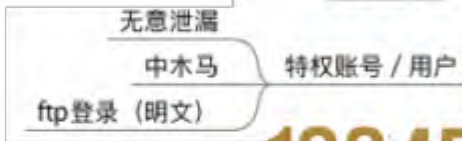
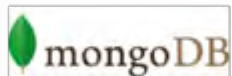


内因：锁被绕过



外因：面临威胁





内因：脆弱性



机房



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。

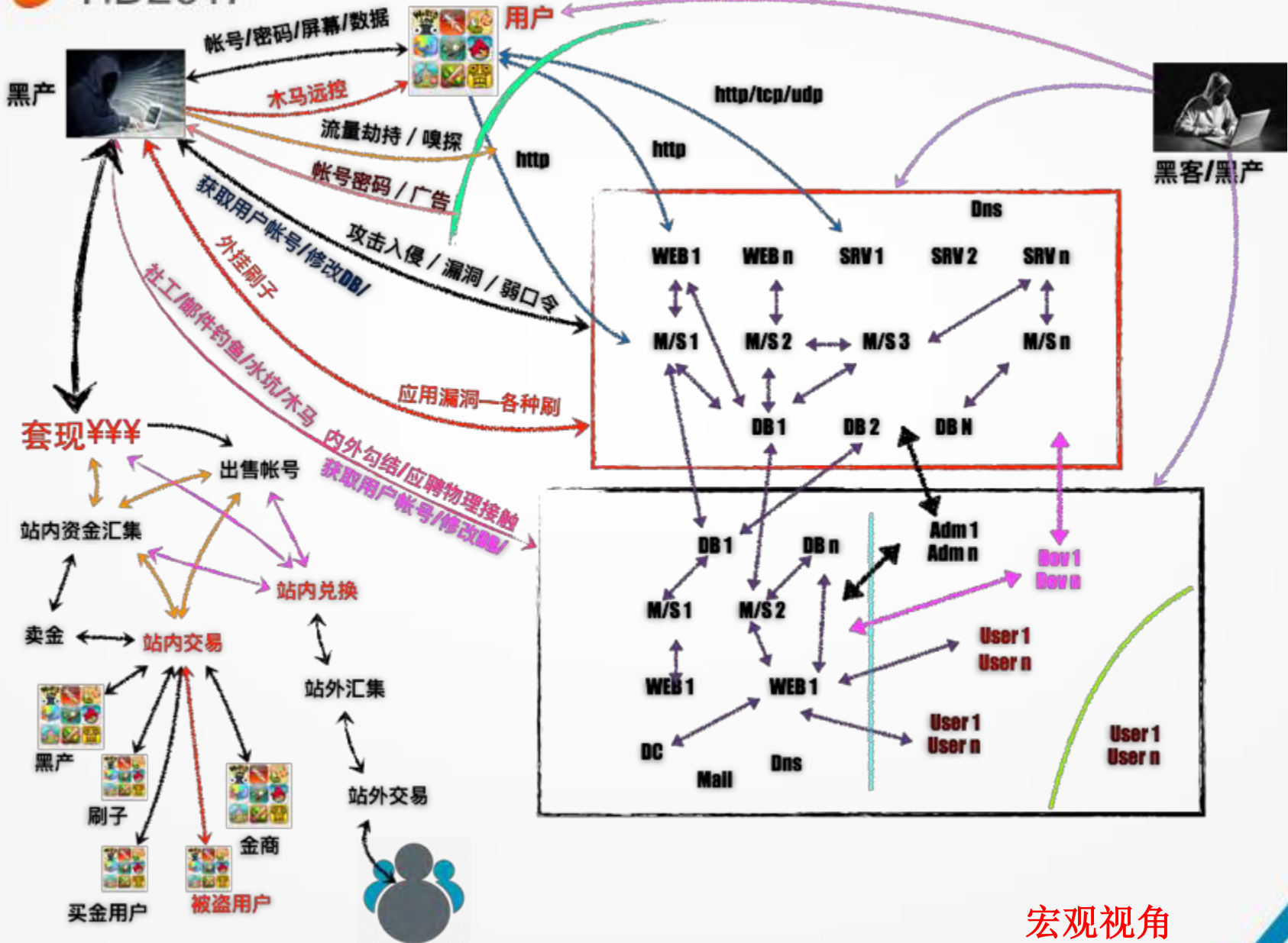
战略

## 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。

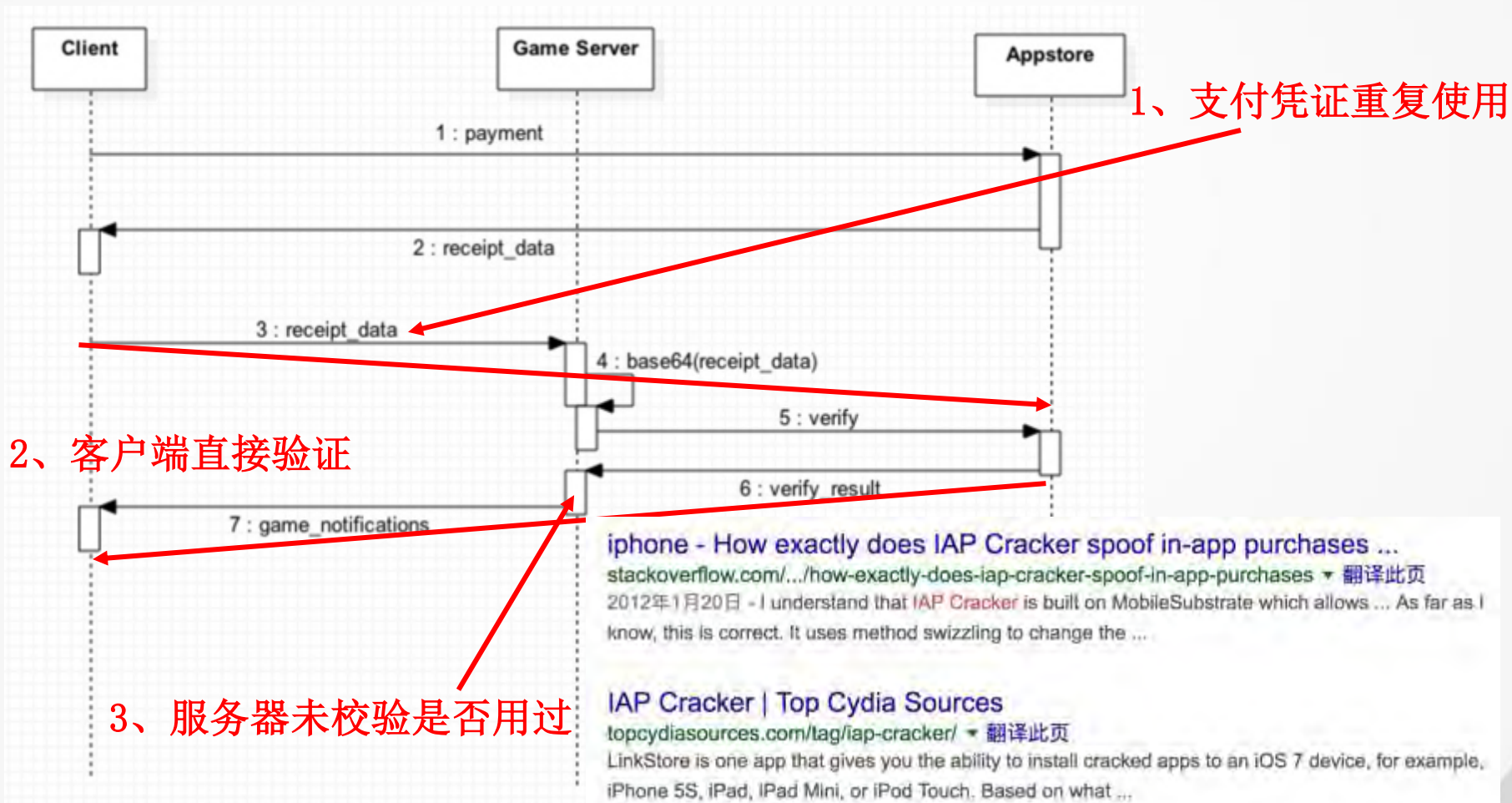
战术





宏观视角

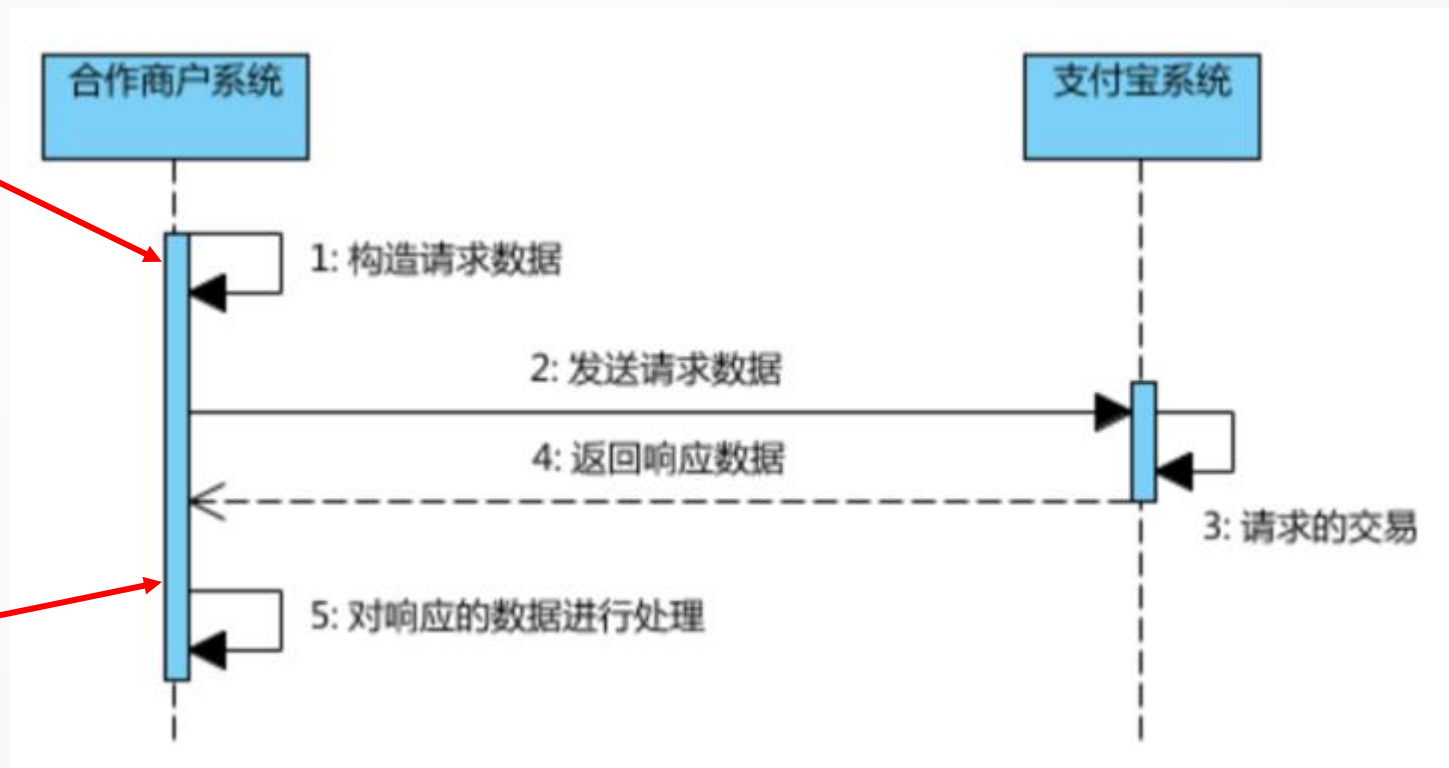
## 支付威胁分析：苹果IAP威胁分析



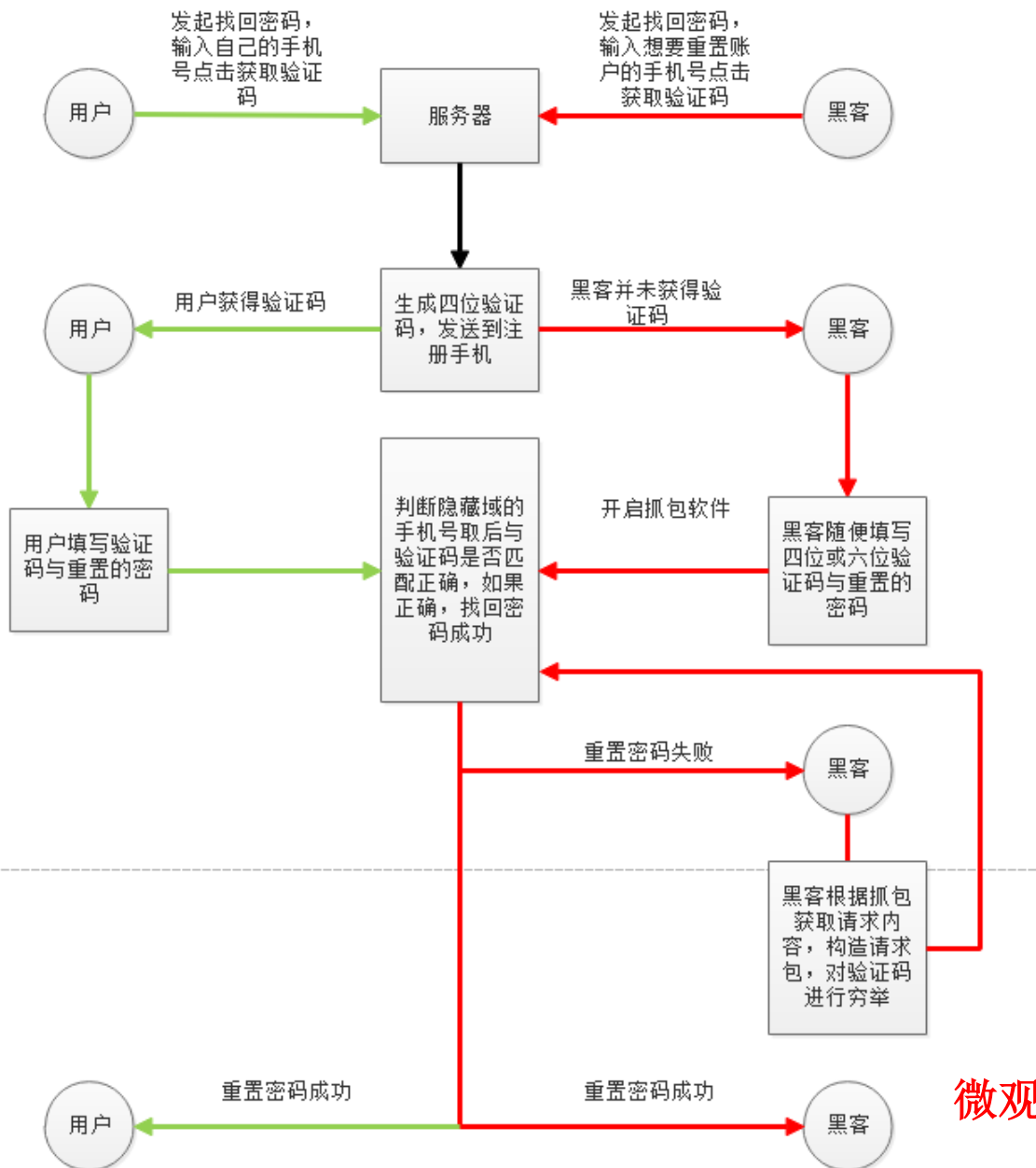
## 支付威胁分析：第三方支付

使用客户端提交数据构造请求数据

未进行有效性校验

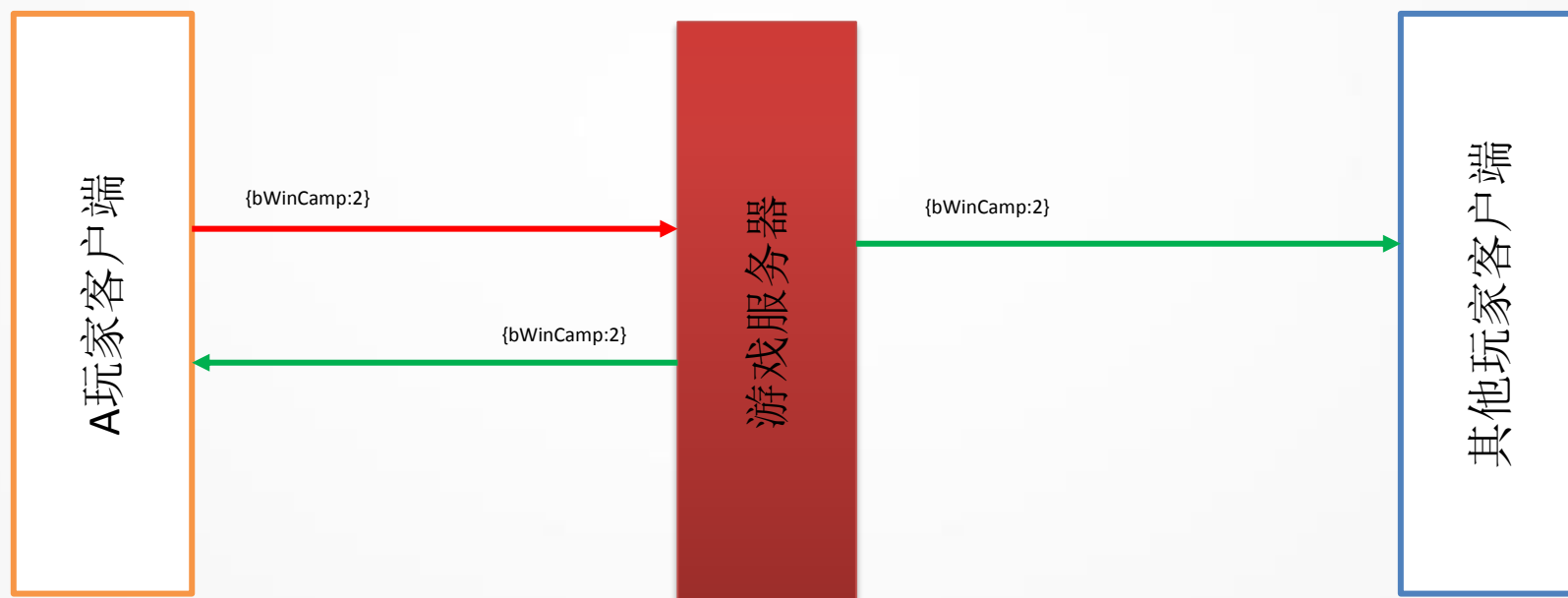


# 密码找回功能 威胁分析



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**



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

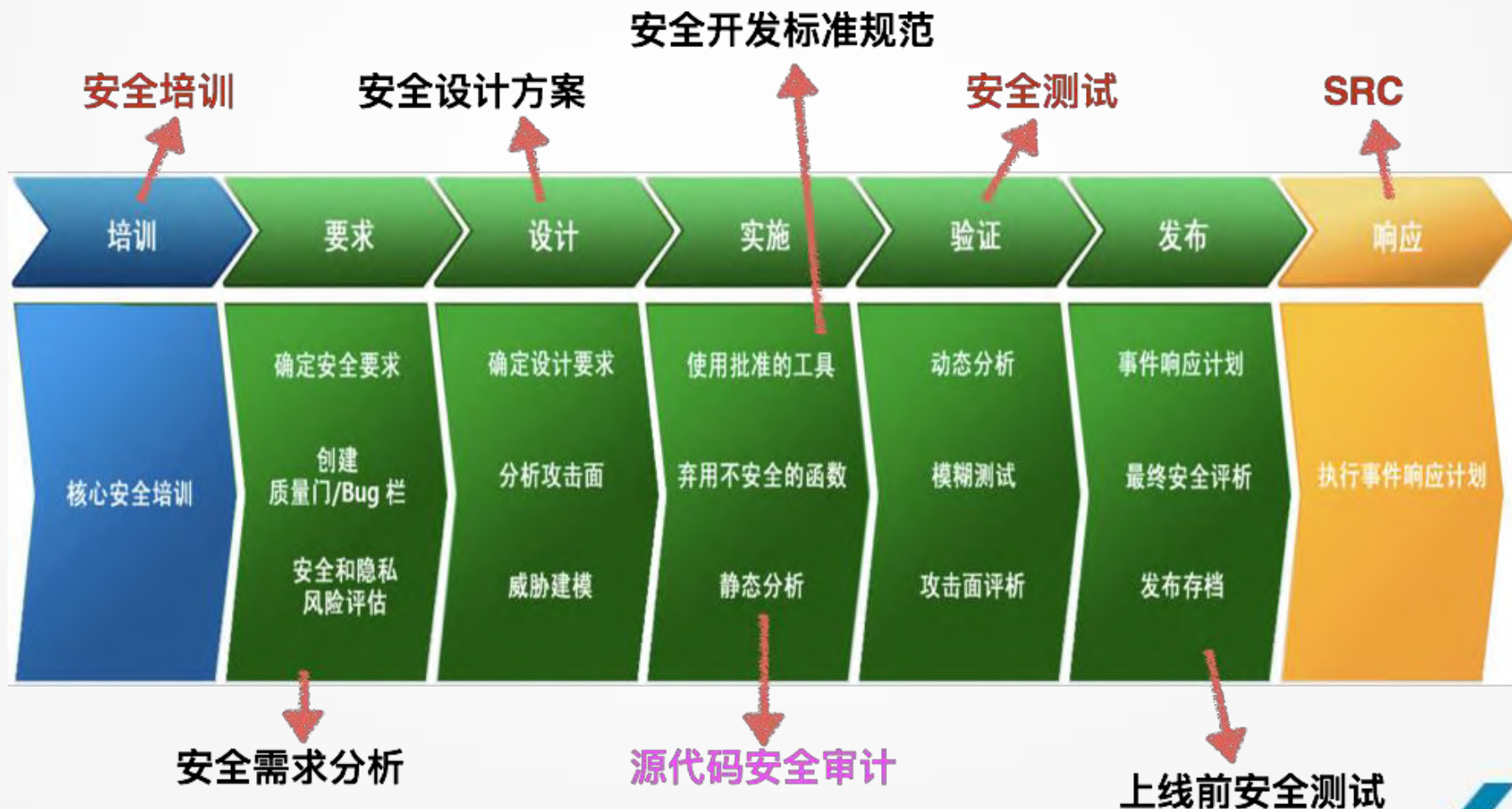
防水  
防潮

硬件生命  
周期管理

机房管  
理规范

大厦管  
理规定

# Security Development Lifecycle

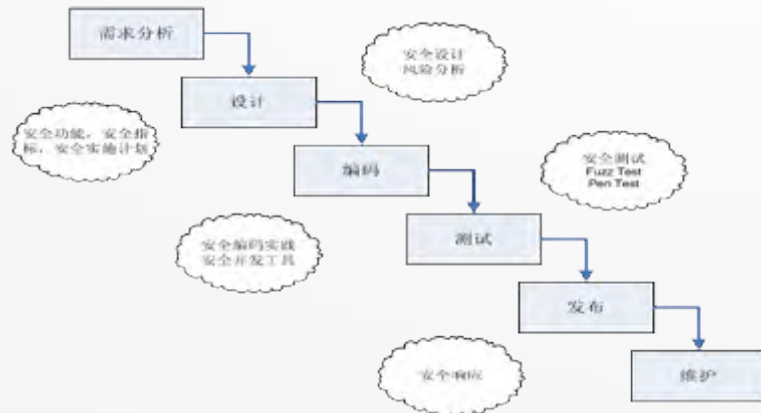


时间紧，任务重，BUG都修不完，还搞这么复杂？！





# 安全 VS 敏捷

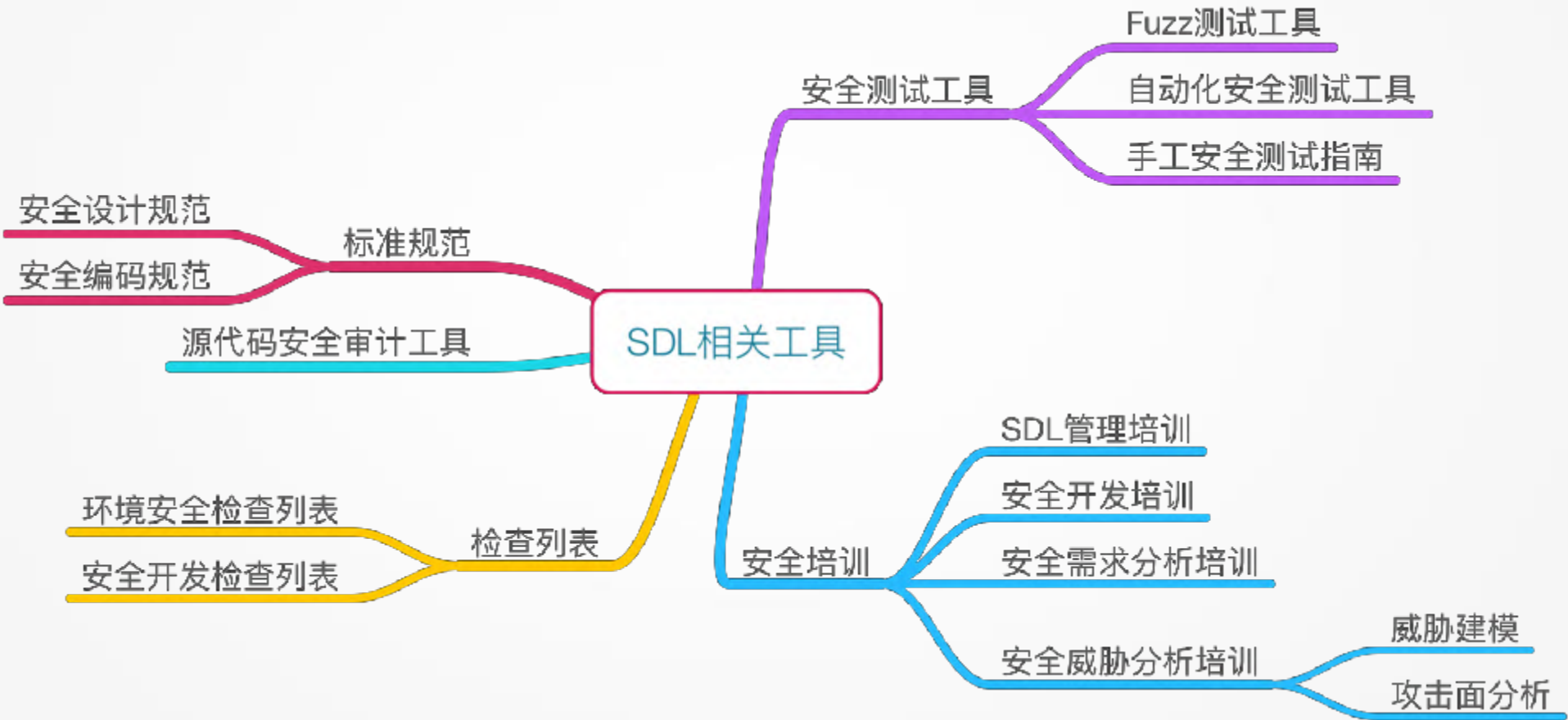


游戏通讯协议被破解？  
刷游戏币漏洞？  
服务器漏洞导致入侵？  
接口泄漏用户隐私？  
越权操作别人账户？

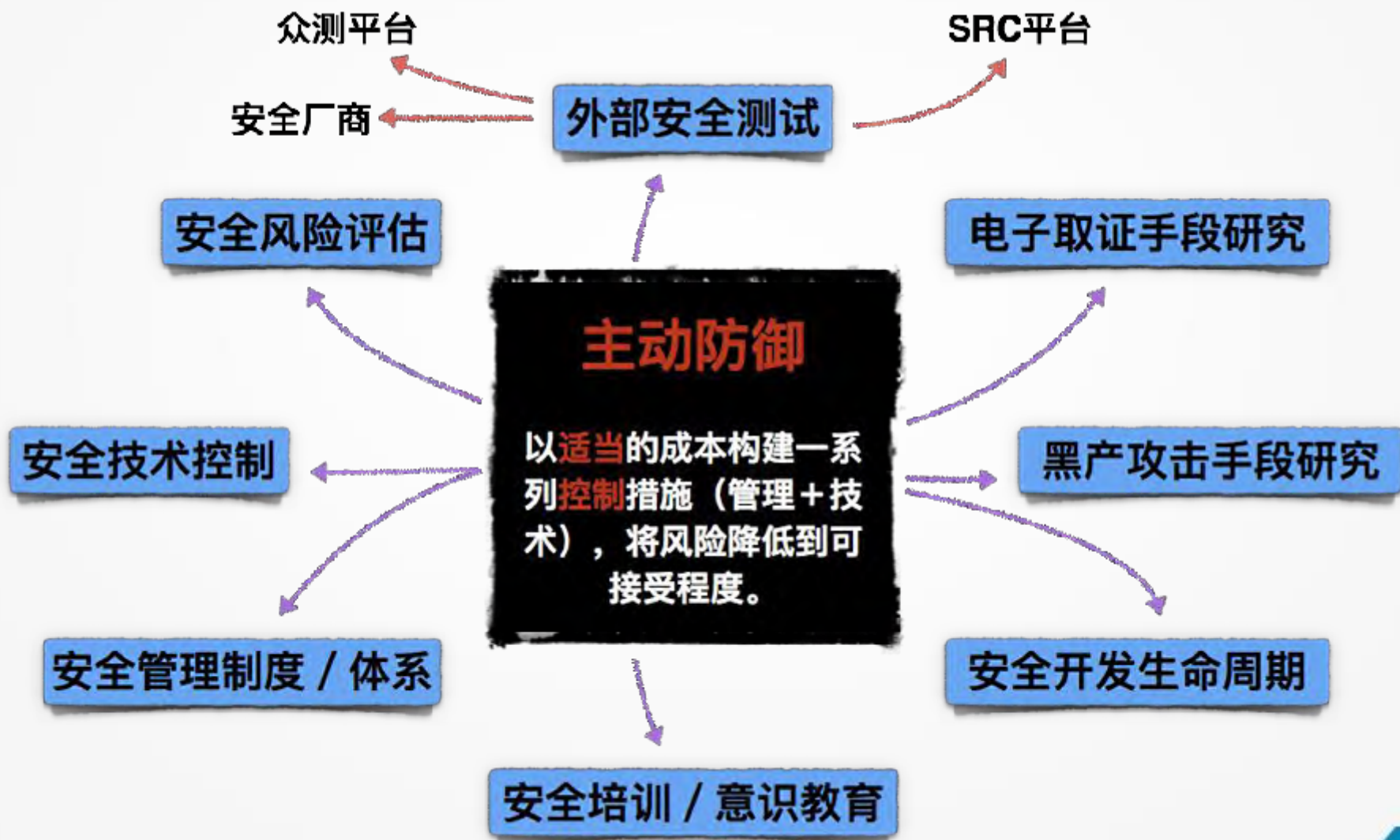


**很多时候损失惨重之后才会吸取教训！**

# Security Development Lifecycle



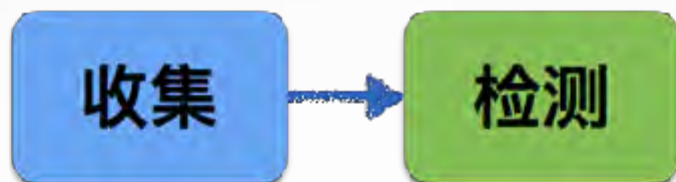




## 检测响应

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**。





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

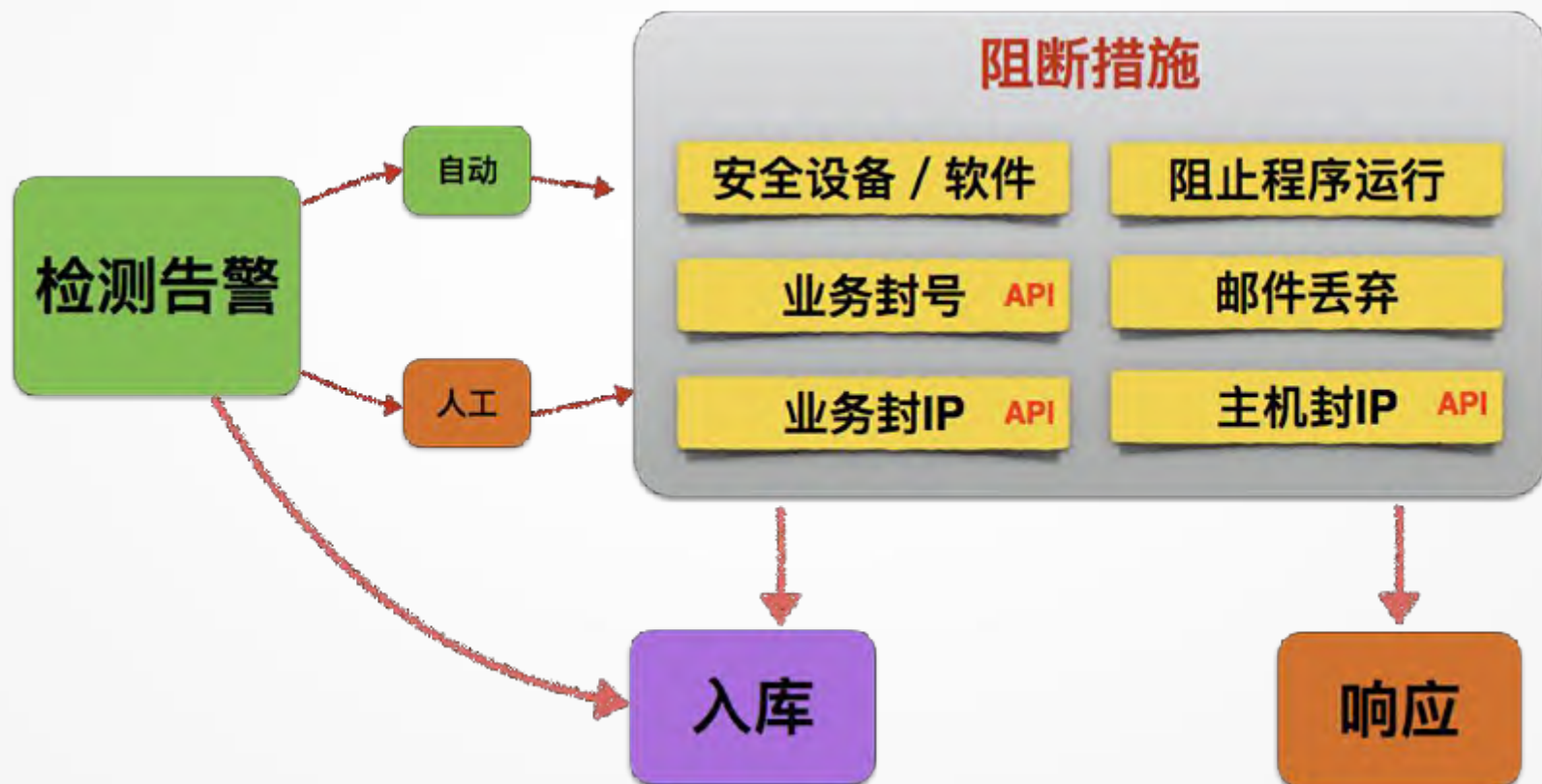
机器学习



特征匹配

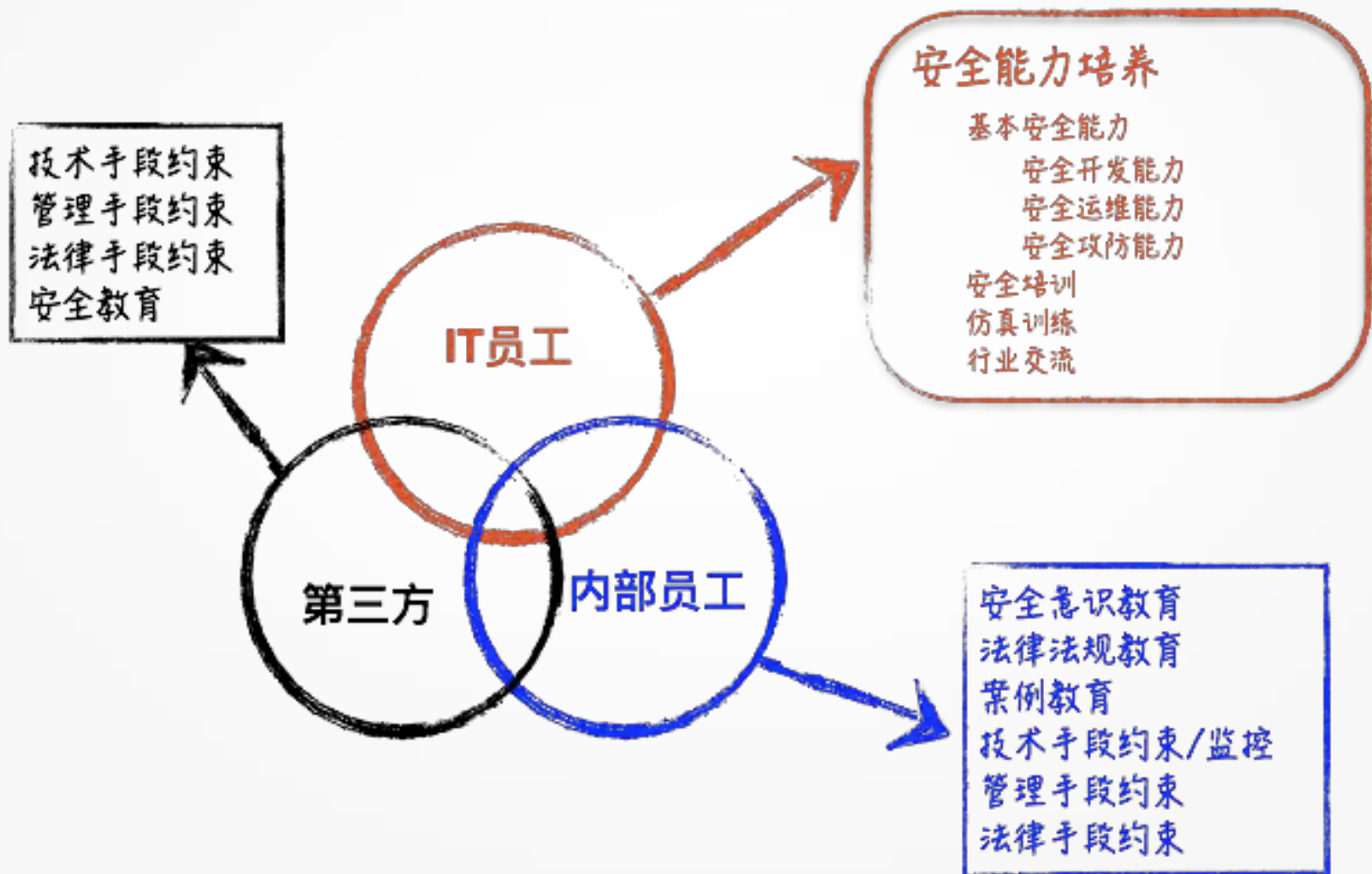
虚拟执行

陷阱——蜜罐





人是“安全”中的关键要素



攻防对抗能力

安全研究能力

业务安全能力

安全应急能力

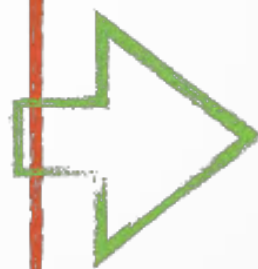
安全开发能力

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





合作



共赢

