FREEBUF | FIT

# 如何做好业务安全红蓝对抗

柳兮 阿里安全 归零实验室

2018.12.13

# 归零实验室

- **归零实验室简介**

- 阿里安全归零实验室成立于2017年11月，实验室致力于对黑灰产技术的研究，愿景通过技术手段解决当前日益严重的网络违规和网络犯罪问题，为阿里新经济体保驾护航。
- 也欢迎各类优秀人才加入我们！

阿里安全

# 主要内容

- 红蓝对抗的简介、价值和意义
- 做好业务红蓝对抗的挑战
- 砺剑蓝军演练平台的建设
- 未来业务红蓝对抗的趋势

# 红蓝对抗的简介



“魔鬼对手”：朱日和蓝军

美国防部邀请黑客攻击五角大楼网站：“黑”我有奖

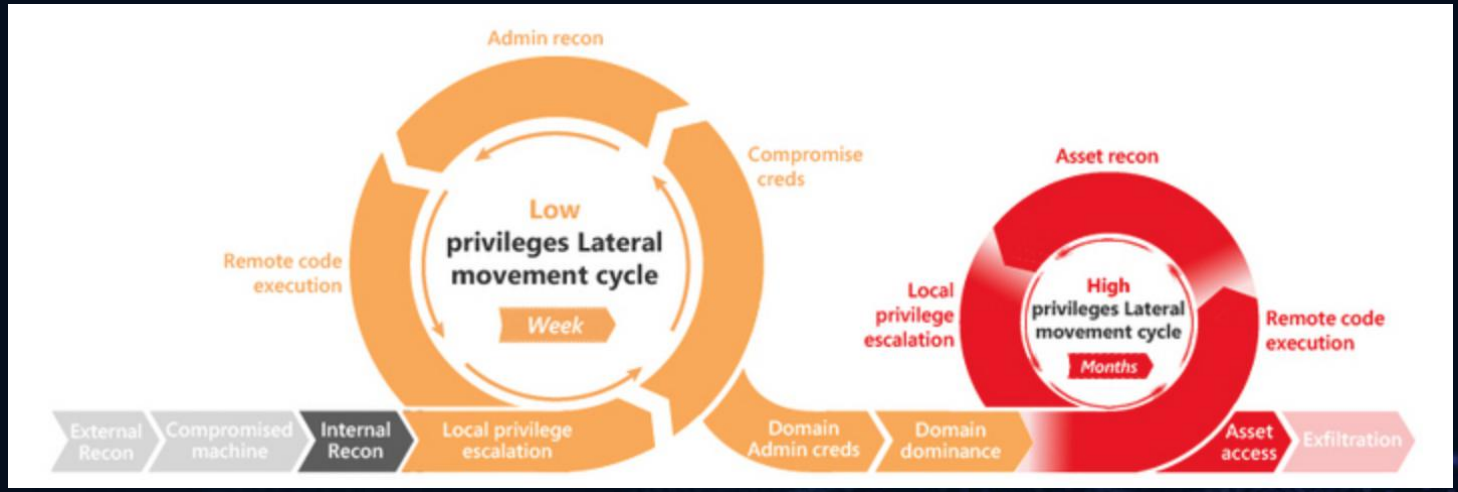
# 红蓝对抗的价值和意义


All Companies Have Been Hacked--Even if They Don't Know It

There are only two types of organizations: those that know that they've been hacked and those that don't yet know,' Crowdstrike's Dmitri Alperovitch says.

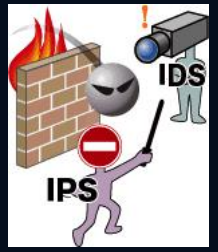
# 红蓝对抗的价值和意义

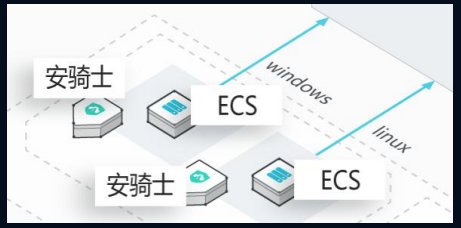
APT攻击越早发现风险越低，业务风险更是如此。



# 常见的规模化业务风险图

# 常见的安全防护体系




防护体系的效果：1+1+1+1+1>5

# 常见安全防护体系-防御业务风险的不足点

**业务安全风险防护体系建设不足**

- 端防护
- 链路
- 数据算法

**业务风险最新攻击手法不清晰**

- 业务情报匮乏
- 不能知己知彼、看清风险

**业务风险防护手法单一**

- 不同业务场景同一套规则、算法模型
- 黑样本匮乏

# 来自另一个视角的解法-业务蓝军

业务情报 + 蓝军演练 =

# 怎么做红蓝对抗演练

通过模拟真实的外部攻击来评估当前的业务安全水位【真枪实弹】

通过线上真实环境的攻防演练来促进防御体系的提升与完善【以攻促防】

结合情报覆盖更多更全的业务攻击路径、手法，进行周期性演练【动态水位评估】

# 做好业务红蓝对抗的挑战

- 如何做好知己知彼，看清“敌人”和风险？
- 如何保证攻击手法、攻击路径的覆盖率足够高？
- 如何自动化的发起大规模、海量节点的实战攻击？
- 如何快速支持多个业务场景，建设通用的风控对抗攻击能力？
- 如何保证演练后红军防御水位提升后的稳定性？

- 需要完成全链路的实战攻击，而不是单点攻击
- 需要从外部，以黑盒视角发起攻击
- 需要真正的帮业务方解决问题，而不是自嗨
- 不能即当裁判，又当运动员

# 如何知己知彼、看清敌人和风险

- 站在黑灰产的视角思考攻击，结合情报看清风险

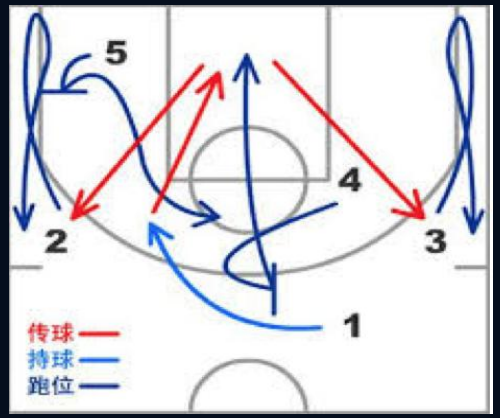

外部黑灰产

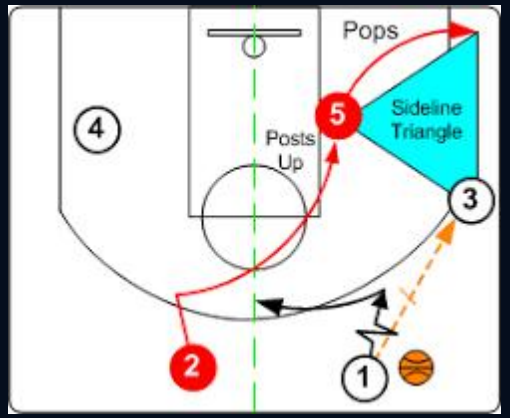
商业间谍


羊毛党


外部黑客

# 如何覆盖更多的攻击手法&路径





- 结合业务反馈、情报等多方信息，列出所有可能的攻击路径
- 梳理每条攻击路径，列出所有可能的攻击手法
- 依照优先级进行攻防演练

# 如何建设通用的风控/业务攻防对抗能力

# 大规模、多场景、海量节点的挑战

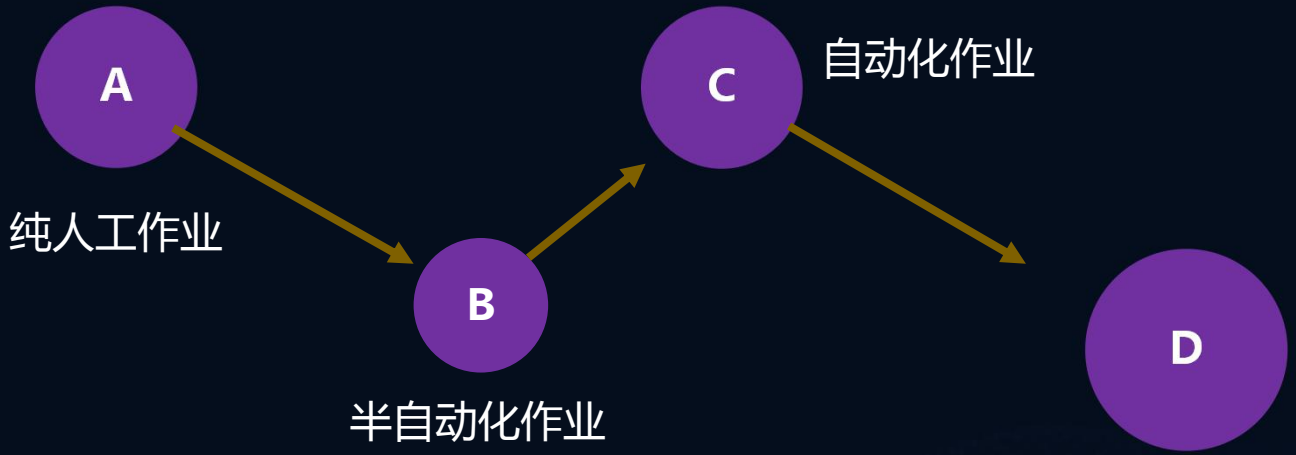
- 业务场景太多支持不过来
- 攻击规模上不去
- 攻击规模上去了调度能力能力跟不上

# 演练后红军防御水位的稳定性保障的挑战

- 传统的0day漏洞（升级漏洞组件、加waf规则等）

- 业务场景是动态变化的，更需要保证防御水位的稳定
- 1）代码、框架层的业务漏洞（修复漏洞代码即可）
- 2）宝贝流量、广告攻击、秒杀等业务场景，则需要持续、动态、周期的进行演练

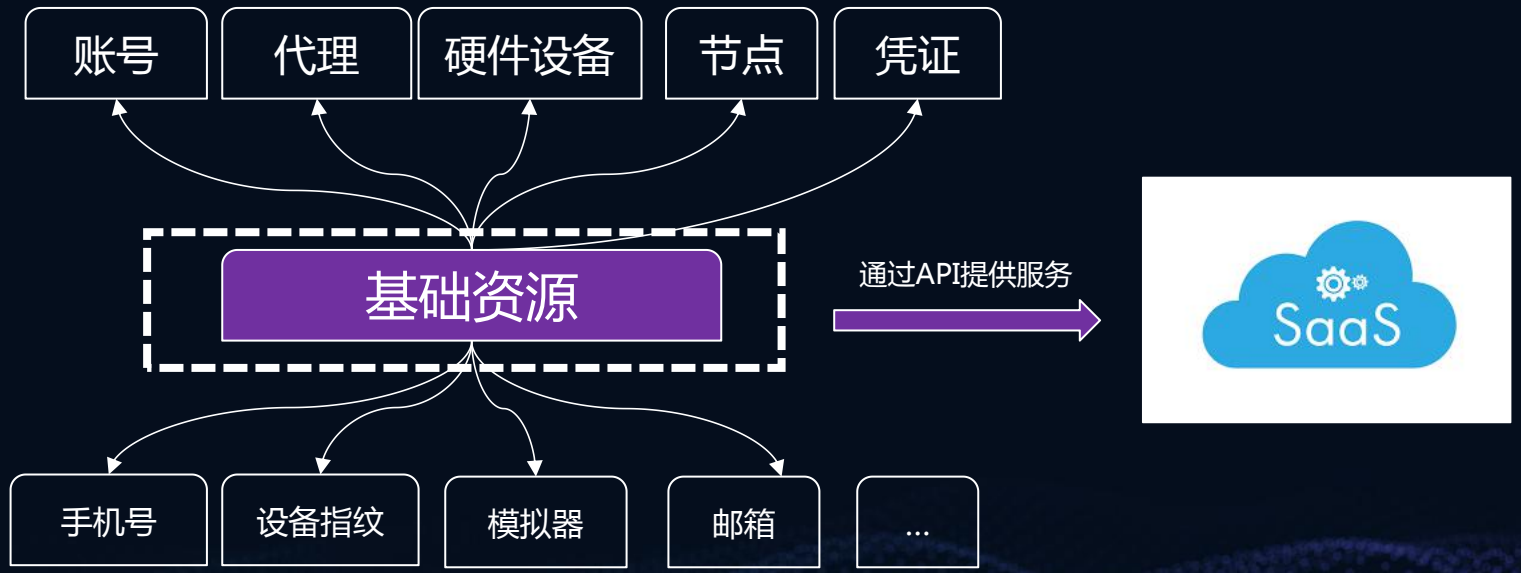
# 大规模、海量节点、多场景持续演练挑战的解法




**平台化作业**

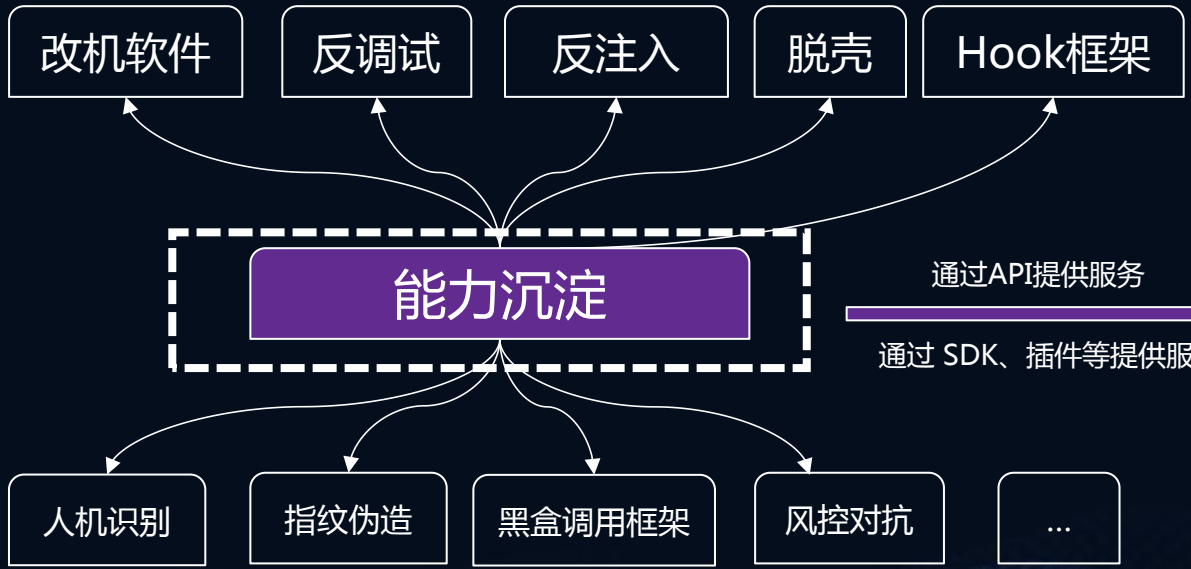
将整个流程平台化，沉淀专家经验到平台

# 业务红蓝对抗的实践-资源管理



# 业务红蓝对抗的实践-能力沉淀






最终形成多个组件

# 砺剑蓝军演练平台大图

# 业务红蓝对抗的典型例子-拉新活动薅羊毛

完成获利

整合一串N二维码，快速完成薅羊毛全链路

重复操作

使用注册好的账号，结合模拟器、改机软件开始薅羊毛

环境策略

IP策略

设备策略

...

调研目标站点防御策略，准备实名黑卡等资源

滑动验证码

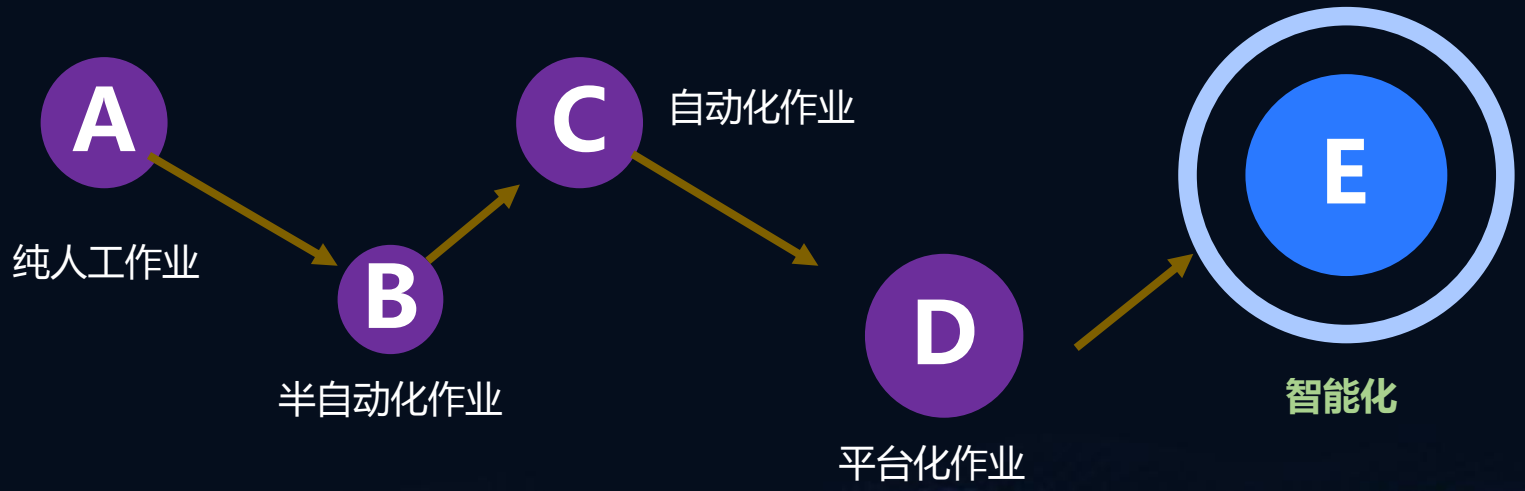
UA

破解安全防护产品，批量注册目标站点的新账号

模拟器

一键新机软件

# 未来业务红蓝对抗的趋势

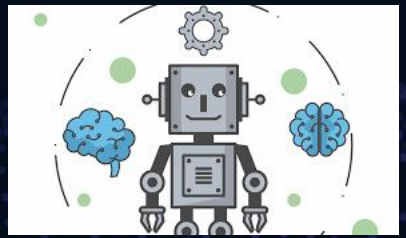


# 未来业务红蓝对抗的趋势-智能化

- **业务风险攻击雏形**
- 通过深度学习识别字母、数字、汉字验证码，绕过滑块验证码，对抗人机识别系统模型

- **攻击趋势**
- 数据投毒
- 对抗样本
- 模型窃取

- **智能化攻防**
- 平台打通攻击全链路，完成智能化攻防



# Q&A

柳兮

中国

扫一扫上面的二维码图案，加我微信

FREEBUF | FIT

# THANKS