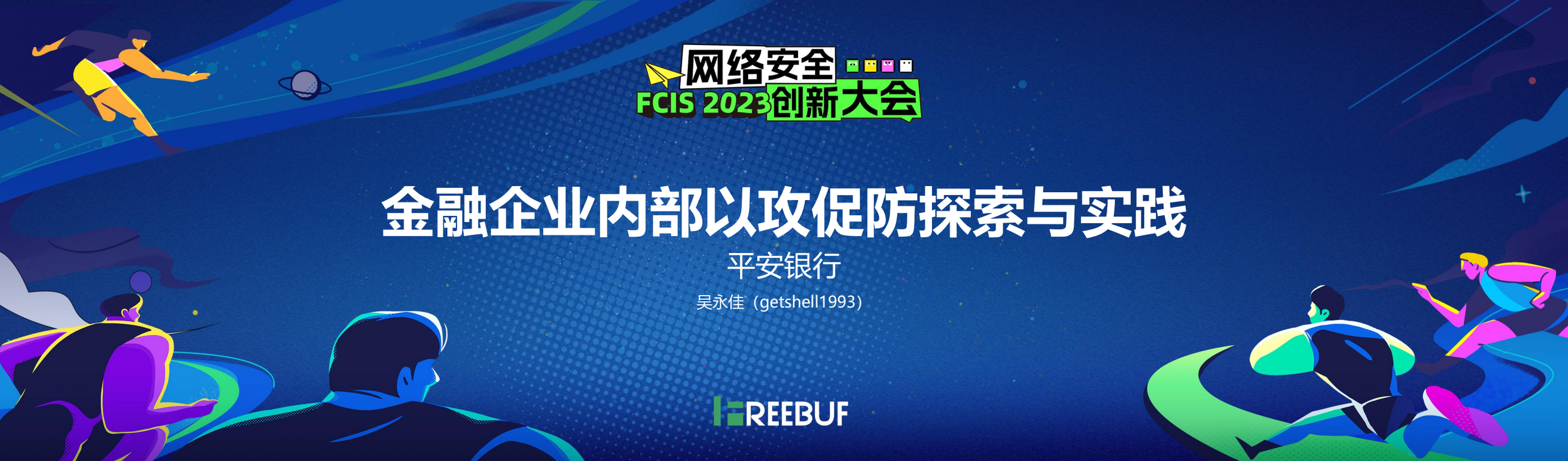


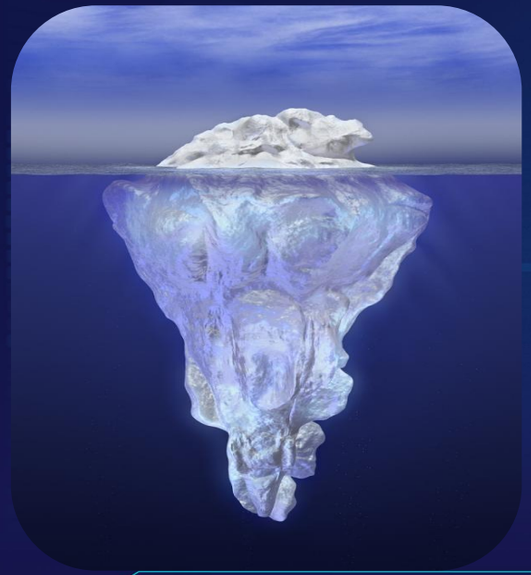
金融企业内部以攻促防探索与实践

平安银行

吴永佳（getshell1993）

FREEBUF

网络安全态势



- **境外国家级网络部队**
  长期对我国重要敏感单位实施网络攻击、企图窃取敏感数据

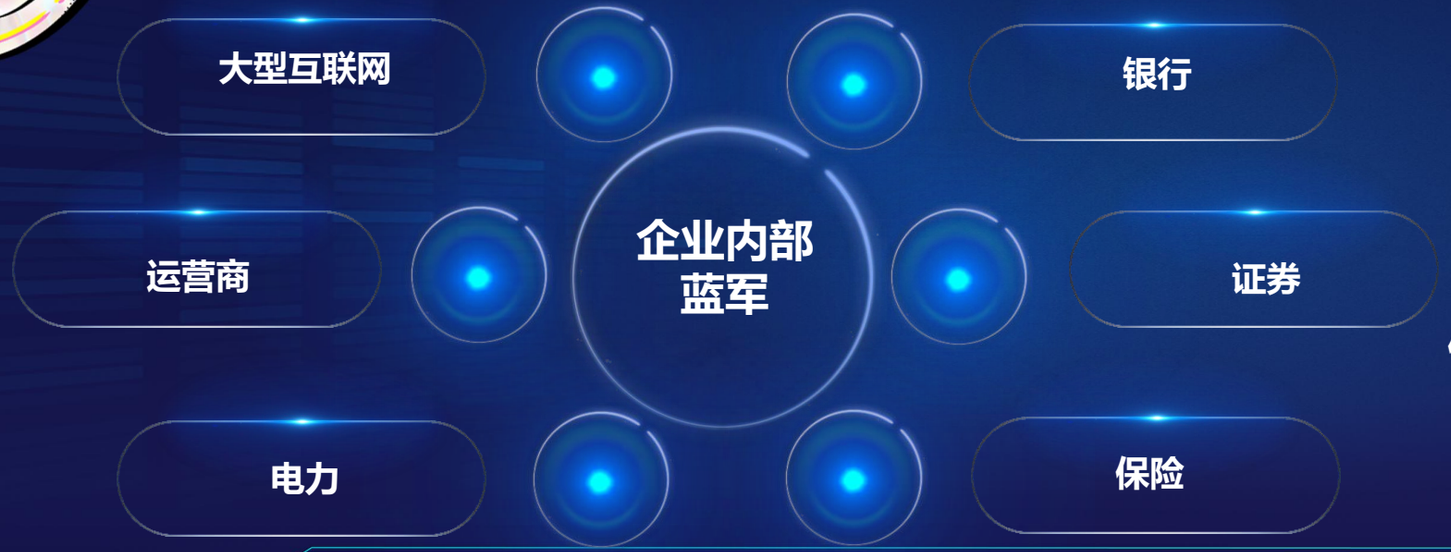
- **商业黑客**
  通过勒索软件、窃取数据等手段对商业组织进行财物勒索

- **竞争对手**
  某些行业竞争对手会使用各种黑客手段窃取商业机密

鉴于严峻的网络安全形势，不同规模的实战攻防演习应运而生

- 国家级攻防演习
- 省级攻防演习
- 地市级攻防演习
- 行业级攻防演习
- **企业内部攻防演习**

企业内部纷纷建立假想敌部队 — 以攻促防



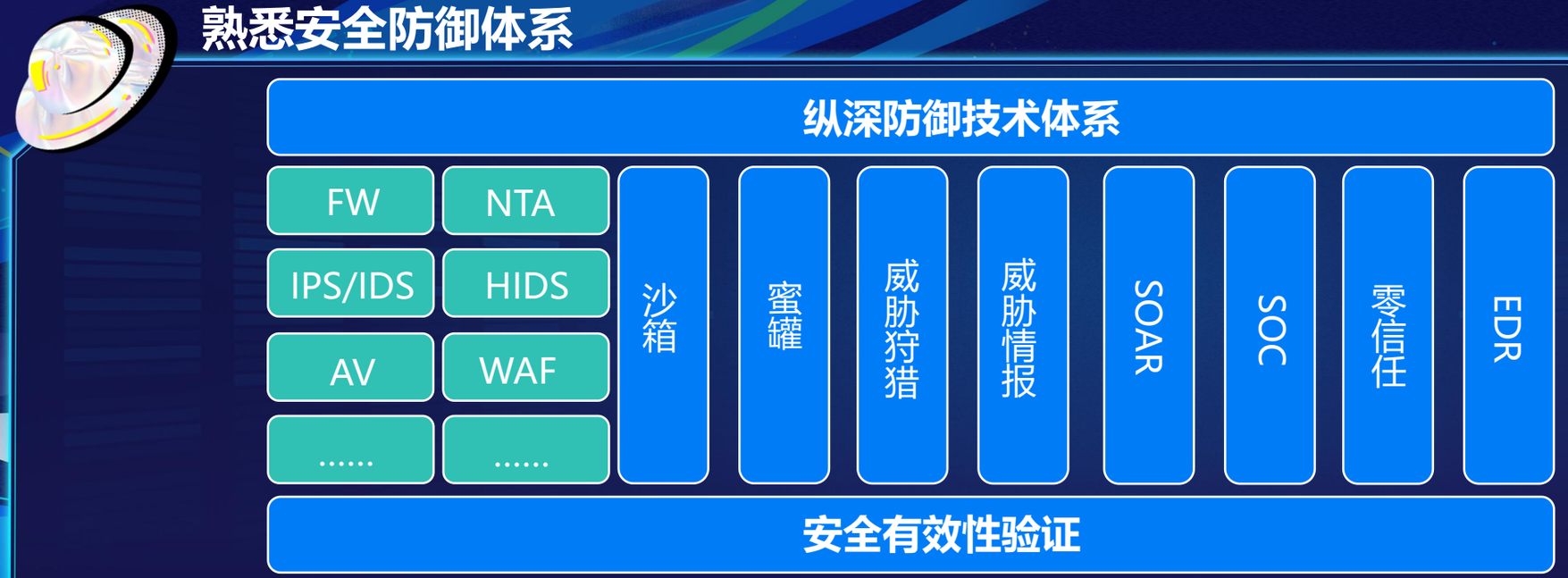
人员规模：

普遍仅有 数名蓝军 成员或虚拟蓝军
仅有极少数大厂蓝军成员人数达到数十人

蓝军人员配置

- ●战术制定
- ●情报搜集
- ●黑盒渗透
- ●代码审计
- ●社工钓鱼
- ●逆向分析
- ● 免杀
- ●近源攻击
- ●内网渗透
- ★熟悉防御体系

熟悉安全防御体系



未知攻，焉知防

知防，更能攻！

“善守者，藏于九地之下；善攻者，动于九天之上；故能自保而全胜也。” -- 《孙子兵法》

威胁企业网络安全的主要攻击方式

1day/0day

应用系统/小程序/公众号
(oa、mail、erp、crm、ehr、srm、cms...)

中间件/框架组件
(weblogic、Apache、fastjson、log4j、shiro...)

各类五花八门的安全工具、集权系统

社工钓鱼

邮件钓鱼
(恶意附件、二维码、超链接...)

社交软件钓鱼
(微信、脉脉、boss直聘、微博抖音、小红书...)

其他社工方式
(电话社工、近源wifi、badusb...)

供应链攻击

攻陷**上级单位、同级单位、下属单位**

攻陷软件**供应商、服务商、合作方**

开源生态投毒

假设我们一定会被0day突破边界！！！

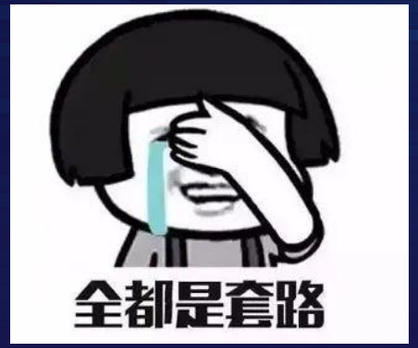
以边界失陷为场景开展演习

演习的攻防起点设置在**各边界突破口**

全年开展以**失陷为假设**的攻防演习

练习红军**快速定位和应急能力**

快速将攻击行为遏制



社工钓鱼手段套路深堪比电诈怎么办?

构建多元化实战化钓鱼场景

- 邮件钓鱼
- 电话钓鱼
- wifi钓鱼
- 社交软件钓鱼
- 线下海报钓鱼
- 勒索病毒演练

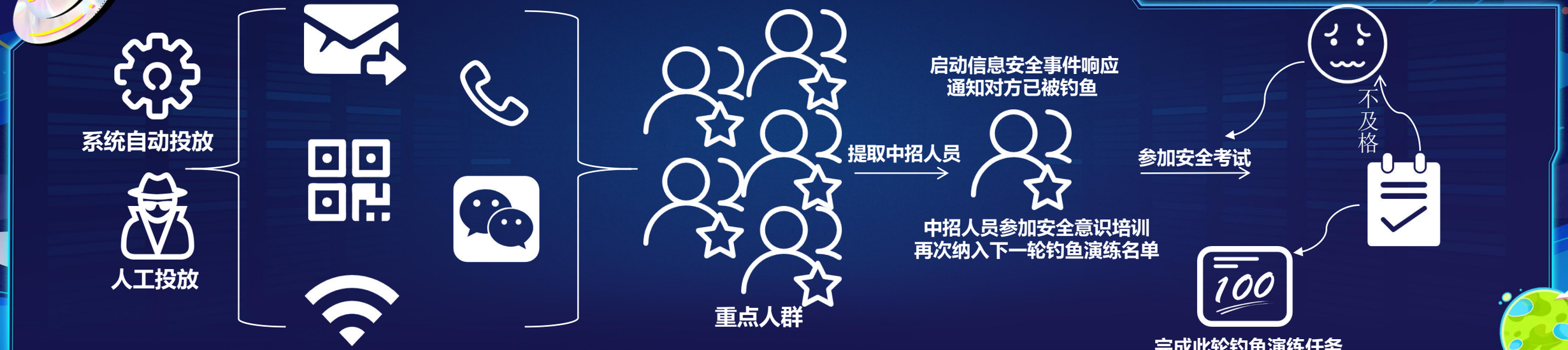
聚焦重点人群

因材施教，以攻击者的思路开展针对重点人群开展针对性的钓鱼演练和安全培训

- 梳理**暴露在互联网的邮箱人群**，此类人群最容易遭受广撒网钓鱼
- 梳理**招聘HR、boss直聘人群**，此类人群最容易遭受病毒简历攻击
- 梳理**脉脉、小红书认证企业员工人群**，此类人群最容易遭受各类话术的社工
- 梳理**各营业网点和职场安保人群**，此类人群最容易遭受物理社工攻击
- 梳理**IT运维岗位人群**，此类人群一旦被攻击成功杀伤力较大

筑牢免疫屏障

钓鱼演习闭环流程


系统自动投放
人工投放
重点人群
提取中招人员
启动信息安全事件响应
通知对方已被钓鱼
中招人员参加安全意识培训
再次纳入下一轮钓鱼演练名单
参加安全考试
不及格
100
完成此轮钓鱼演练任务

供应链的风险问题蓝军可以做哪些工作?

针对外购系统开展安全研究

安全工具

网络设备

集权系统

哑终端

对外购产品进行针对性的审计、0day漏洞挖掘

2023年产出20+个高危0day

针对深度合作的供应链厂商开展演习

- 开展密切合作的重点供应商梳理
- 获得供应商开具的渗透授权
- 针对供应商开展攻防演习
- 建立联防、协作网络安全防护体系

内部分支机构攻防演习活动

概况说明

- 总行蓝军成员组成攻击队在**互联网、办公网**使用钓鱼社工、漏洞攻击等攻击手法， 向**所有分行**防守单位发起攻击，防守单位负责进行监控防守。

演练结果

- 攻击方累计**可控制*****台服务器**，累计可直接**获取数*****万客户敏感信息**，演练期间**发现*****个通用产品0day**漏洞。

达成效果

- **发现各分行的安全隐患并推动修复，提出针对性解决方案和后续整改措施；**
- **通过演习进一步提升分行安全事件的应急处置能力和总分行联动的应急处置效率；**
- **对防御体系有效性进行验证，进一步优化安全设备防护规则及告警规则；**

外部蓝军-引入外部安全厂商、众测与白帽子

以**众多**的第三方的**独立视角**发现实际安全风险

实网攻防对抗

每年组织**10支顶级安全厂商攻击队伍**

以更加集中的方式开展**攻防对抗+沙盘推演**

持续时间:两周

全年开展众测活动

全年对外接收我行漏洞及情报
测试范围:
所有web、app资产
所有公众号
所有小程序
其他相关情报

- 平安SRC众测
- 众测平台1
- 众测平台2
- 众测平台3
- 众测平台4
- 众测平台5

自有蓝军全年随机对抗+外部蓝军辅助参演模式，实现“**平时如战时**”

但仍会存在**周期性**、依赖**人员水平**、**不可复现性**问题

阻碍了攻击成果转换为防守场景

以战养战，实现攻防收益持久化

内部分支机构演练发现的监控失效点

- **分行、**分行、**分行nta无任何流量
- 针对***漏洞、**漏洞的成功入侵nids无对应的检测规则
- 个别机器资产未在cmdb收录，机器未安装hids
- 内存木马hids无相关告警

闭环能力

- 将演练的成果固化成常态化的验证能力
- 开展自动化的失陷场景的防御有效性验证
- 让演练成为促进安全防御能力提升的内生动力

用例执行， 有效性平台持续验证

7*24小时自动巡检验证

队伍练兵机制

- 靶场
- 内部演练
- 知识库
- 漏洞库
- 技术分享
- CTF竞赛
- 实网攻防
- 安全琅琊榜

引进高校毕业生，培养其攻防技能，打造一支**高素质、能攻善守**的后备攻防人才队伍

网络安全 FCIS 2023创新大会

THANKS

FREEBUF