ICBC
工银科技

于细节处见精神

——些许银行信息安全工作实践心得

工银科技/王贵智

威胁框架：细粒度对抗

提纲

关于我：

银行业信息安全工作从业者

13年一线安全工作经历

CISSP/CISA

努力做好金融业信息安全工作

关于分享内容：

介绍实践的经验/分享工作心得/寻求合作共赢

长缨待展

CONTENTS

目 录

01 商业银行信息安全工作概览

02 信息安全工作实践举例

03 总结与展望

01 商业银行信息安全工作概览

商业银行信息安全工作特点

信息安全工作特点：

- 安全事件影响范围广，危害程度深
- 黑客能力高，威胁隐蔽性强
- 行业关联融合加深，风险跨领域传导广
- 木桶效应突出，综合防护要求高，攻防对抗不对称
- 技术变化快，衍生安全风险多
- 安全敏感性强，自主可控要求高

+

行业特点：

- 行业敏感度高
- 行业监管严格
- 业务规模大、条线多
- 业务场景变化快
- 技术互联网化，版本迭代快
- 数据价值高
- 业务对安全需求高

=

商业银行信息安全工作：

- ✓ 信息安全顶层要求高、行业监管严中趋于更严
- ✓ 银行开放化、数字化转型扩大风险面，新渠道、新合作方成为新风险集中点。
- ✓ 新技术的演进不断引入新风险，云计算、大数据、生物识别等金融科技新技术发展，需要新的安全防护技术
- ✓ 金融生态圈涉及交易参与方多、环节多、风险暴露面增加、防护链条长、防护面广
- ✓ 数据价值激发的数据泄露、数据滥用风险日益严峻
- ✓ 资金利益紧密相关方，网络攻击、网络犯罪的最终目标所在。
- ✓ 所有人都知道信息安全工作很重要，但是。。。。。。

商业银行信息安全工作实践

我行高度重视信息安全工作，秉承既严谨求实、又开拓进取的态度，积极运用新思维、新技术解决风险难题；自主研发了安全态势感知平台（SOC），积极参与拟态防御、量子技术等新技术运用研究。多年来在防护体系建设、自主可控实施、安全技术研究与实践、安全核心能力提升等方面，在各项安全工作成果中，都在商业银行中保持了显著优势位置。

全行“一盘棋”管理模式，管理层深度参与

重视运营，构建主动防护体系，全集团一体化智能化安全运营

安全工作与新技术工作，同步设计、同步建设、同步运行

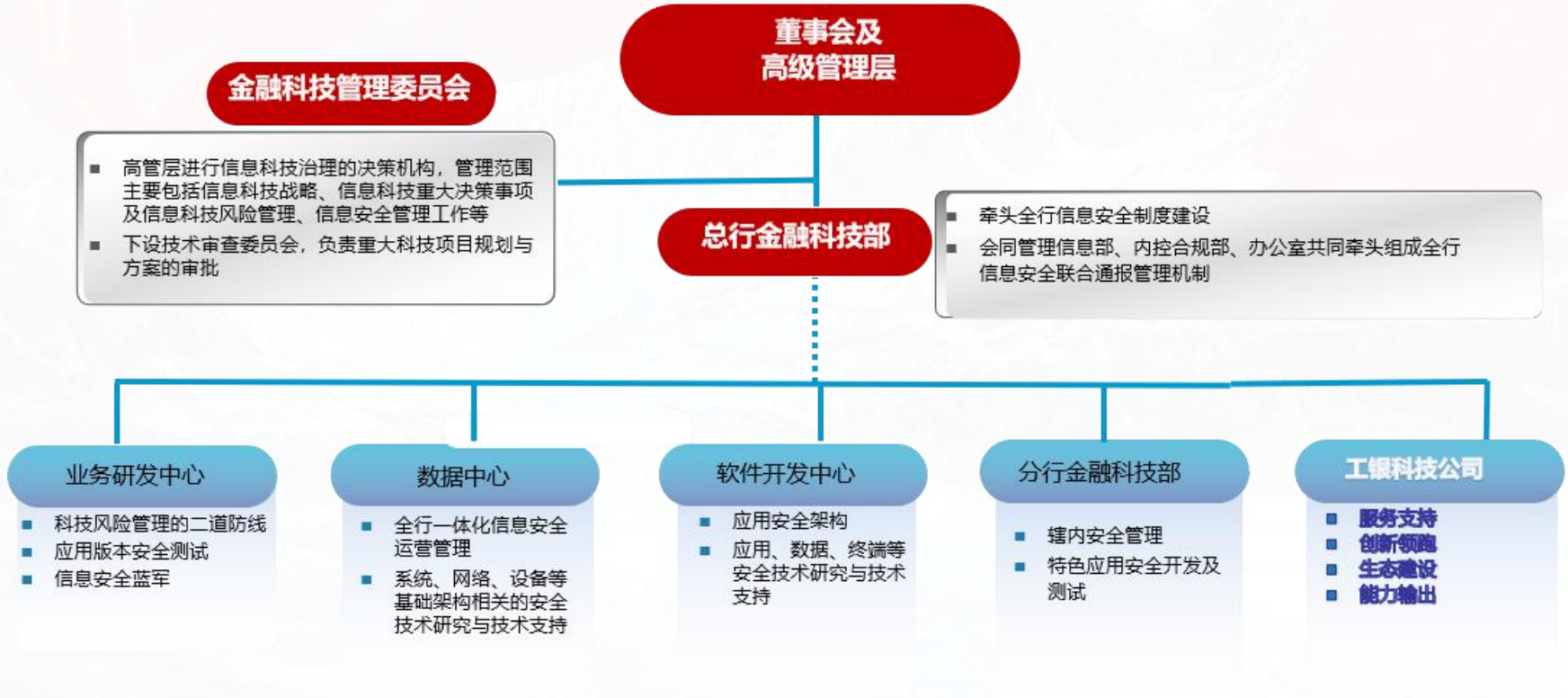
持续加强基础安全防护，满足内外部环境变化需求

攻防相长，安全体系螺旋式自我提升

嵌入式、全流程研发过程安全管理体系

威胁框架：细粒度对抗

银行实践之职责明晰的组织架构



银行实践之统一管理框架

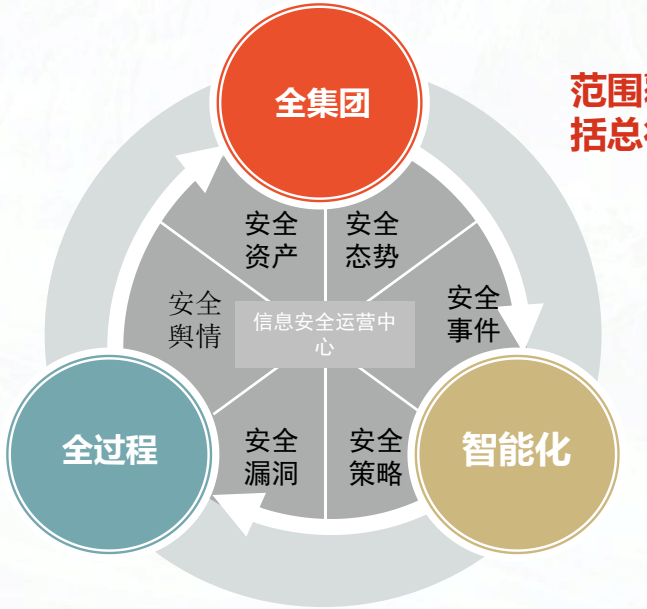
结合国际国内标准规范以及我行实际，制定了全行信息安全管理总体框架，构建了完备信息安全体系，指导全行信息安全工作。

- 通过攻击视角以攻促防
- 建立全生命周期防护机制
- 构建独立信息安全运营中心
- 引入新技术场景
- 构建纵深防御网络防护体系
- 有效防御外部各类安全攻击
- 自主研发终端安全防护软件
- 有效防范内部信息泄露风险

威胁框架：细粒度对抗

银行实践之一体化安全运营

➢建立完善了全集团、全过程、智能化的安全态势感知平台(soc)，围绕此平台,建立覆盖全集团、统一的信息安全运营中心，进一步提升工商银行主动、立体的安全防御能力，切实保护银行信息系统以及客户信息和资金安全。



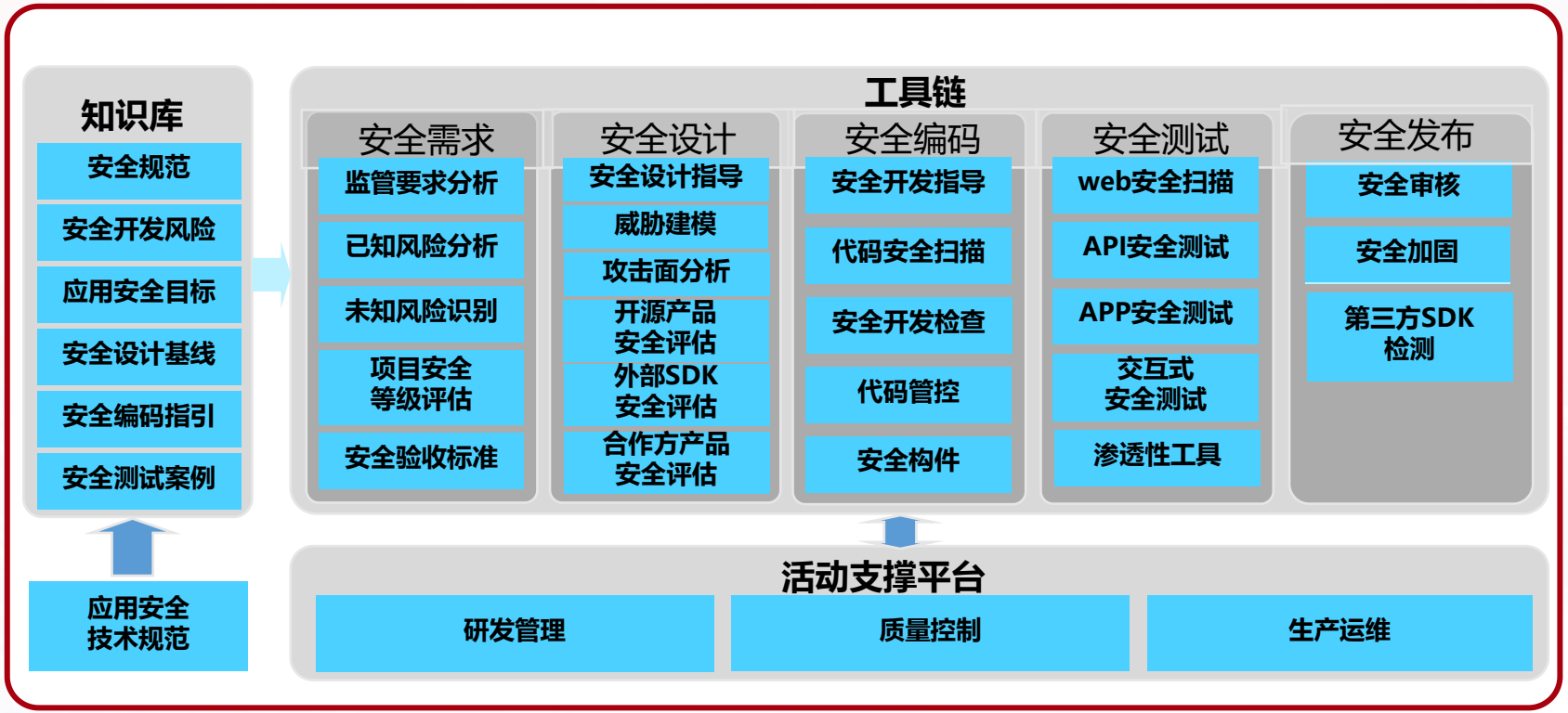
范围覆盖工商银行全集团各个机构，包括总行本部、三大中心、各分支机构。

实现事前预防、事中监测与处置、事后分析全生命周期安全管控。

通过引入大数据、机器学习等技术，探索人工智能与安全技术的深度融合，全方位全天候实时感知和处置各类攻击行为，与各安全系统联动实现智能防御。

威胁框架：细粒度对抗

银行实践之全流程安全管理体系

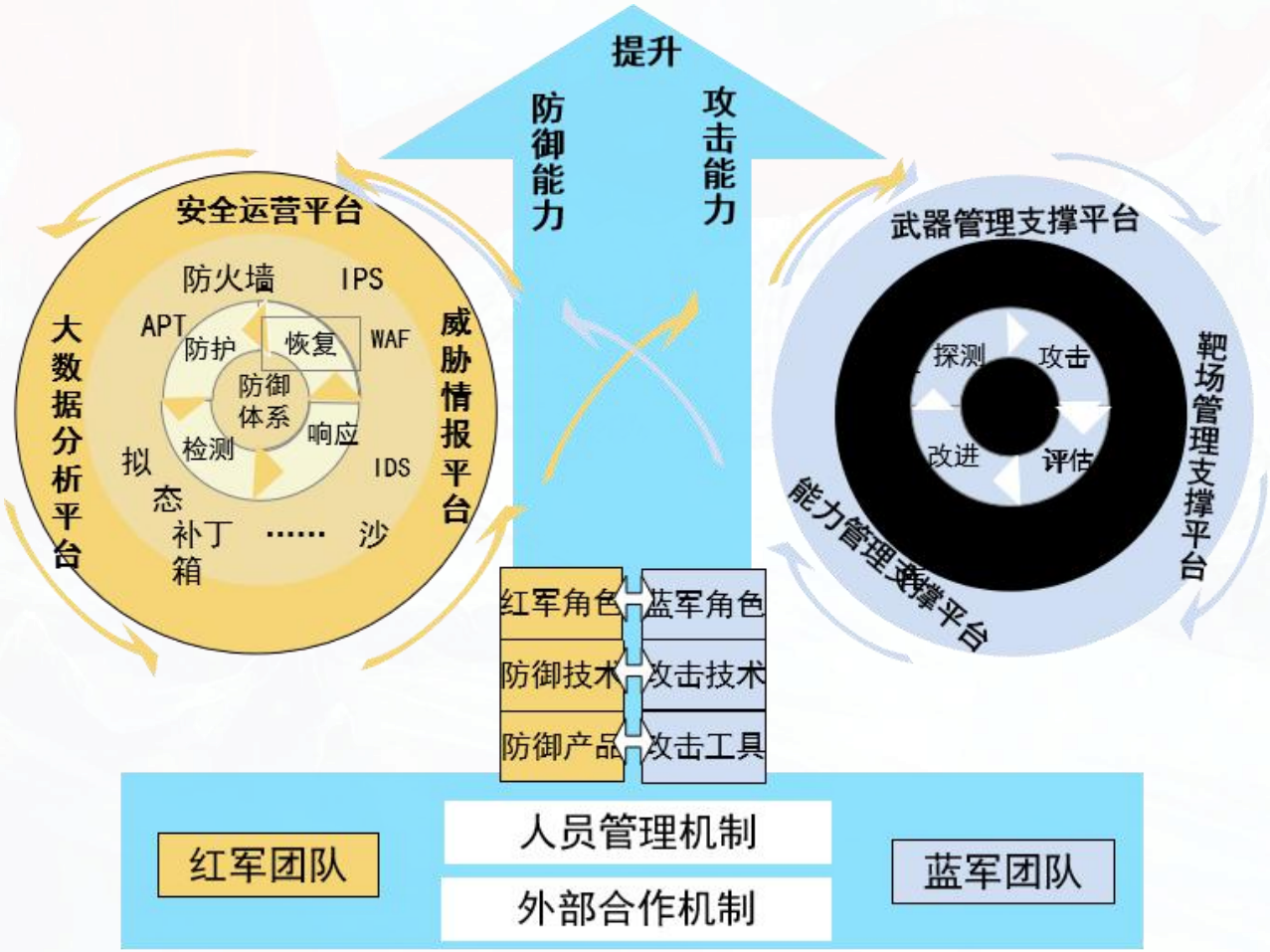


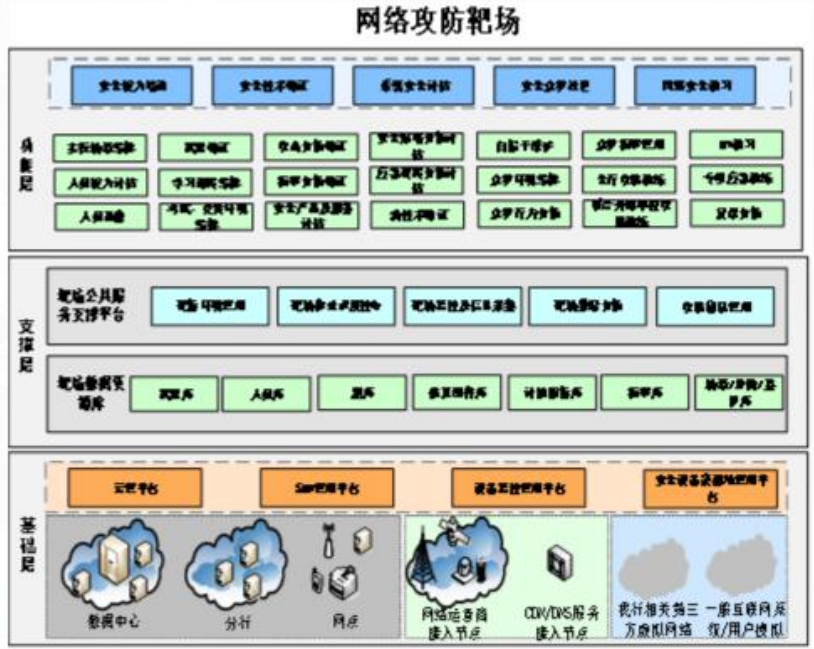
知识库：为研发测试各阶段落实安全技术规范提供具体的操作指南，能够覆盖不同应用的业务及技术特性。

工具链：针对不同应用特性进行工具差异化 、本地化建设；实现与DevOps的集成，提升安全活动效率。

支撑平台：对现有研发测试管理系统进行改造，补充安全活动，并与知识库、工具链集成，提升安全活动的自动化水平。

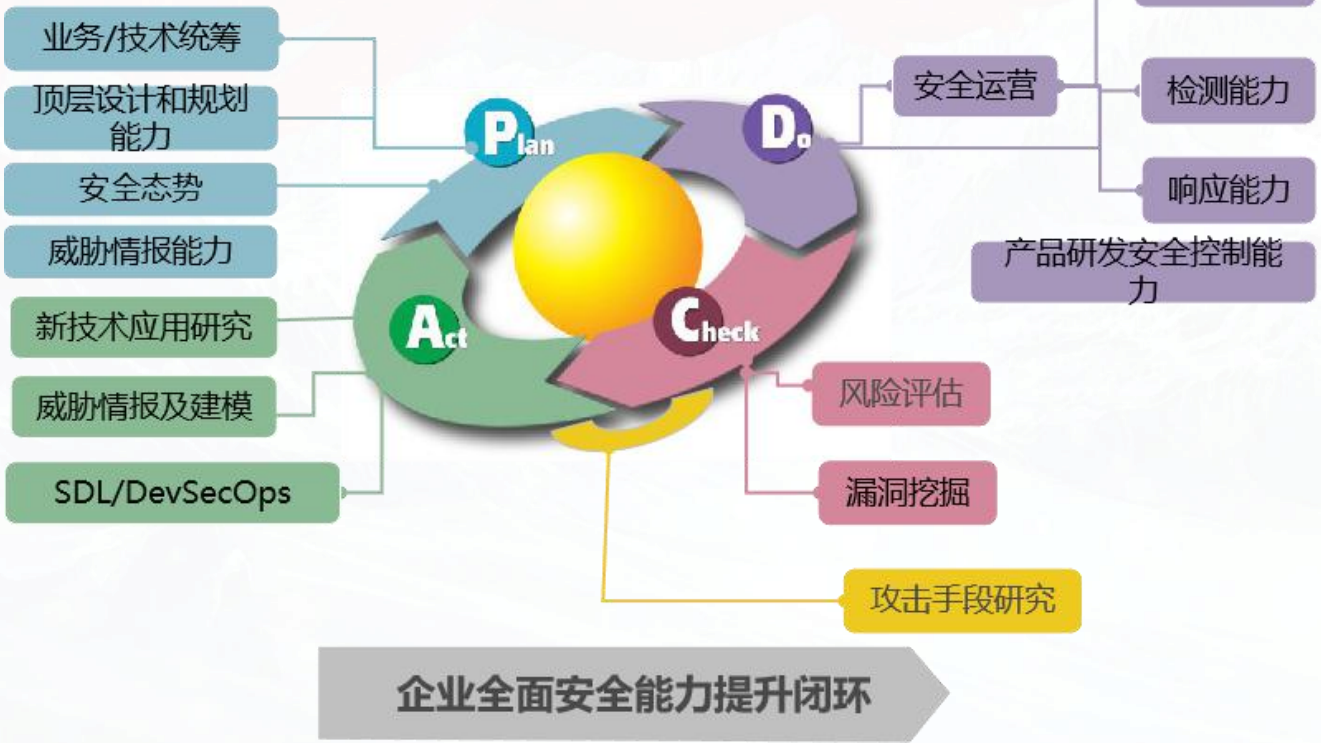
银行实践之攻防对抗能力相长





威胁框架：细粒度对抗

实践成效



- 等保建设
- 技术比赛
- 监管评级
- HW演练
- 风险课题
- 统一运营
- 。。。。

威胁框架：细粒度对抗

长缨待展

威胁框架：细粒度对抗

02 银行信息安全工作实践举例

安全实践：于细节处见精神

何以称之为安全？什么是安全运营精神？

图片来源：Getty Images、BBC

1. 「狂热的纪律」
2. 「以实证为依据的创造力」
3. 「建设性的偏执」
4. 「第五级领袖心」

- 信息安全的实质在于对抗；站在更高的视角，我们都是对抗中的防守者，安全运营就是要将我们的防守做更好！
- 安全人员不仅仅是“背锅帝”和“求火队”，更是安全能力的“建设者”，是不断挑战极限的“攀登者”。
- 既有成绩不是一蹴而就的，而是靠实践积累、时间沉淀，是真刀真枪磨练出来的；成就没有捷径，唯有尊重实践，脚踏实地才是唯一的达到目标的“捷径”。
- 安全不是一个结果，安全是一个过程；安全不仅是内容，安全更是态度。

“向荆棘丛寻宝藏，于无声处听惊雷”

反钓鱼的自主发现工具

一起典型的欺诈案例

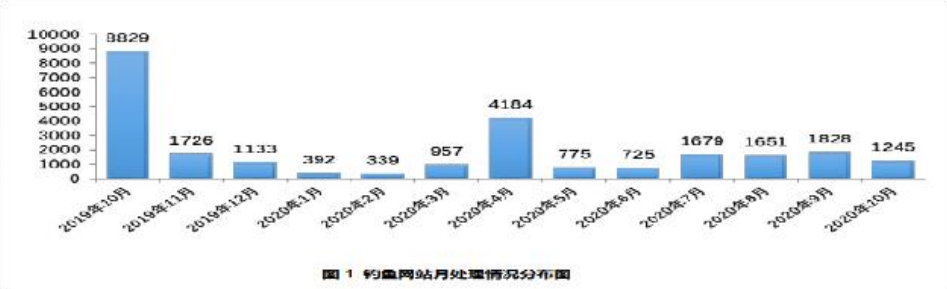
■2019年12月，深圳市的周女士和陈女士收到一条短信告知因中行卡延时还款将影响征信，请及时联系客户专员。在联系客户专员后，专员告知可以通过微信公众号进行处理。两位女士添加了中行自助服务部公众号，并按照“客户专员”指导进行了多步操作，包括绑定个人的信用卡,输入授权码（其实是转账金额），填入微信验证码，最终被骗走了两笔9817元。通过点击该公众号其实假冒的中行公众号，通过查看账号主体信息可以看到这并不是中行的公众号。

威胁框架：细粒度对抗

网络钓鱼危害与现状

1-钓鱼网站现状

- 假冒网站是网络钓鱼、电信诈骗的重要渠道之一，中国反钓鱼网站联盟每月要处理上千个举报的假冒网站；2020年10月，**支付交易类和金融证券类**的假冒网站占据全部假冒网站的**99%**以上，是假冒网站的主要风险集中区。
- 钓鱼网站的**生存周期短**，根据我们的统计平均为1~7天，业界有说法为平均不足2天。
- 据CNCERT统计，2020年9月共监测到15128个境内仿冒网站，此外，在其9月份受理的8,002件事件报告中，排名前三位的安全事件分别是恶意程序、漏洞、**网页仿冒类**事件；
- 钓鱼网站是最经典的中间人攻击行为，结合其他欺诈手段（比如SPAM、伪基站等）仍然是网络诈骗犯罪经常使用的手段之一，也是银行面临的最典型、最常见的安全难题之一。



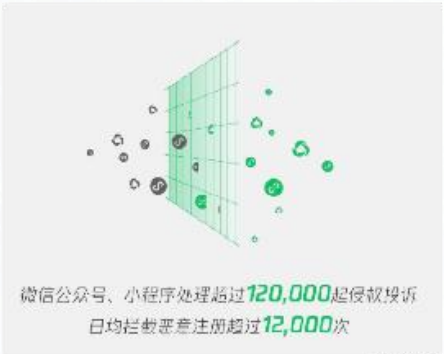
钓鱼网站攻击流程

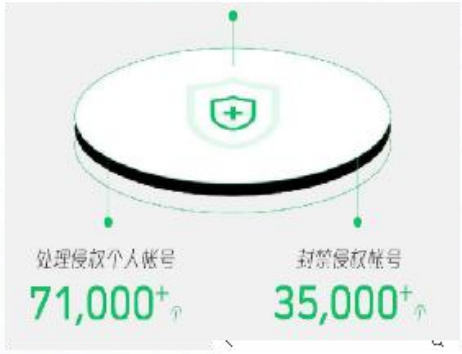
网络钓鱼危害与现状

➢ 2-假冒公众号现状（公众号钓鱼）

■ 假冒微信公众号安全风险加剧

- ✓ 微信公众号因注册成本低，用户群广，使用便捷，已经成为犯罪分子进行网络钓鱼、实施诈骗的新途径。
- ✓ **假冒微信公众号数量大，**根据《2020年微信知识产权保护报告》，全年处理12万起侵权投诉、封禁3.5万以上的侵权账号，而这只是被发现的冰山一角而已。





➢ 3-App钓鱼现状

■仿冒APP是实施诈骗的新型手段，金融领域涉及金钱交易，更是仿冒APP的重灾区，上海黄金交易所、京东金融、微粒贷、蚂蚁花呗、360金融、苏宁金融等知名企业的APP都曾被仿冒过。

■国家互联网金融风险分析技术平台显示（截至2020年5月底），互联网金融仿冒APP共发现2801个，累计下载3343.7万次。

威胁框架：细粒度对抗

反钓鱼工作实践

➢ **反钓鱼技术发展路线图：**

2009年，反钓鱼网站

基于门户、个人网银等应用的web日志自主开发了钓鱼网站发现工具

2013年，反钓鱼网站加强

基于互联网遍历相似域名，将反钓鱼网站发现工具加强，覆盖面更广

2017年，反假冒APP

自主研发假冒APP识别工具；
基于图像对比技术；
基于APP数字证书过滤技术；
基于可疑权限分析

2020年，反假冒微信公众号及不合规内容监测

自主研发假冒微信公众号识别工具；
基于图片相似度计算；
领域知识库构建；
词向量构建、语义分析模型等技术。

……

持续优化

我行因客户过亿，多年来一直在反钓鱼方面投入巨大，被仿冒的钓鱼网站数量多年位居被仿冒对象第一名，深受其扰，同时也在反钓鱼领域也积累了深厚的技术和防御经验。2019年共发现**4972**例针对工行的假冒网站，2020年共监测发现假冒工行微信公众号**79**个，包括诱导转账、假冒贷款链接，收集银行卡号、身份证号等敏感信息；发现**295**例不合规的公众号风险。

钓鱼网站防治实践

发现假冒网站的几种方法

- 利用假冒网站通常引用合法网站页面资源的特点，从合法网站的后台的访问日志中寻找发现；
- 自2009年开始使用这种方法自主发现假冒网站；
- 准确性高但发现时效性不足

- 用户的上网终端安装客户端，提供客户端举报（人工\自动）的渠道；
- 网银防钓鱼控件，但覆盖度不高、体验差。
- 准确性高、时效性较好，但发现程度依赖客户端数量。

- 通过互联网搜索相似域名或相似页面，再进一步通过自动和人工分析的方法，发现正在提供服务的假冒网站；
- 相似页面的分析依赖专业互联网搜索引擎技术和识别算法的准确性；
- 覆盖面广、发现量大、时效性较好，但消耗资源大且发现效率不高（仍需依赖人工识别）

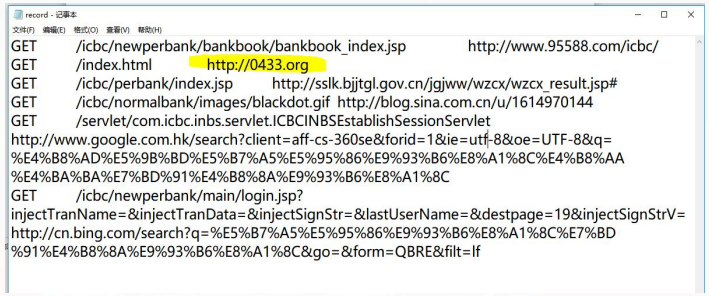
- 通过在电信骨干网络节点上部署网络嗅探工具，发现和分析相似域名、相似页面，进而识别发现钓鱼网站；
- 只能由具备资源的企业或机构开展
- 时效性好、覆盖面广

处理假冒网站的几种方法

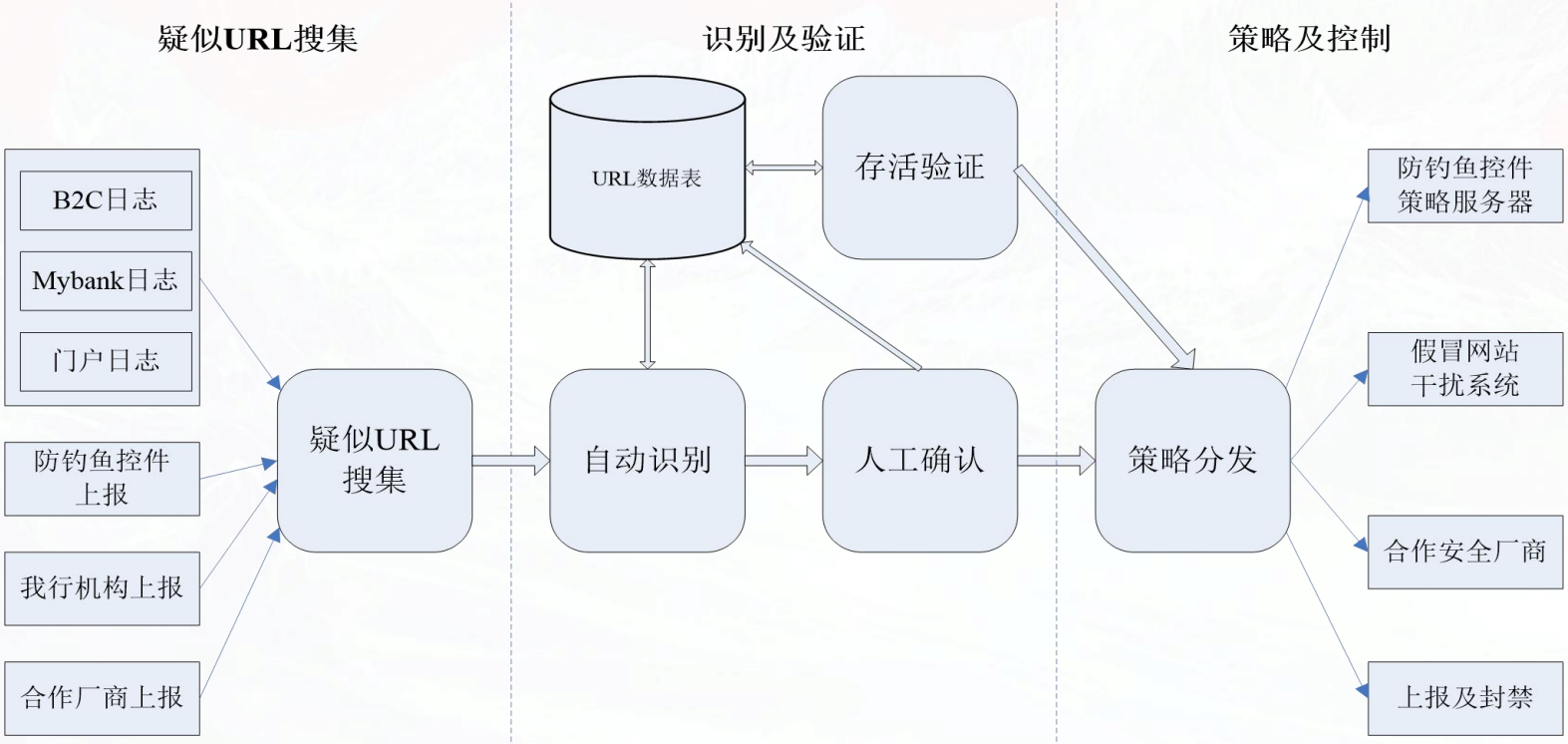
- 端点访问阻断
- 域名访问阻断
- 网站关停下线
- 网站可用性破坏（干扰数据）

威胁框架：细粒度对抗

钓鱼网站防治实践（2009年）



没有足够的终端侧代理。没有必要的骨干流量或域名请求信息。
那么就从我们掌握的数据着手，从海量web日志中寻找价值。



威胁框架：细粒度对抗

钓鱼APP防治实践（2014年）

实现流程：

1、HTTP(GET/POST）请求，从应用市场上获取APP应用

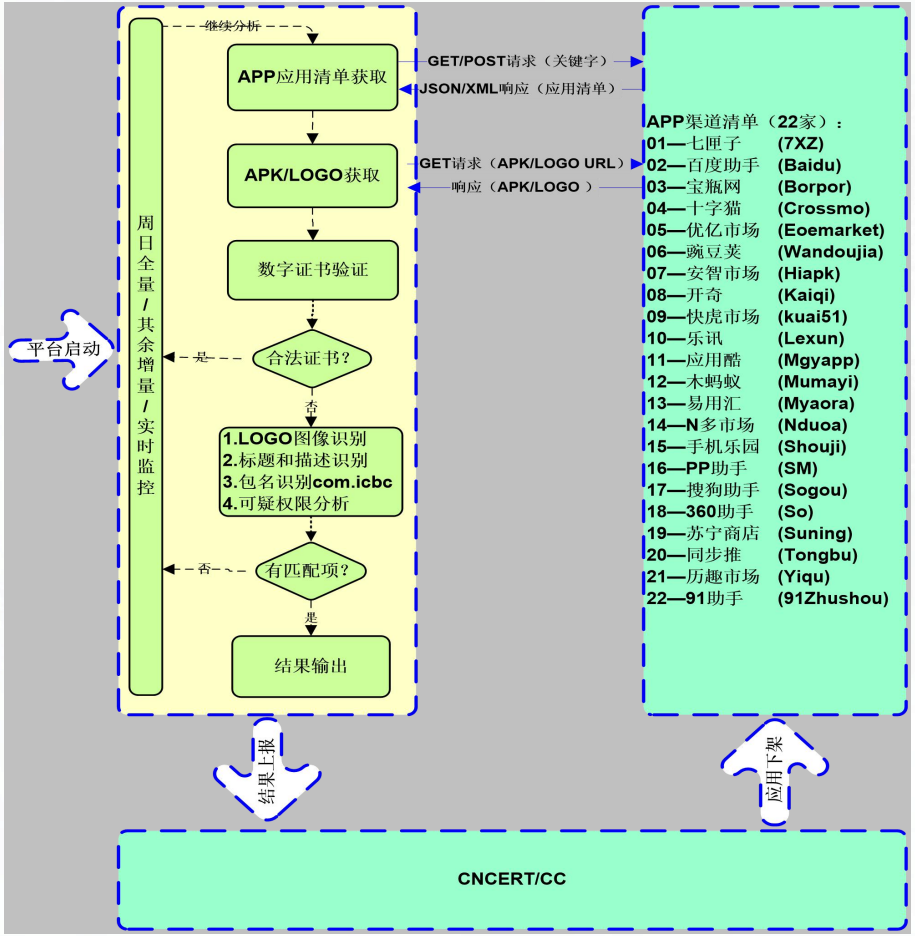
2、验证APP应用的数字证书是否为我行签发

3、采取关键字匹配、图像识别、包名识别等技术排除干扰项

4、反编译分析可疑权限

5、人工装机确认

6、通过CNCERT/CC协调应用市场下架



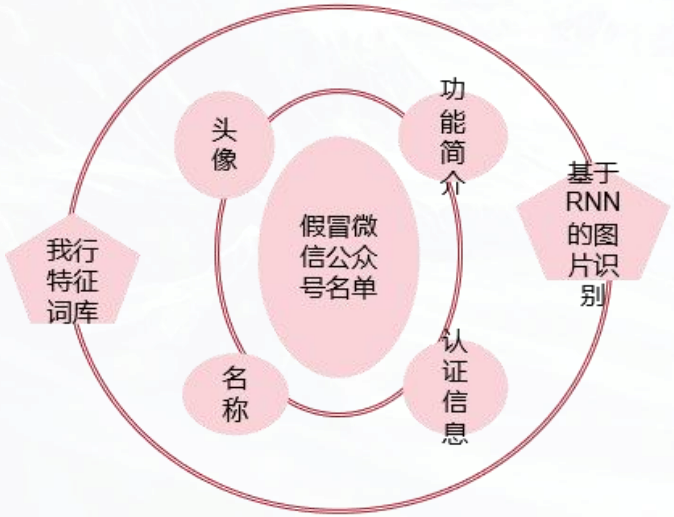
实现原理：

android系统通过证书签名体系确保APP内容的真实性和完整性，开发人员在完成APP开发后，使用私钥对APP文件进行签名生成证书，通过非对称密钥体系保证证书的不可抵赖性。签名发布后，如果修改了APP中的文件，android系统在安装APP时会进行告警并停止安装

钓鱼微信公众号实践（2019年）

假冒公众号发现

- 假冒形式多种多样，针对关键字及图片的变形、组合，插入特殊符号的假冒类型检
- 实现了基于名称、认证信息、头像、功能简介等多因素实现了假冒公众号综合判断算法，提高识别准确性和全面性。

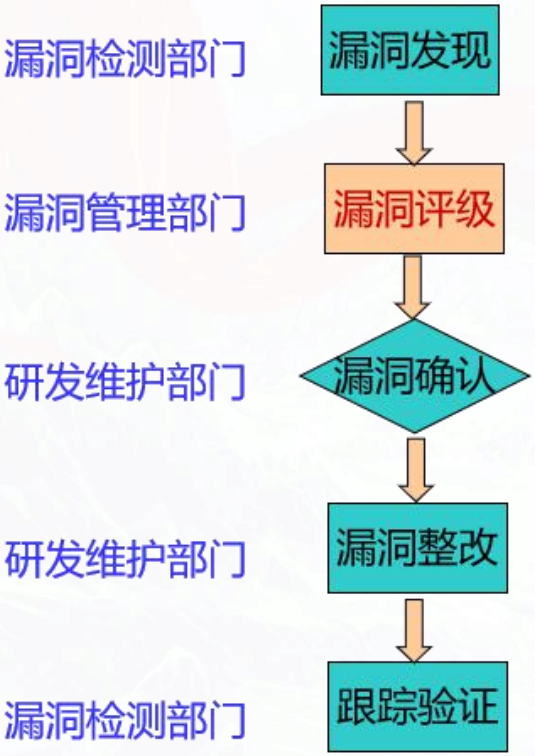


安全漏洞定级工具

安全漏洞管理中经常遇到的疑问

- **一个漏洞不改会产生风险的可能性到底多高?**
- 开发人员开发的是产品，本来就很忙，为什么还要我去改漏洞!
- 漏洞到底要不要整改，怎么整改才算没有风险?
- **通常所说的“高风险”漏洞，到底有多高?**
- 能见到一个工作流平台的漏洞问题单流转1年甚至更长，怎么办?
- **漏洞风险等级到底谁说了算数?**
- 漏洞整改过程中出现业务中断风险，谁来承担责任?

安全漏洞管理流程及相关部门



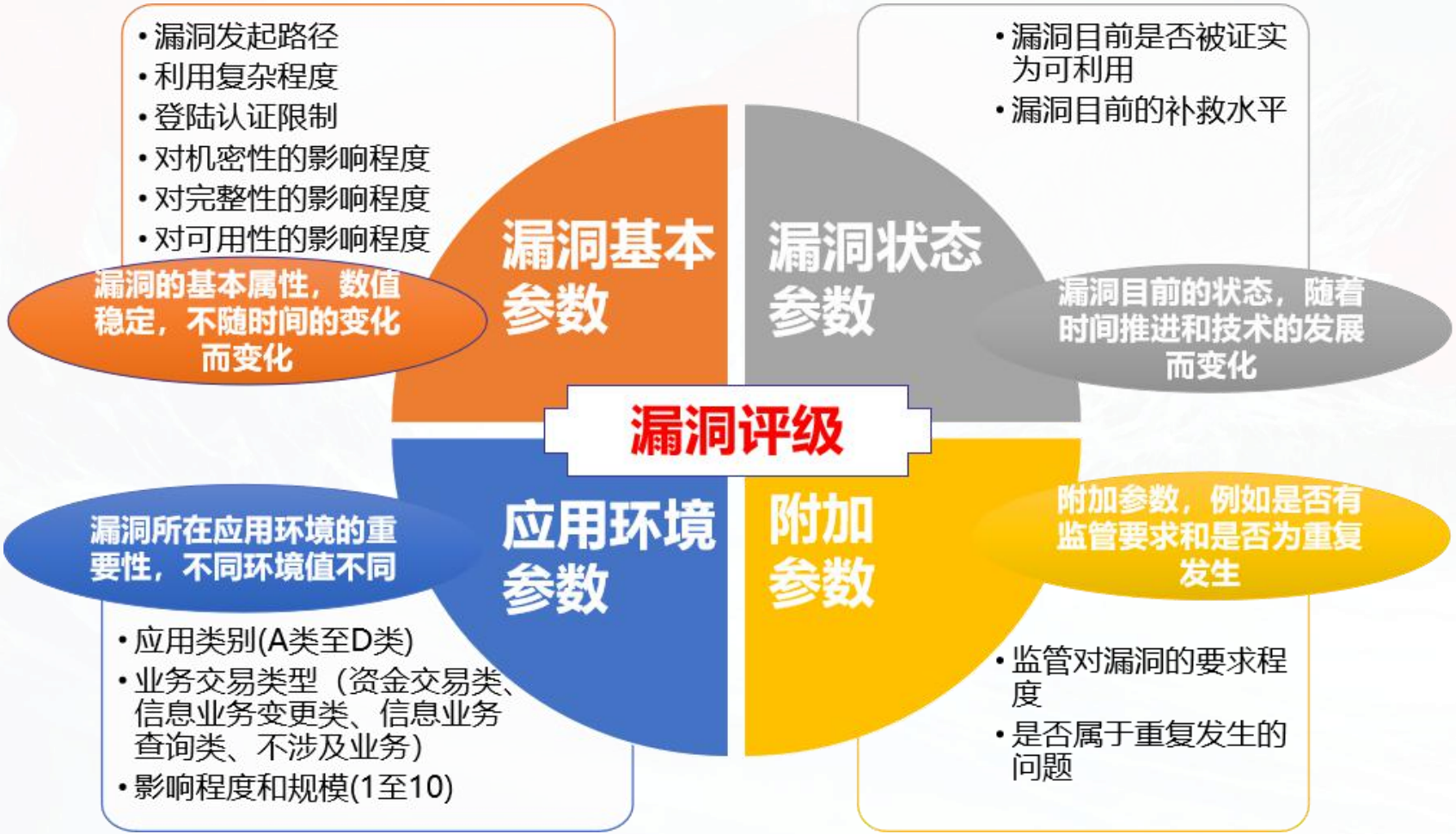
发现途径：①内部测试、评估；□ 外部审计、测评

评审内容：
□ 漏洞确认及评级准确性
□ 漏洞整改时限及补偿控制措施

整改时限要求（默认要求，特殊情况单独说明）：
（1）生产环境发现的问题
严重、高风险：24小时内完成整改；
中风险：5个工作日完成整改，
低风险（包含提示级）：当季度版本完成整改，
（2）测试环境发现的问题
严重、高、中风险：版本投产前完成整改；
低风险（包含提示级）：当季度版本完成整改

漏洞定级是漏洞管理推进的关键和基础。

安全漏洞评级工具（2014年）

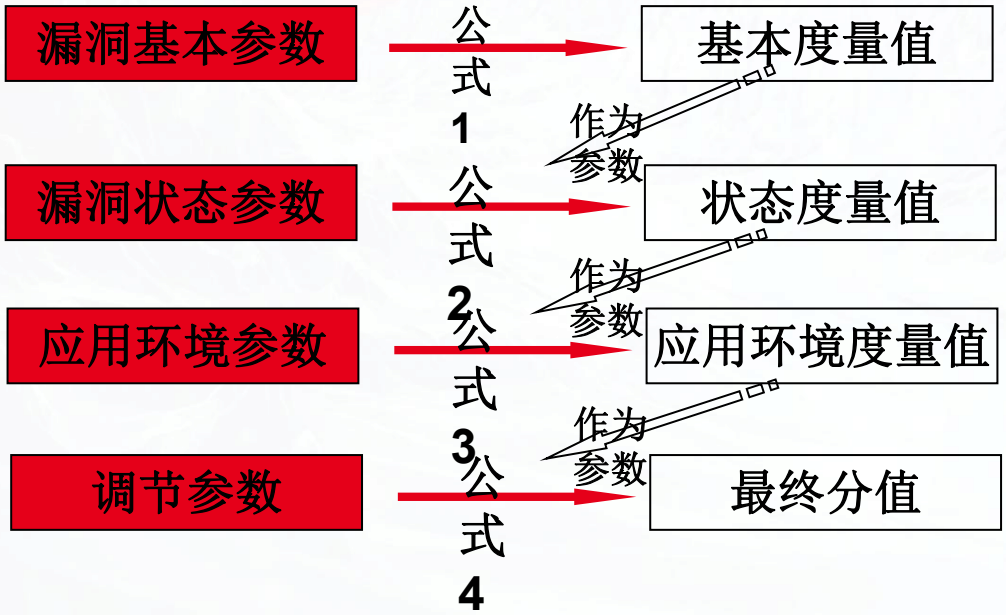


4类参数
4方参与
5个等级
10分分值

威胁框架：细粒度对抗

漏洞等级计算过程

漏洞分值主要参考了CVSS（Common Vulnerability Scoring System，通用漏洞评分系统）计算方法，并根据我行实际应用情况对算法进行了改进。基本计算过程如下：



Impact=10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability=20*AccessVector*AccessComplexity*Authentication
BaseScore=round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)–1.5)*f(Impact))

TemporalScore=round_to_1_decimal(BaseScore*Exploitability*RemediationLevel*ReportConfidence)

AdjustedImpact=min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)*(1-AvailImpact*AvailReq)))
AdjustedTemporal = TemporalScore recomputed with the BaseScore’ s Impact subequation replaced with the AdjustedImpact equation
EnvironmentalScore=round_to_1_decimal((AdjustedTemporal+(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)

部分参数赋值方法

1、应用安全级别赋值公式 = 0.2+（8-应用类别-业务交易类型）*1.31/6

机密性需求、完整性需求、可用性需求分值		应用类别			
		1-A类应用	2-B类应用	3-C类应用	4-D类应用
业务交易类型	1-资金交易类	1.51	1.29	1.07	0.86
	2-业务变更类	1.29	1.07	0.86	0.64
	3-业务查询类	1.07	0.86	0.64	0.42
	4-非业务类	0.86	0.64	0.42	0.20

2、根据监管要求调整分值：　　分值调整1== CVSS + （10 - CVSS） * 监管要求

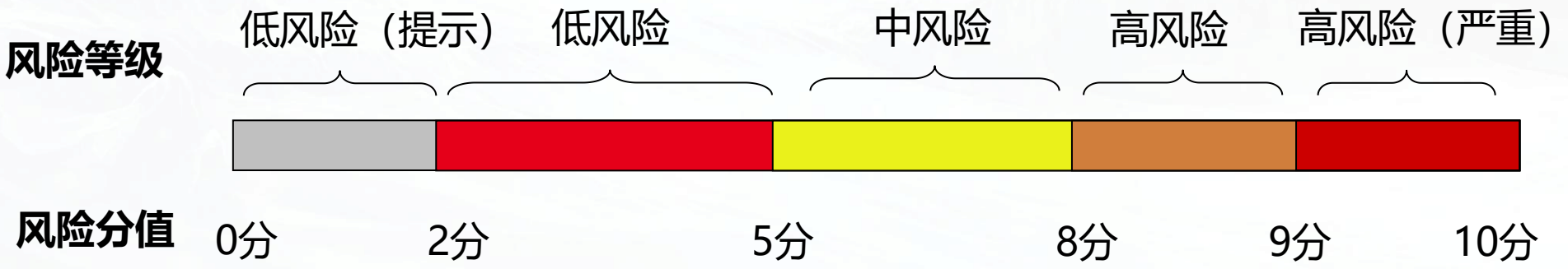
其中，监管要求定义为三个级别，权值分别为高（0.3），一般（0.15），无（0）。

3、根据漏洞是否重复发现或是否长期未修复调整分值：　　分值调整2 = 分值调整1 * 重复发生值

其中，对于重复发生值，如果漏洞属于重复发生，则取值1.05，否则取值为1。如果“分值调整2”计算结果大于10，则取值为10。

漏洞等级与分值对应关系

评级	分值范围
低风险（提示）	评分0.0分 ~ 1.9分
低风险	评分2.0分 ~ 4.9分
中风险	评分5.0分 ~ 7.9分
高风险	评分8.0分 ~ 8.9分
高风险（严重）	评分9.0分 ~ 10分



备注：参考了OWASP、CVE、CNVD等漏洞库的漏洞等级

实践举例1：同一漏洞在不同业务应用

例如：通过互联网接入测试发现了某全行网站登录前页面的一个跨站脚本执行漏洞。监管对跨站脚本执行漏洞的要求比较高，另外假设这是首次在该网站上发现跨站脚本执行漏洞，并且开发部门有成熟的解决方案。另设定影响程度和范围值为6。基本参数、漏洞状态参数、调节参数如下：

漏洞基本参数						漏洞状态参数		调节参数	
利用途径	利用复杂度	登录认证次数	对机密性的影响	对完整性的影响	对可用性的影响	目前的可利用状态	目前的补救水平	监管要求	重复问题
远程	中	无需认证	部分影响	部分影响	部分影响	高可利用	官方补丁	高	否

经过计算，不同应用对应的分值和等级如下：

应用类别 业务交易类型	A类	B类	C类	D类
资金交易类	8（高风险）	7.7（中风险）	7.3（中风险）	6.9（中风险）
业务变更类	7.7（中风险）	7.3（中风险）	6.9（中风险）	6.4（中风险）
业务查询类	7.3（中风险）	6.9（中风险）	6.4（中风险）	5.7（中风险）
非业务类	6.9（中风险）	6.4（中风险）	5.7（中风险）	5.1（中风险）

实践举例2：同一漏洞在不同位置

例如：在某信息安全等级为3级的B类应用上存在一个SQL注入漏洞。监管对SQL注入漏洞的要求比较高，另外假设这不是第一次在该系统上发现跨站脚本执行漏洞（重复发现），并且假设开发人员有成熟的解决方案。

漏洞基本参数						漏洞状态参数		应用环境参数		
利用途径	利用复杂度	登录认证次数	对机密性的影响	对完整性的影响	对可用性的影响	目前的可利用状态	目前的补救水平	应用类别	业务交易类型	受影响程度或规模
（待定）	低	（待定）	严重影响	严重影响	严重影响	高可利用	官方补丁	B类应用	业务查询类	6

经过计算，同一应用，不同访问方式和不同位置的漏洞对应的分值和等级如下：

认证次数\利用途径	远程	局域网	本地
无需认证（无需登录）	9.3（严重）	8.3（高风险）	7.5（中风险）
一次认证（需登录认证）	8.7（高风险）	7.9（中风险）	7.3（中风险）
多次认证（需多次认证）	8.3（高风险）	7.6（中风险）	7.1（中风险）

实践举例3：门户类站点常见漏洞等级测算

漏洞名称	风险级别	分值	漏洞基本参数						漏洞状态参数		应用环境参数			调节参数	
			途径	复杂度	登录认证次数	对机密性的影响	对完整性的影响	对可用性的影响	目前可利用状态	目前的补救水平	应用类别	业务交易类型	受影响程度或规模	监管要求	重复问题
SQL注入	高风险	8.9	远程	低	无需认证	严重影响	严重影响	严重影响	高可利用	官方补丁	B类应用	业务查询类	6	高	否
跨站脚本执行（存储型）	中风险	7.3	远程	低	无需认证	部分影响	部分影响	部分影响	高可利用	官方补丁	B类应用	业务查询类	6	高	否
跨站脚本执行（反射型）	中风险	6.9	远程	中	无需认证	部分影响	部分影响	部分影响	高可利用	官方补丁	B类应用	业务查询类	6	高	否
跨站脚本执行（DOM型）	中风险	5.8	远程	高	无需认证	部分影响	部分影响	部分影响	高可利用	官方补丁	B类应用	业务查询类	6	高	否
端口开放过多	中风险	6.5	远程	低	无需认证	严重影响	无影响	无影响	可利用	官方补丁	B类应用	业务查询类	6	一般	否
JAVA错误信息泄露	低风险	4.3	远程	中	无需认证	部分影响	无影响	无影响	可利用	官方补丁	B类应用	业务查询类	6	一般	否
403隐藏页面泄露	低风险	4.3	远程	中	无需认证	部分影响	无影响	无影响	可利用	官方补丁	B类应用	业务查询类	6	一般	否

DNS日志分析工具

用DNS日志分析补充防病毒技术的实践（2017年）

由于当前大型企业的终端、服务器的数量巨大，且一些设备对于计算资源消耗更为敏感，因此当前传统的反病毒技术仍然是企业主要依赖的安全技术之一。但因为传统技术多是基于特征码和病毒库的，因此存在一些局限：

1、滞后性，特征码必须要有样本支撑，因此必然存在滞后性。

2、准确率低，病毒的特征是模糊的，过分严格的策略会影响正常程序使用，甚至影响业务。

3、效率低，要检测的病毒数量有时甚至会超过正常文件数。

4、针对性差，针对0day等APT攻击行为，无法有效发现恶意程序。典型的案例包括孟加拉央行swift系统被攻击案件等。

- 为隐藏攻击源和躲避查杀，恶意程序进入内网后，需通过DNS请求与远程控制服务器通讯，获取攻击指令或传递窃取的信息。
- 可通过发现异常DNS请求，即可找出内部异常计算机及恶意程序。

基础准备：数据准备

- 为实现多中心多活的应用灵活部署，我行实施了DNS服务器集中工程。
- 10台DNS服务器，每日约5亿条请求，100G日志
- 没有恶意样本，只能另辟蹊径

收集数据，构建机器学习预测模型

恶意网址集

4540个

历史积累恶意网址

100万

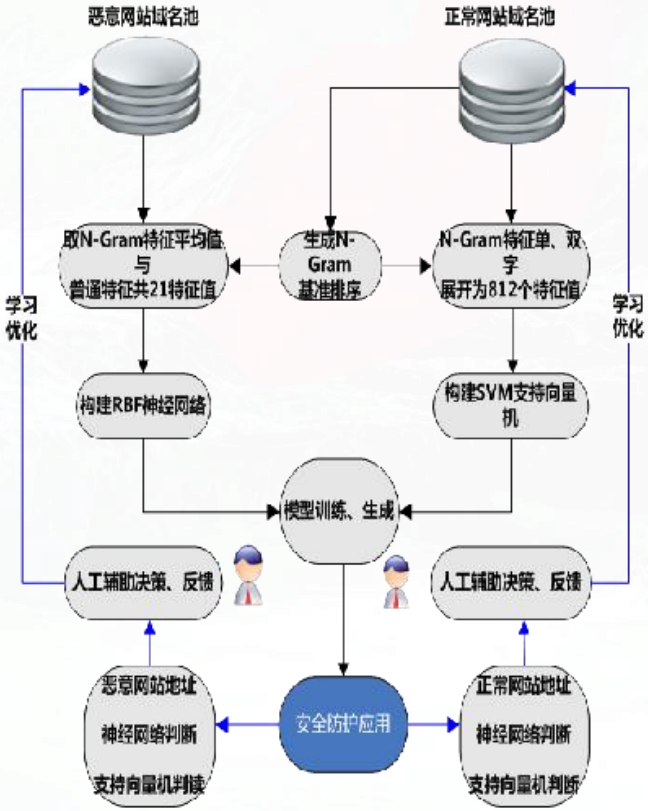
威胁情报厂商提供

恶意程序源代码生成

正常网址集

100万

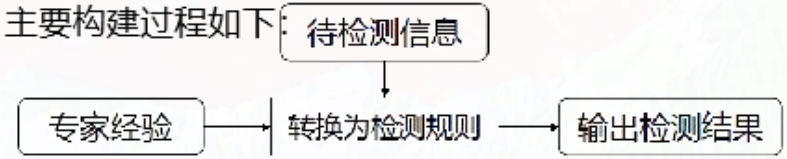
世界访问量前100万



基础准备：模型构建

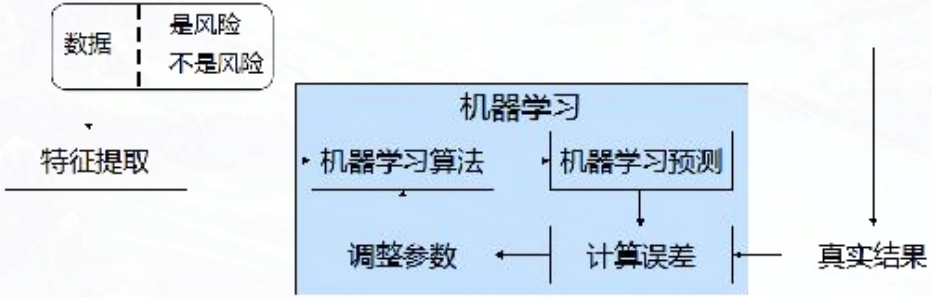
➢基于规则的安全模型构建过程

基于规则的安全模型是SOC平台上的主流模型。此类模型实质上是信息安全专家经验的直接转化，目前SQL注入检测模型，参数污染监测模型，均属于此类模型。主要构建过程如下：



➢基于机器学习的安全模型构建过程

机器学习可分为有监督学习、无监督学习、强化学习三类，业界使用较为广泛且有较为显著效果的为有监督机器学习。目前，SOC上提交和实现的基于机器学习的安全模型：DNS恶意域名检测模型等，均为有监督学习。主要构建过程如下：



■构建模型—支持向量机　映射高维空间，解决低维空间线性不可分，提升预测精度

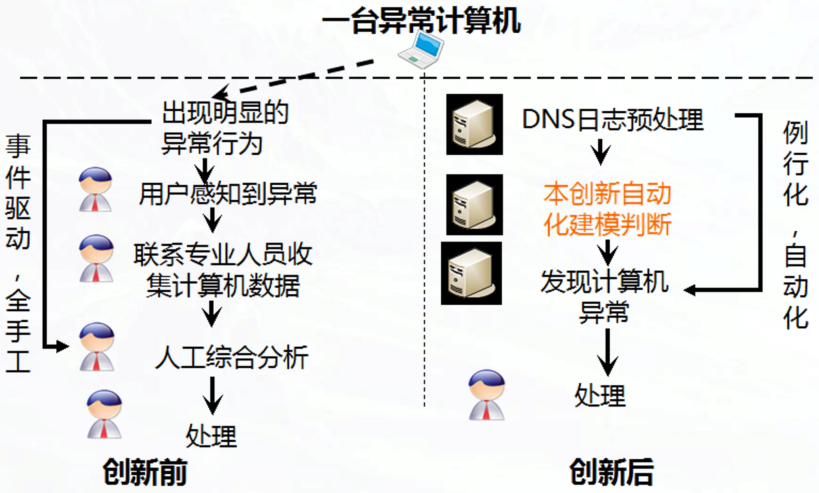
■构建模型—神经网络　模拟人脑，构建人工神经网络，迭代调节，实现分类

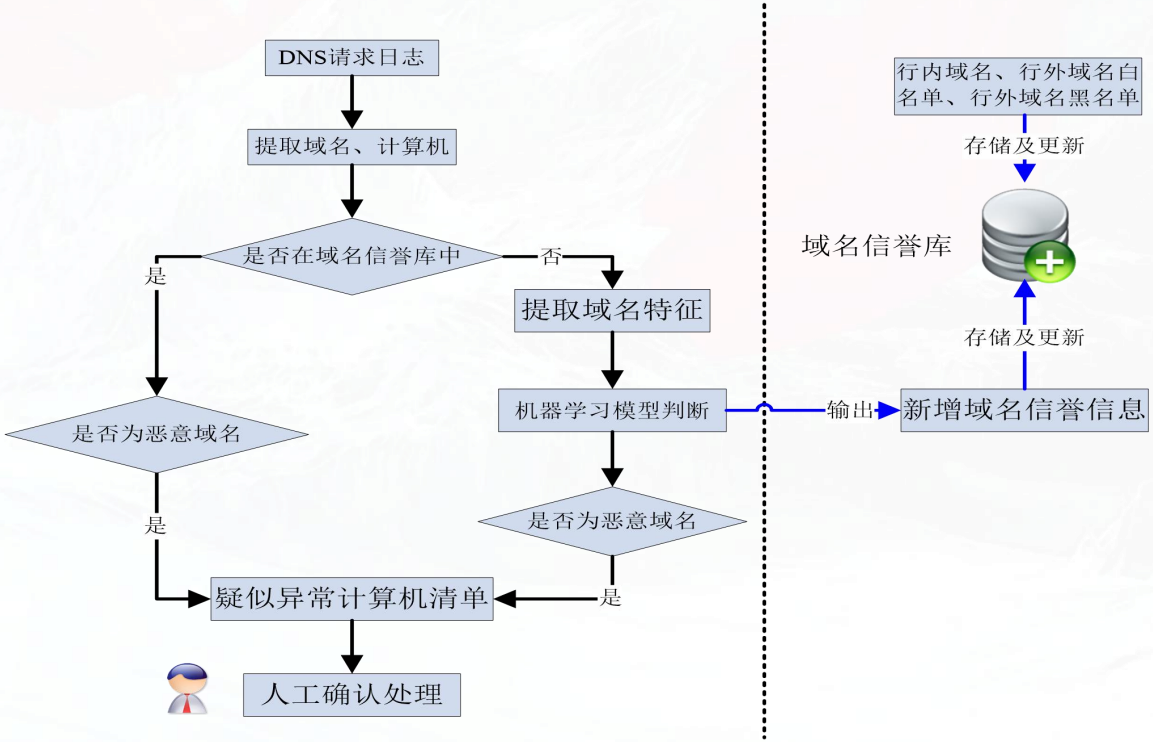
实现流程

域名	域名信誉	备注
google.com	行外域名白名单	谷歌搜索
baidu.com	行外域名白名单	百度搜索
sina.com	行外域名白名单	新浪
16p2hjyn2r4ln1urcw9d1k29qoq.net	黑名单	远控
bekvzpjprsrgnvxpjdefilvdqrs.biz	黑名单	远控
bepbaxdmaeozswpzcaby.com	黑名单	远控
ahmgqytwcdelzwgpzbmlkrusgefa.biz	黑名单	远控

正常网站网址

恶意网址





实现效果

网址	性质
www.amazon.com	亚马逊
www.alibaba.com	阿里巴巴
www.google.com	谷歌
www.fryjfdhtyrs.biz	恶意网址
www.uepxlrj.com.ai	恶意网址
www.lnhqzqevs.com.do	恶意网址

- 模拟人脑鉴别恶意网址的思维方式，将人类思维量化为计算机语言
- 从信息量、可读性、可记性、统计规律四方面，设计了21个特征向量

■特征一：Shannon熵

➢比较fryjfdhtyrs.biz、libaba.com

➢恶意域名更加随机，应描述其随机性

➢随机的无意义的字符，其信息量少

➢选取Shannon熵表达域名所包含信息量，衡量网址随机性。

$$H = -\sum_{x \epsilon U} P(x) \log P(x)$$

■特征二：元音比重

➢比较amazon、alibaba、google

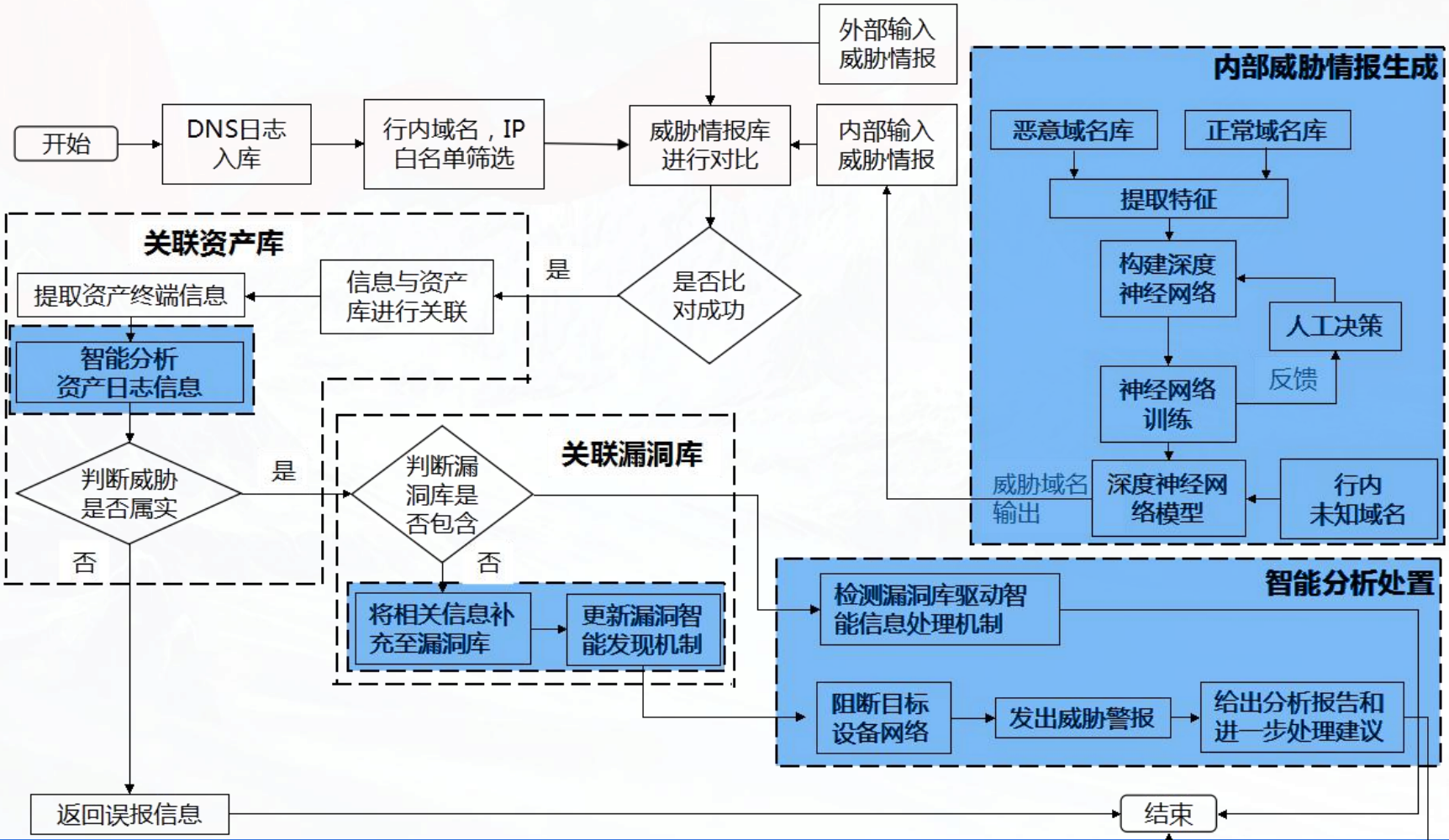
➢上述网址都含有元音字母

➢元音字母，是语言里起发声作用的字母

➢发音不受发音器官阻碍，容易发声

➢元音字母比重可考察网址是否好读

机器学习在安全运营中的应用



威胁框架：细粒度对抗

03 总结与展望

不算总结的总结

- 这些工具的产生都**有鲜明的时间背景**，在大数据概念还没有兴起时，我们事实上已经在应用一些理念来做安全运维工具的创新。
- 这些工具的产生都**有典型的技术局限**，比如因为我们没有办法获取大量的恶意程序样本，又没有办法在小样本量的模型训练中取得好的效果，因此才去分析DNS日志；因为没有快速的应对钓鱼网站的处置方法，才想起去干扰数据。
- 这些工具的产生都**有应用局限**，可能换一个单位，换一个场景就完全无效。

- 但恰恰是这些很有局限的工具，是我们自己在**实践中摸索出来、总结出来、创新出来的**；给我们自己的安全运营工作带来了非常显著的提升效果。当然我们的工具还不仅仅是这些，比如针对终端非法连接互联网，我们研制了内外网互联检测工具；针对病毒传播快，我们研制了有病毒自动断网卡的小工具等等。
- 工具可以不断的改进，唯一不变的就是**从实践中来，到实践中去。于细节处见精神！**

一点心得

- 更高站位，信息安全是国家战略。
- 底线思维，安全合规事件0容忍。
- 广泛参与，信息安全需要每一个人的参与。
- 自主可控，“自主”才是“可控”的前提。
- 对抗本质，能力对抗的基调不变，能力提升的空间延伸，直面安全能力的求索。
- 平衡能力，管理者应在可用性和安全性之间达成一种可接受的平衡。
- 技术思维，安全虽说是技术和管理结合的学科，但很多时候导致隐患的根本原因还是技术管控不过硬。
- 持续改进，要相信当前安全工作的已有成绩，但更要坚持不断提升和改进安全工作。

工银科技公司介绍

工银科技有限公司（以下简称“工银科技”）是中国工商银行股份有限公司控股的全资子公司， 注册资本6亿元人民币，总部位于河北雄安新区，于2019年5月8日挂牌开业，在北京、雄安两地办公。

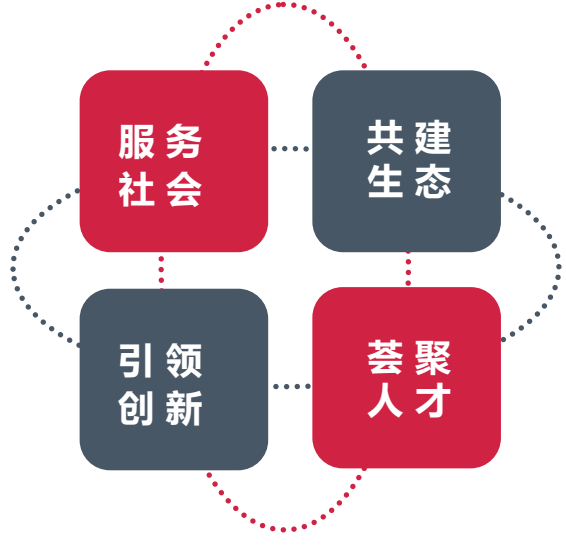
工银科技是工商银行“一部、三中心、一公司、一研究院”总行金融科技布局的重要组成部分，

工银科技有限公司坚持“服务社会、共建生态、引领创新、荟聚人才”的经营理念，

对内赋能集团智慧银行战略，成为金融科技创新领跑的孵化器与助推器，

对外赋能行业客户业务创新，成为“金融+行业”生态建设的 新动能与新范式 。

工银科技依托工商银行35年的科技积累，高效协同的金融科技体系，1万5千人的高素质、复合型金融科技人才队伍，积极为客户提供卓越服务。公司目前开展的服务客户包括政府、大型企业、大中小金融机构等近100家。



工银科技公司目标

打造“四型”公司

服务支持型

发挥市场化运作优势，为工行智慧银行建设及同业提供技术能力，推动业务模式变革和服务升级；

创新领跑型

发挥公司化机制体制优势，通过人才引进、技术控股、联合共建等方式，深耕金融科技领域，提升科技创新能力；

生态建设型

用云计算、大数据、区块链等实验室创新成果以及业界新技术，借助API开放平台和金融生态云，构建金融生态建设新模式；

能力输出型

面向金融同业提供研发、托管服务以及优势科技产品和服务。

工银科技服务理念与价值创造

工银科技坚持“以客户为中心，提供安全、领先的科技产品与服务，为用户创造价值”的核心理念。让工商银行的科技优势、资源优势充分服务社会、服务广大客户。

坚持开放合作共赢的理念，与外部机构开展合作，共建生态，在发挥自身优势基础上，与合作方共同开拓“金融+”新蓝海。致力于与合作伙伴一起构建开放、合作、共赢的金融科技生态圈。

工银科技公司业务范围

1 重点客户IT系统研发

通过自主研发、合作共建等多种方式，拓展金融服务场景，为政府客户、行业客户等提供“行业+科技金融” 一揽子解决方案。

2 科技产品输出

向金融同业、行业客户输出集团成熟的业务系统及产品化技术创新平台，提升科技价值创造力。

3 系统运营与托管

为集团重点客户提供机房、网络等IT基础设施以及业务系统的托管和运维支持等服务；面向集团及第三方的SaaS服务建设者提供运营支持服务，着力构建“开放、合作、共赢”的金融生态圈。

4 技术创新与孵化

针对新技术研究与实践开展高效的联合创新和技术孵化，为集团智慧银行建设及行业服务升级转型引入核心技术和高端人才。

5 股权投资

试点股权投资，为工行新技术创新和高端人才引入形成战略协同

谢谢大家