数据驱动的智能移动安全防护体系

程智力 CISSP CISA

目录

CONTENT

网络安全的顶层对抗

国家层面互相挟制推动网络信息安全持续高速发展

美国—

《网络安全法》2015

《国土安全法》2015

NIST-《提升美国关键基础设施网络安全的框架》2018

网络威胁指标评估
防御性具体措施
隐私数据保护

欧盟—

NISD-《网络与信息系统安全指令》2016

GDPR-《一般数据保护条例》2018.5

中国—

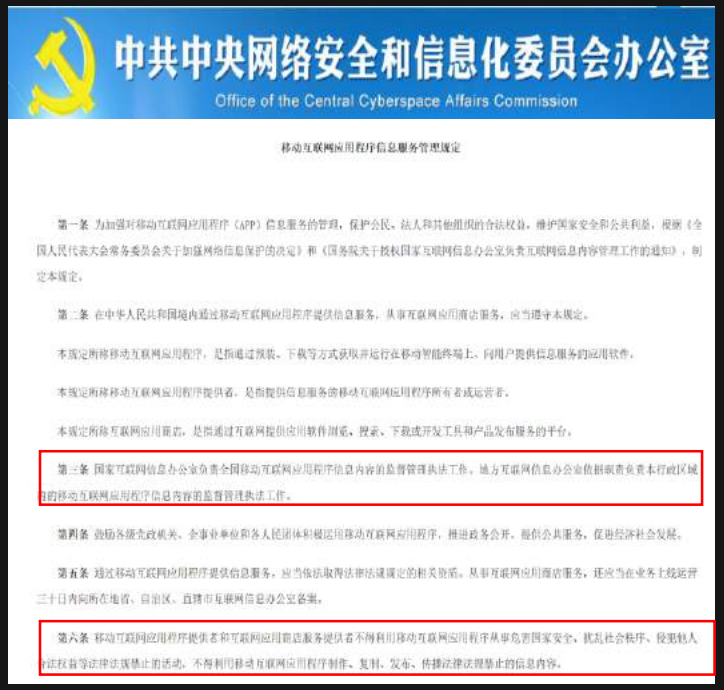
《网络安全法》2016

《等保2.0》-2018.7待定

《个人信息和重要数据出境安全评估办法》2017

网络运行安全
网络信息安全
评估、检测、预警与应急

监管单位的高度重视与保护条例



中共中央网络安全和信息化委员会办公室
Office of the Central Cyberspace Affairs Commission

移动互联网应用程序信息服务管理规定

第一条 为加强对移动互联网应用程序（APP）信息服务的管理，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》和《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内通过移动互联网应用程序提供信息服务，从事互联网应用商店服务，应当遵守本规定。

本规定所称移动互联网应用程序，是指通过预装、下载等方式获取并运行在移动智能终端上、向用户提供信息服务的应用软件。

本规定所称移动互联网应用程序提供者，是指提供信息服务的移动互联网应用程序所有者或运营者。

本规定所称互联网应用商店，是指通过互联网提供应用软件浏览、搜索、下载或开发工具和产品发布服务的平台。

第三条 国家互联网信息办公室负责全国移动互联网应用程序信息内容的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内的移动互联网应用程序信息内容的监督管理执法工作。

第四条 鼓励各级党政机关、企事业单位和各人民团体积极运用移动互联网应用程序，推进政务公开、提供公共服务，促进经济社会发展。

第五条 通过移动互联网应用程序提供信息服务，应当依法取得法律法规规定的相关资质。从事互联网应用商店服务，还应当在业务上线运营三十日内向所在地省、自治区、直辖市互联网信息办公室备案。

第六条 移动互联网应用程序提供者和互联网应用商店服务提供者不得利用移动互联网应用程序从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律法规禁止的活动，不得利用移动互联网应用程序制作、复制、发布、传播法律法规禁止的信息内容。

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部关于印发《公共互联网网络安全威胁监测与处置办法》的通知

各省、自治区、直辖市通信管理局，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司，国家计算机网络应急技术处理协调中心、中国信息通信研究院、国家工业信息安全发展研究中心、中国互联网协会、域名注册管理和服务机构、互联网企业、网络安全企业：

为深入贯彻习近平总书记关于网络安全的重要讲话精神，积极应对严峻复杂的网络安全形势，进一步健全公共互联网网络安全威胁监测与处置机制，维护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》等有关法律法规，制定《公共互联网网络安全威胁监测与处置办法》。现印发给你们，请结合实际，切实抓好贯彻落实。

工业和信息化部
2017年8月9日

第二条本办法所称公共互联网网络安全威胁是指公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件，包括：

（一）被用于实施网络攻击的恶意IP地址、恶意域名、恶意URL、恶意电子信息，包括木马和僵尸网络控制端，钓鱼网站，钓鱼电子邮件、短信/彩信、即时通信等；

（二）被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序等；

（三）网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等；

（四）网络服务和产品已被非法入侵、非法控制的网络安全事件，包括主机受控、数据泄露、网页篡改等；

（五）其他威胁网络安全或存在安全隐患的情形。

《网络安全等级保护条例（征求意见稿）》18年6月份

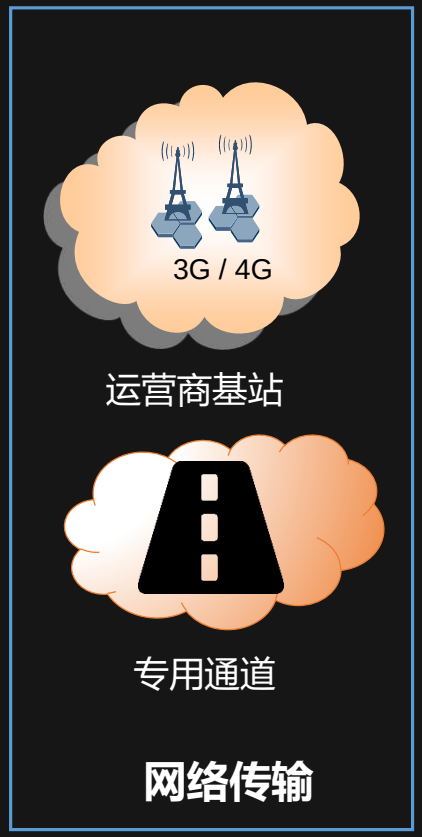
“事前”检测	“事中”监督	“事后”检查
上线检测（第二十二条）新建的第二级网络上线运行前应当按照网络安全等级保护有关标准规范对网络的安全性进行测试。	安全监督管理（四十九条）对第三级以上网络运营者按照网络安全等级保护制度落实网络基础设施安全、网络运行安全和数据安全保护责任义务，实行重点监督管理。	第二十条【一般安全保护义务】（五）落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，并按照规定留存六个月以上可追溯网络违法犯罪的相关网络日志；

关键基础行业

移动互联 | 云计算 | 大数据 | 人工智能 | 区块链 | 物联网 | 车联网

新兴科技应用

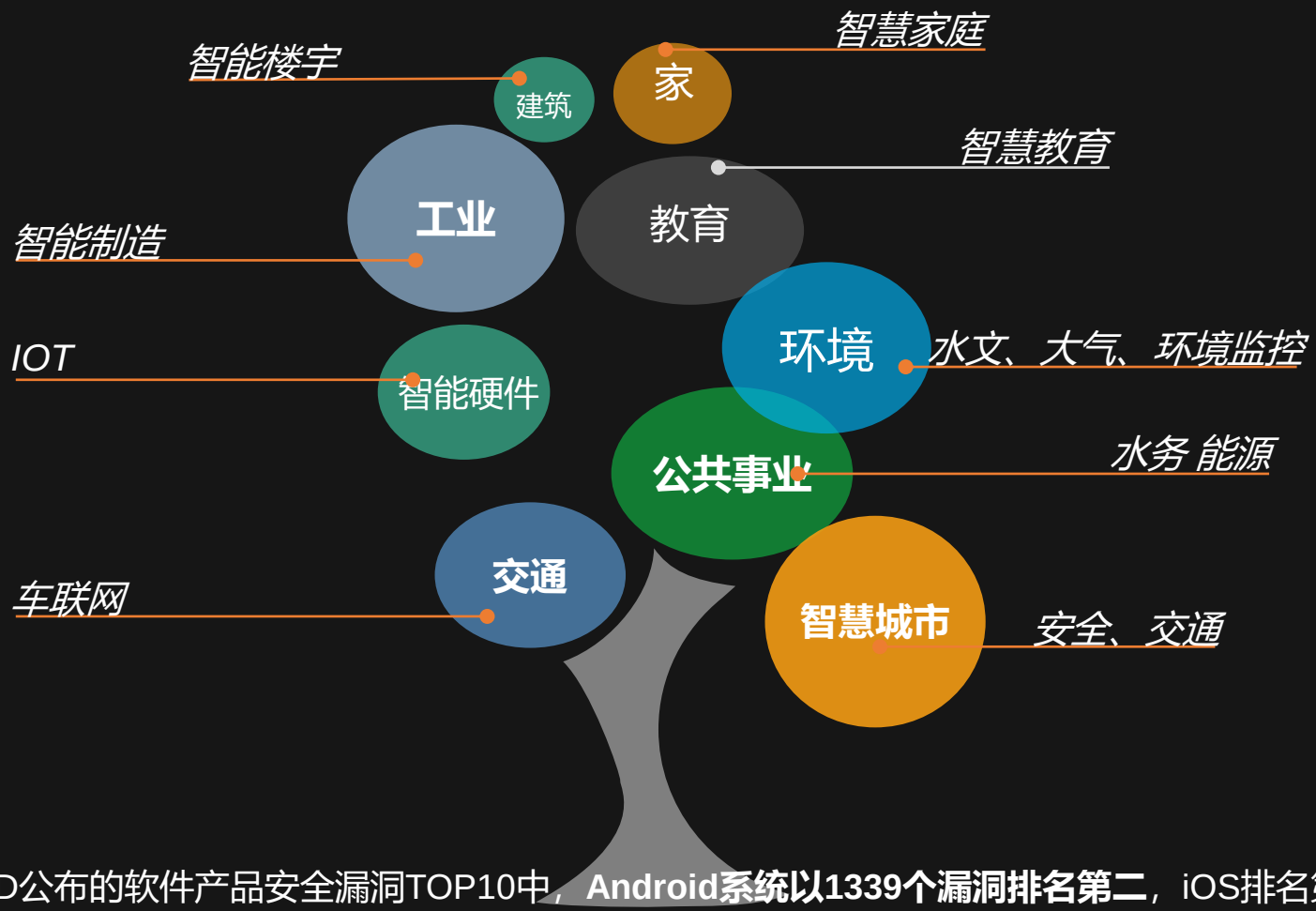
移动安全和传统安全的本质区别



新兴安全防护
应用的不同形态、多类型的智能设备、这些资产默认是不可信，且非受控

传统安全防护
自己的服务器、自己的资产，边界清晰、易于防护、易于管理

应用场景爆发式增长带来系统性安全隐患



应用数量成倍增加
成为业务安全最重要一环

CNNVD公布的软件产品安全漏洞TOP10中，**Android系统以1339个漏洞排名第二**，iOS排名第8，已公布654个漏洞。基于移动终端系统的漏洞利用，恶意软件行为、交易劫持、信息泄露、业务欺诈等一系列安全事件层出不穷，造成大量用户隐私泄露、企业经济利益受损，对企业及社会均造成了难以估量的影响，同时也给国家信息安全带来了重大安全隐患。

AI时代下的数字化企业的风险边界

来自安全的风险

- 物联网风险
- 病毒木马
- 劫持攻击
- 注入攻击
- 调试攻击
- 框架攻击
- 网络攻击
- 云安全风险
- 其他攻击

来自业务场景的风险

- 交易欺诈
- 虚假营销
- 刷单刷量
- 其他场景

来自自身的风险

- 性能下降
- 响应迟缓
- 功耗增加
- 程序崩溃
- 其他缺陷
- 体验缺失

来自运营场景的风险

- 转化率下降
- 留存率下降
- 无效推广
- 运营策略缺失
- 其他场景

移动业务安全的未知威胁

对于监管机构和企业而言，数据是有限的，面对有限的已知风险，如安全风险，业务风险，运营风险，可以通过现有的经验进行分析与对抗。但是现代科技创新的核心在于未知的应用场景，而未知场景衍生未知风险。决定现在科技创新安全发展成败的关键在于如何建立面对不可预测的未知风险的能力。

目录

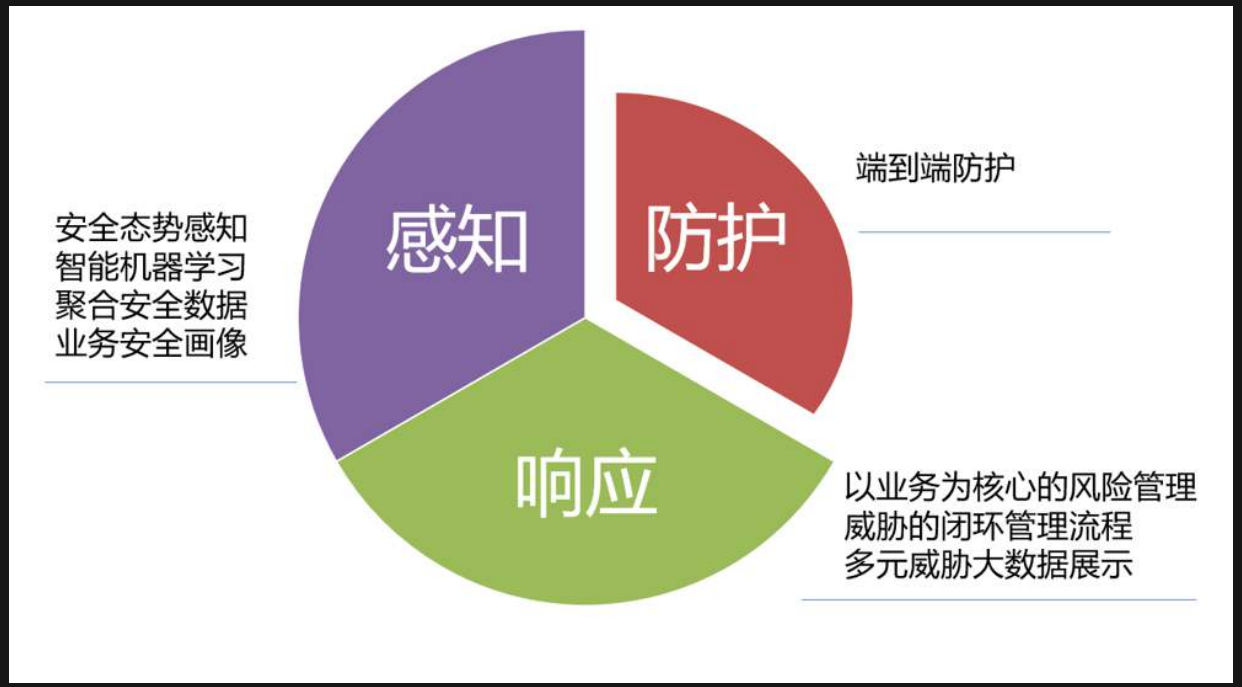
CONTENT

智能防护环境建设基础

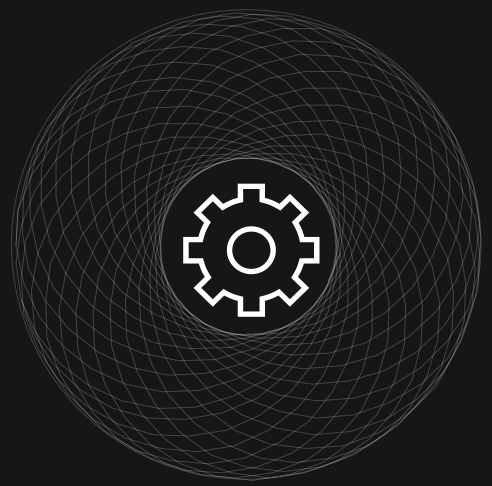
技术平台

云计算　大数据　人工智能　移动互联网　物联网　区块链　边缘计算

以感知响应为核心的理论设计



全范围的安全数据支撑

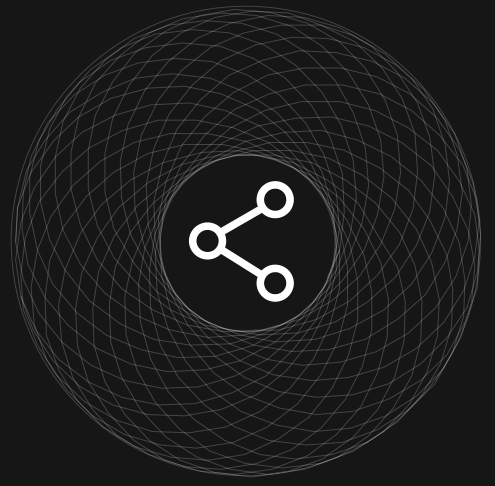


企业侧安全数据

指企业内部APP业务正常运行的备案数据、安全数据，威胁数据等信息。

用户侧安全数据

客户端运行的APP提供的日志、恶意行等信息，包括采集到的安全运行环境信息。



互联网侧安全数据

第三方市场或政务网站等提供的可采集数据，以及从合作伙伴处获取的相关数据。

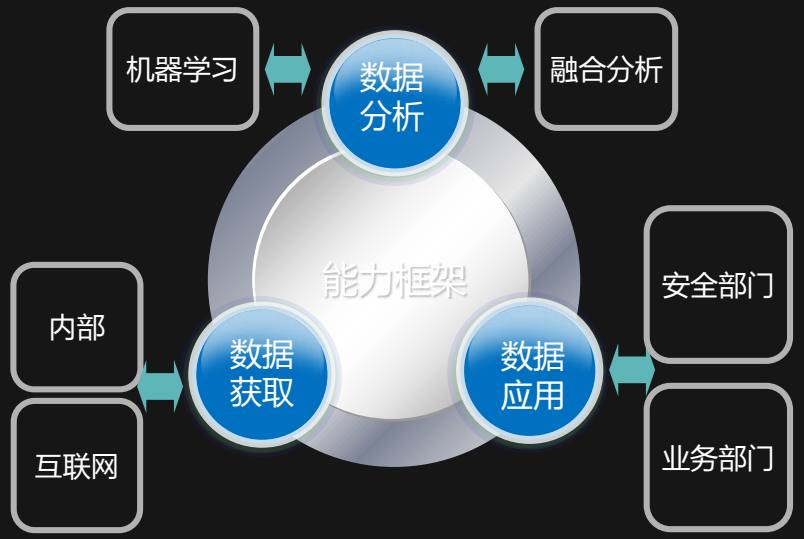
场景化智能化数据分析能力

场景模型构建能力

模型数据
提供场景分析项目使用

- 木马劫持交易
- 模拟器自动化工具
- 短信劫持与设备迁移
- ……

非结构化数据分析能力



内外部数据融合分析能力

政策、标准、情报…

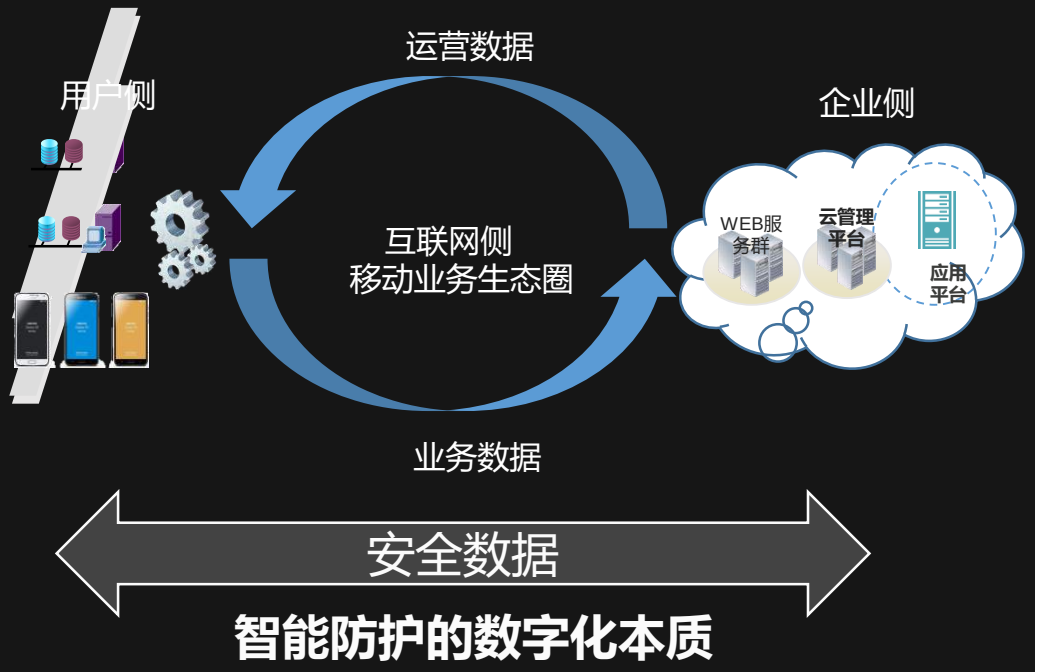
内部数据源

结构化、非结构化

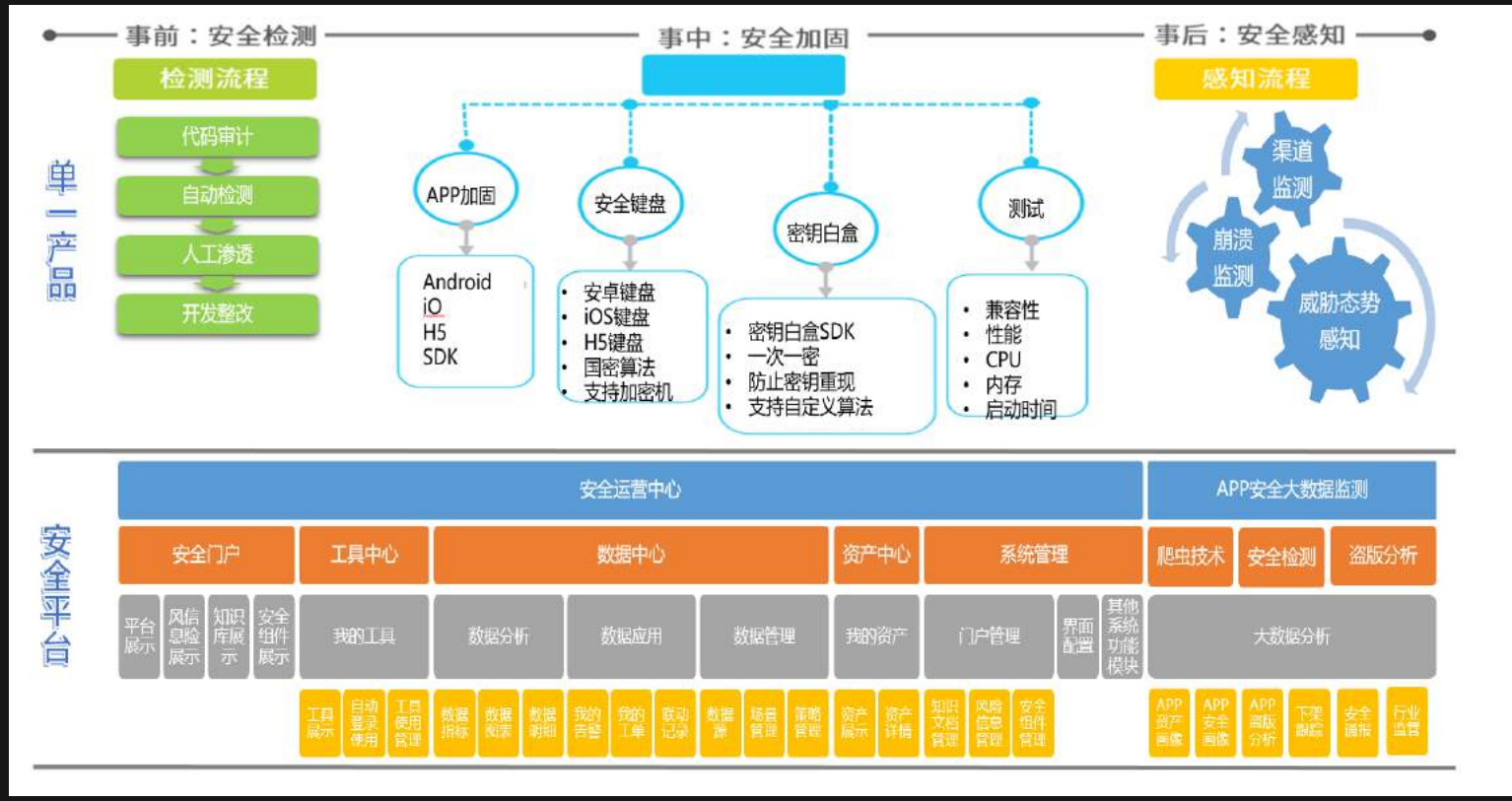
目录

CONTENT

企业侧移动应用智能防护平台



智能防护的数字化本质

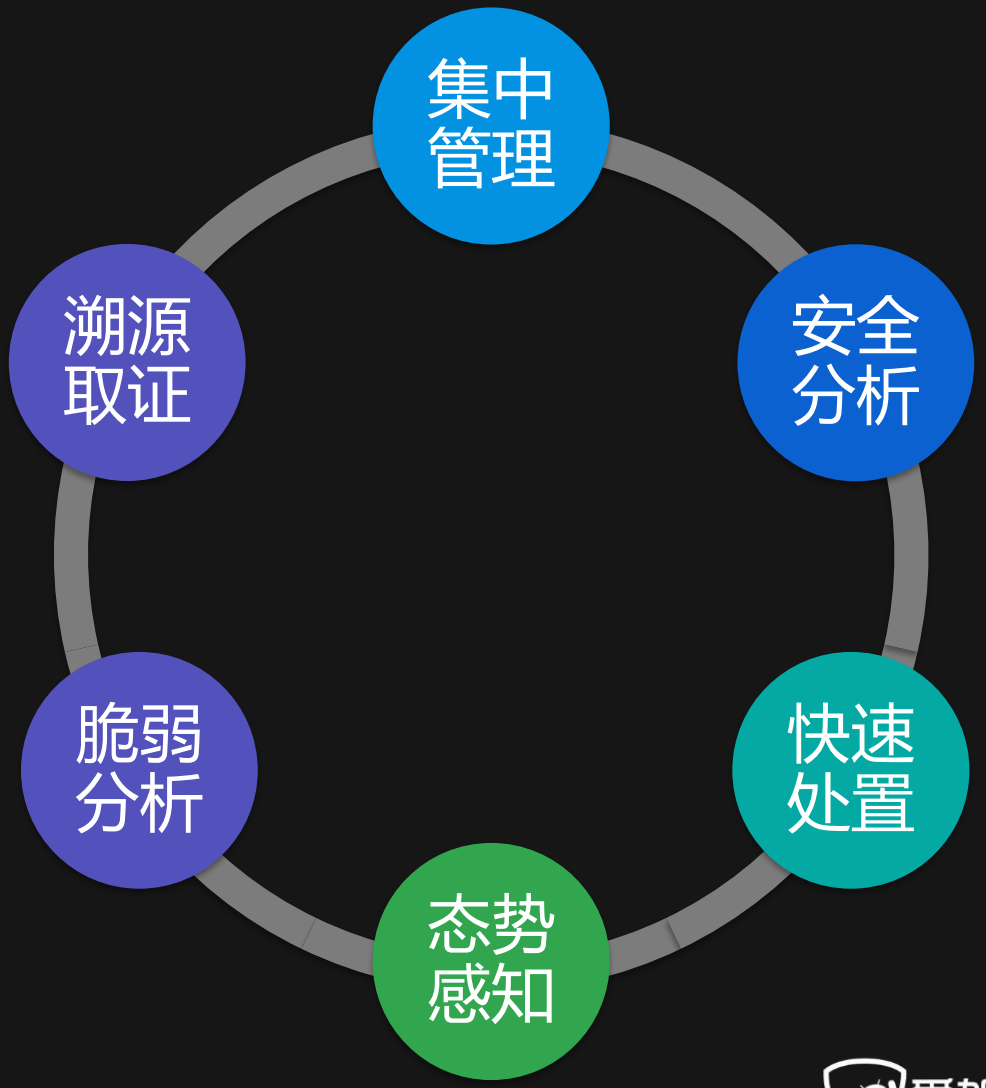


用户侧移动应用智能防护

通过探针准确识别终端威胁和业务异常行为

快速响应与终端动态防御，降低威胁发现和响应时间

安全事件日志审计与溯源取证



威胁态势感知-已知威胁

已知威胁分析能力

业务分析：
针对常见业务威胁如交易欺诈，刷单抢单，位置欺诈等场景建立威胁样本库，当威胁发生时快速匹配决策，无需人工干预，高效反馈给企业推动决策与应用。

安全分析：
针对常见应用威胁攻击场景利用业界成熟的安全检测体系进行特征分析，当威胁发生时直接进行防御应用。

运营分析：
针对常见运营痛点进行分析，通过对运营场景下的多种数据与威胁事件进行匹配关联分析出当前运营中的问题，提供有力的决策支持。

威胁态势感知-未知威胁

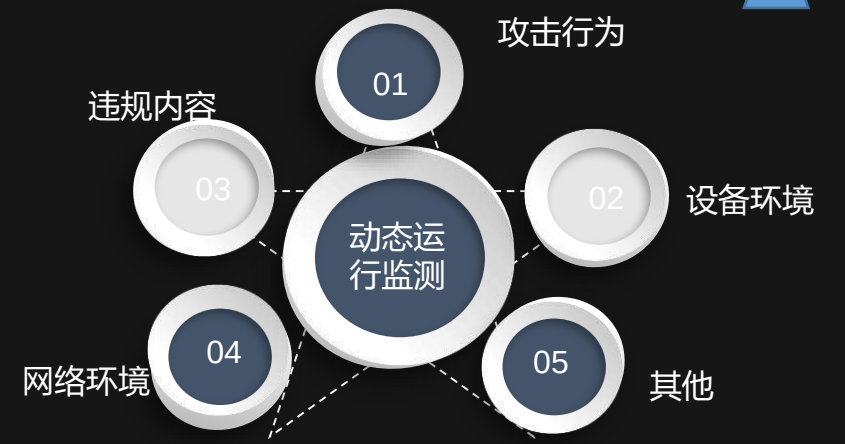
针对不可预测的未知威胁场景，感知体系**通过无监督聚类算法，将海量数据元分类，挖掘出数据之间的关联性，通过人工干预标签化并训练入库，从而预测出可能出现的未知威胁，**随着企业数据的不断积累与业务的壮大，威胁感知体系自身会随着企业业务体系的壮大一起成长，不断探索出更多未知威胁服务于企业本身。

互联网侧移动应用智能监管

多维统计
多维资产画像

态势预测
安全趋势画像

安全告警
及时安全通报



渠道 | 地区 | 行业

应用类别

新闻信息
社交网络
网络直播
加密代理
即时通讯
网咯交易
网络支付
网络金融

行业类别

公共交通
信息服务
电子政务
能源制造
金融证券
……

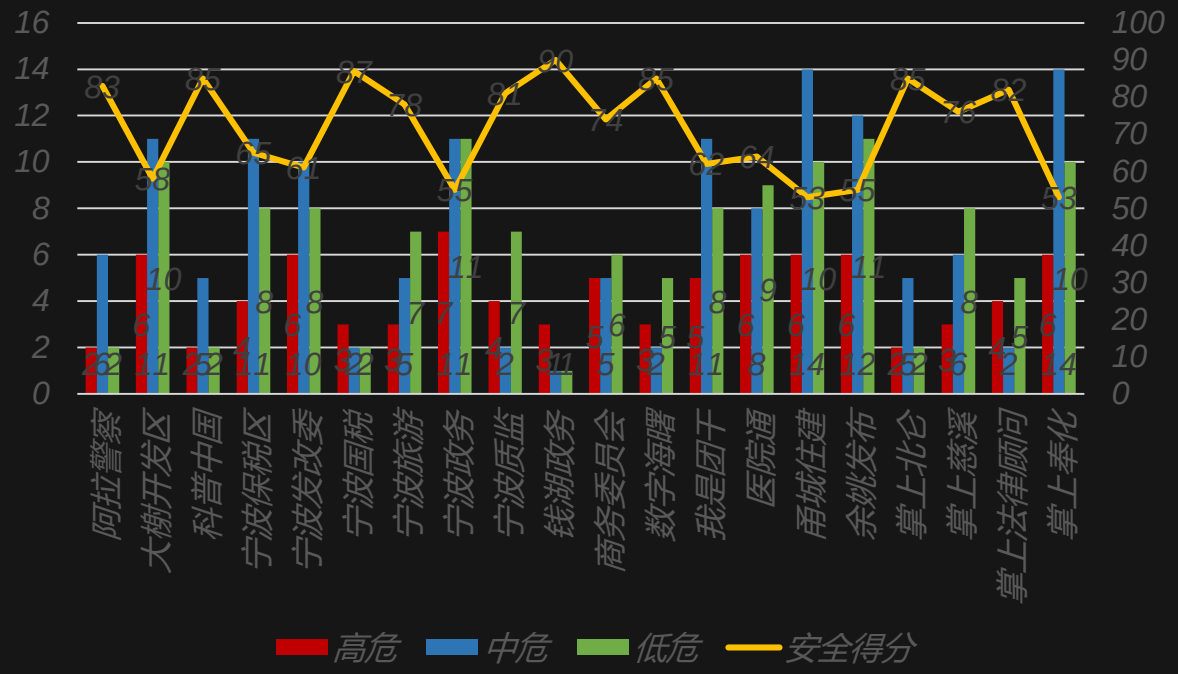
渠道类别

第三方应用市场
手机市场
网站
……

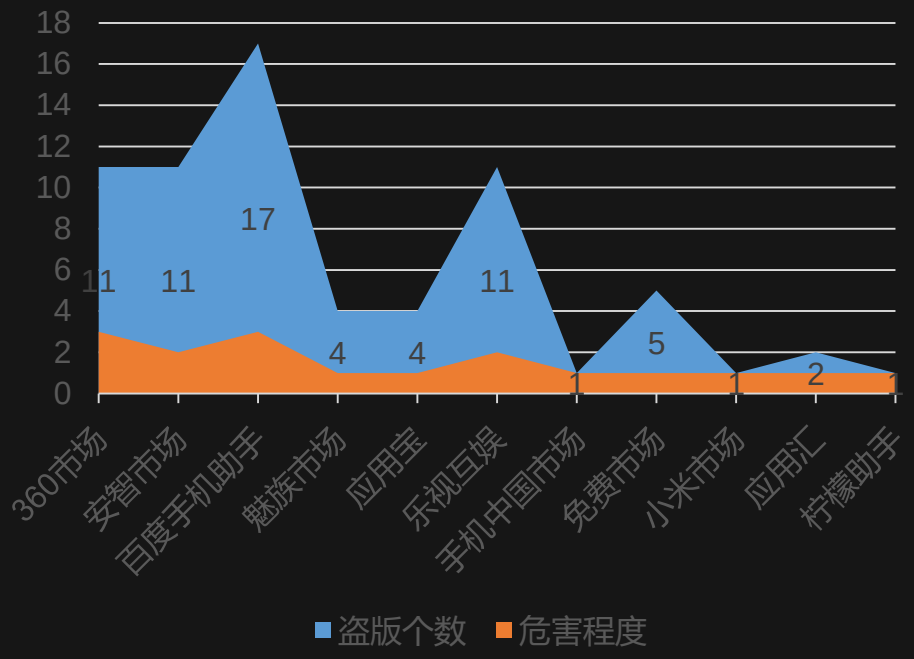
业务APP5 | 业务APP4 | 业务APP3 | 业务APP2 | 业务APP1

多维度互联网安全监督管理

XX行业XX类APP安全状况分析统计



盗版应用渠道分布图

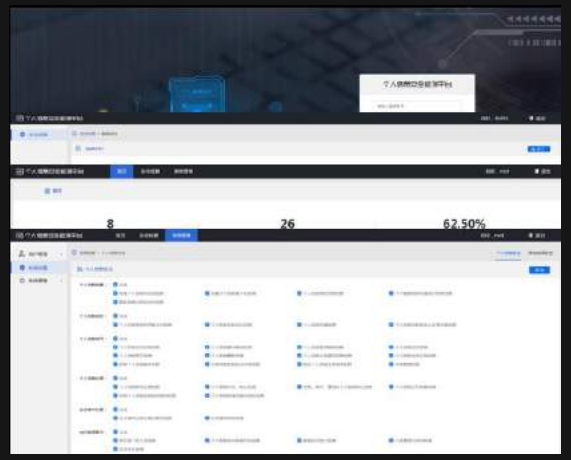


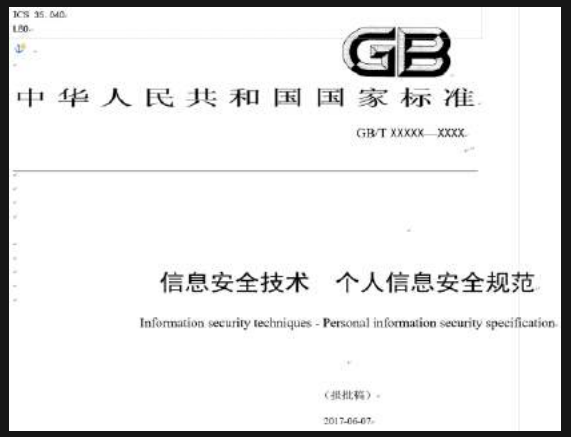
安全检测能力

Android、iOS、H5、SDK安全检测

- 源码风险漏洞
- 恶意程序漏洞
- 调试风险漏洞
- 通用组件漏洞
- 数据风险漏洞
- 业务风险漏洞
- 。。。

个人信息、权限合规检测





移动应用内容违规检测

基于海量数据的深度学习，检测图像中的中关键主体位置，通过图片特征类比进行智能检测

基于敏感词与反垃圾特征库进行内容比对，极速智能分析垃圾信息、涉政、违禁内容

- 广告检测，应用程序中出现包含宣传、推广为目的给第三方导流的内容会被检测识别。
- 违禁检测，应用程序中出现包含国家法律法规限制的物品信息会被检测识别。
- 智能鉴黄，应用程序中出现含有色情内容的文字、图片将会被检测识别。
- 涉政检测，应用程序中出现包含法律法规相违背的涉政敏感等不良信息，涉及宗教、文化或种族群体的引用或评论包含诽谤性、攻击性或狭隘内容的文字、图片会被检测识别。

异常应用安全告警通报流程

通报类型

1. 安全高风险应用
2. 感染恶意程序应用
3. 钓鱼应用监测
4. 动态攻击应用

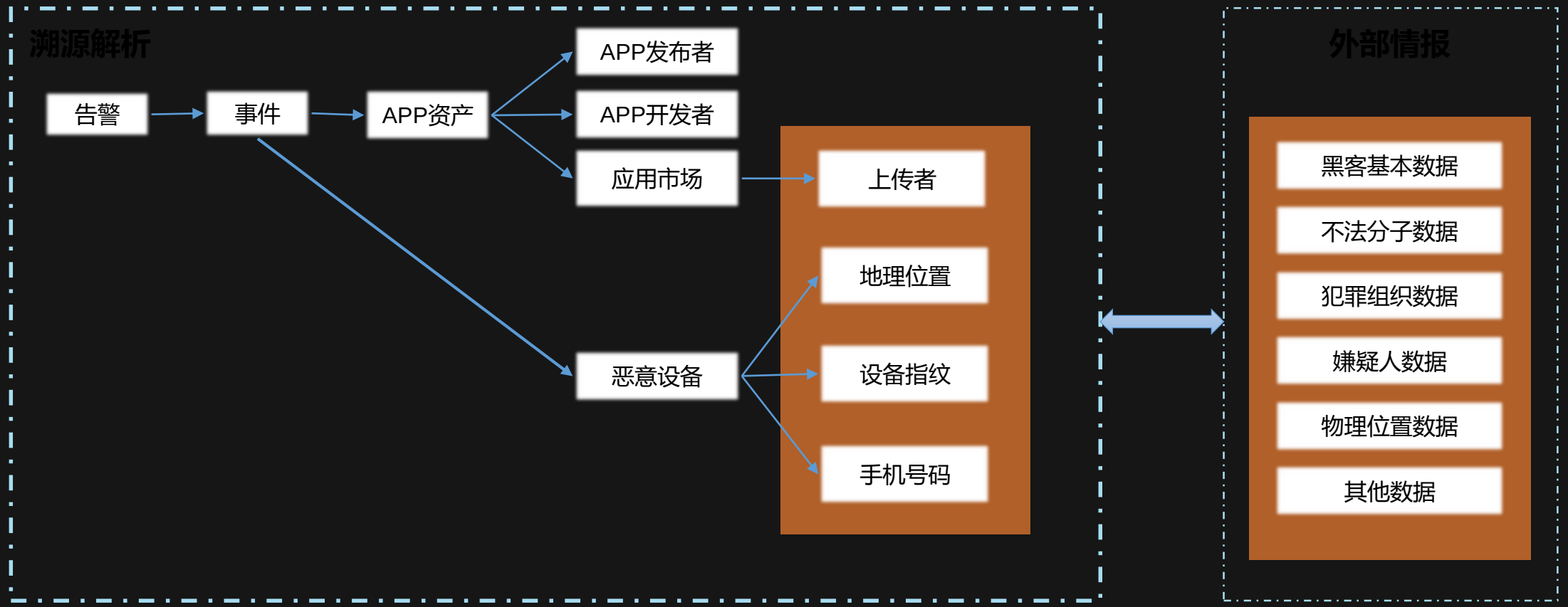
通报对象

- 监管机构
- 涉事组织

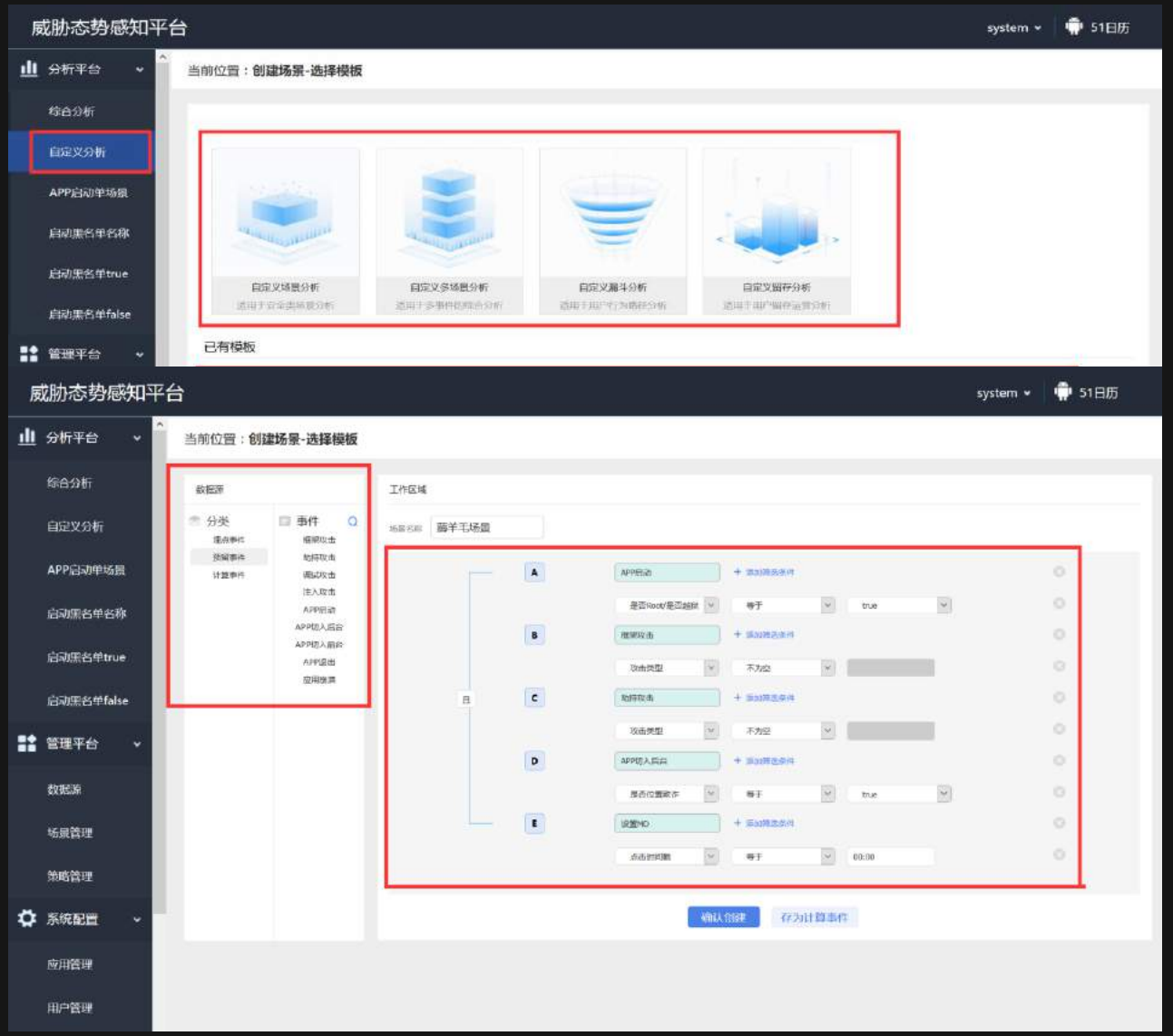
通报事件管理

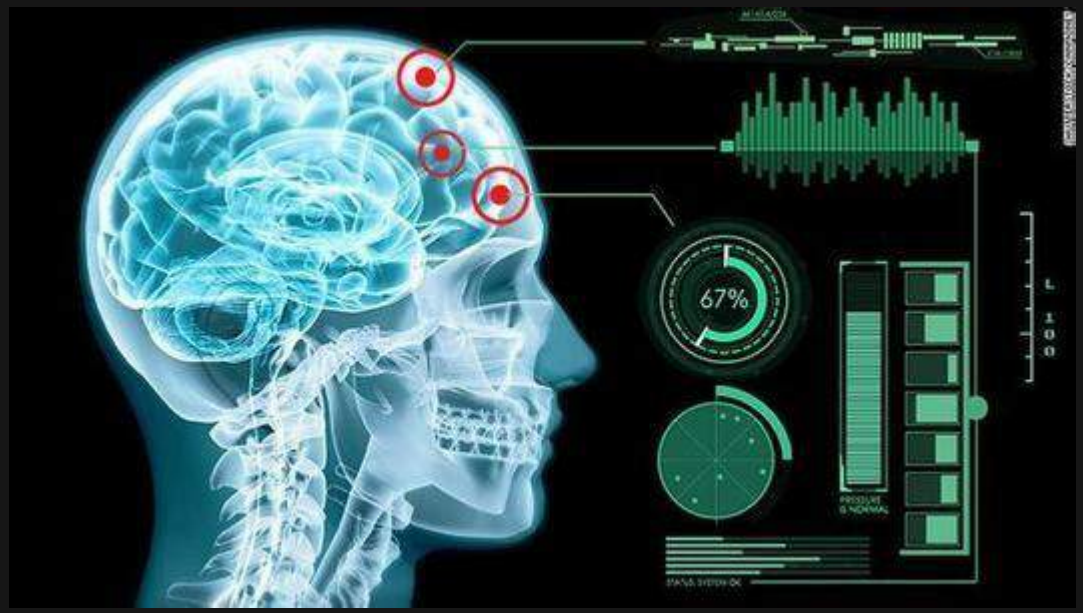
- 事件类型统计
- 事件数量统计
- 涉事组织统计
- 动态趋势

违规应用朔源取证

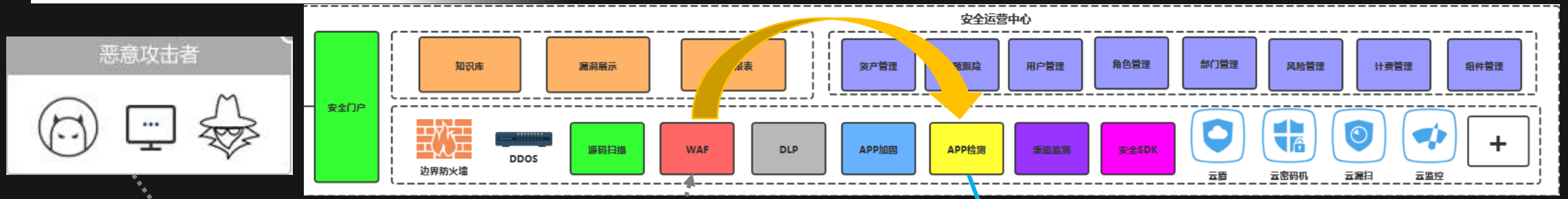


智能化风险威胁场景分析





移动应用智能安全防护管理示意图



全生命周期风险闭环智能管理

“事前”

威胁发现和管理

checklist
应用检测
病毒检测
权限检测
信息采集
…

“事中”

行为检测与阻断

界面劫持感知
Gdbserver调试感知
Ida调试感知
Inject注入检测
Xposed插件和zjdorid
攻击…

消息提示
页面弹窗
终止程序
…

“事后”

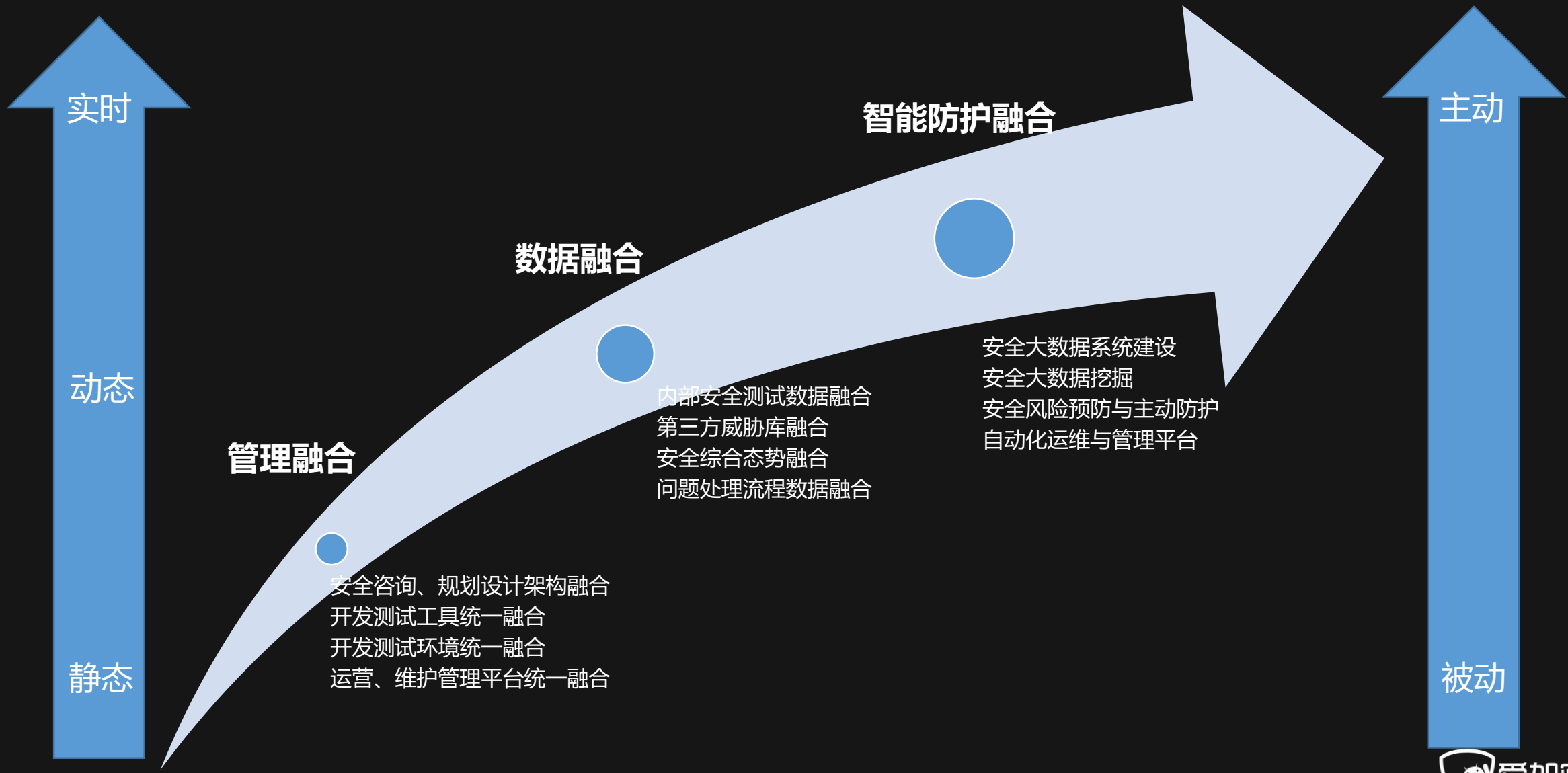
事件报告、分析与整改

破解痕迹确认
溯源与反制策略
日志审计
整改与**加固**
…

安全报表
攻击态势统计
事件分析
…

风险闭环管理

移动安全防护建设规划



目录

CONTENT

公司简介

北京智游网安是国内最大的移动信息安全综合服务提供商，全球移动信息安全领导品牌。公司总部位于北京，在全国十几个城市设立了分公司和办事机构，为金融、政府、运营商、军工、能源、企业等重要行业客户提供基于物联网、大数据、云计算以及移动互联网等全方位的信息安全服务。

- 超过200员工
- 超过一半为技术人员
- 超过2000+标杆行业客户
- 50+公司权威资质认证

- 覆盖Android、iOS、H5及物联网传感器
- 保护100万+APP
- 覆盖9亿+个人智能终端
- 50+产品软著及专利

我们的优势

公司优势

- 垂直领域的技术与市场领先者
- 全面的权威资质认证
- 遍布全国的分公司与办事处
- 所有产品均为自助研发，拥有核心代码及知识产权
- 与网信办、工信部、公安、CnCert、计算机病毒防治中心等深入合作

技术优势

- 领先的双重VMP加固核心技术
- 创新的iOS加固技术
- 纯净防护，不侵入源代码
- 全面的Android、iOS、H5和物联网嵌入式系统覆盖
- 高性能、不影响兼容性
- 众多核心技术及软著、专利

人员优势

- 70%的专业技术人员
- 风险评估相关人员超过40人
- 众多CISSP/CISA/CISP/PMP/CISAW等专业安全资质认证

方案优势

- 移动安全前生命周期解决方案
- 物联网解决方案
- 安全态势感知解决方案
- 安全大数据解决方案
- 业务风险治理解决方案
- 围绕国家网络安全法和等保2.0的方案设计思想

经验优势

- 超过2000+的行业标杆客户
- 专业的服务和响应团队
- 专业的评估服务流程

谢谢欣赏

THANK YOU APPRECIATE