山东省计算中心
SHANDONG COMPUTER SCIENCE CENTER

道普测评
TOP TEST AND EVALUATION

APP安全检测及安全赋能




→ 让信息化更简单更安全

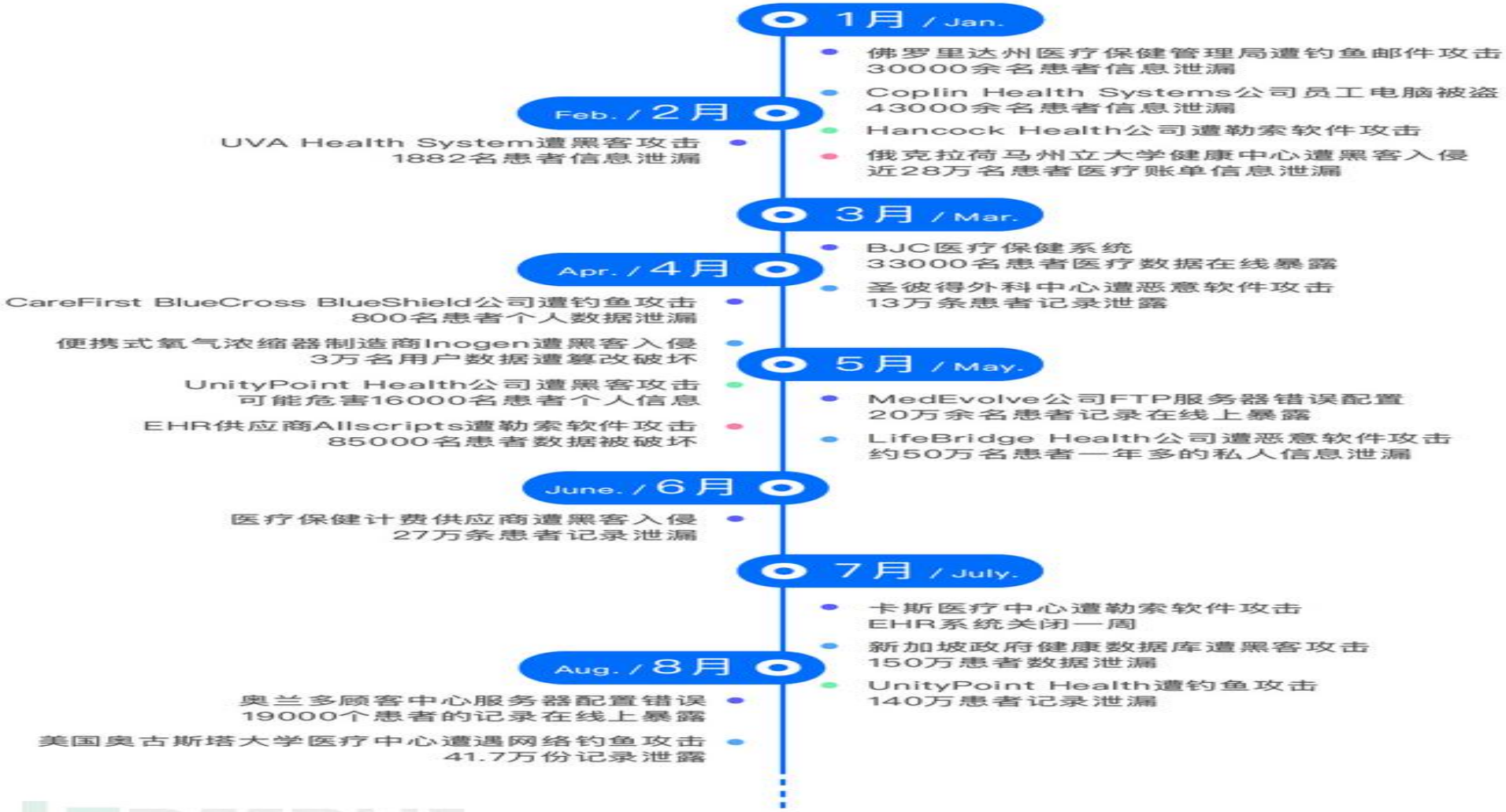
演讲人：韩晓龙

国家保密科技测评中心山东省系统测评实验室副主任
山东省计算中心软件评测中心道普测评副主任
公安部高级等级保护测评师
山东省政府采购评审专家

目录 CONTENTS

医疗行业安全事件

2018国外医疗安全事件



医疗行业安全数据统计

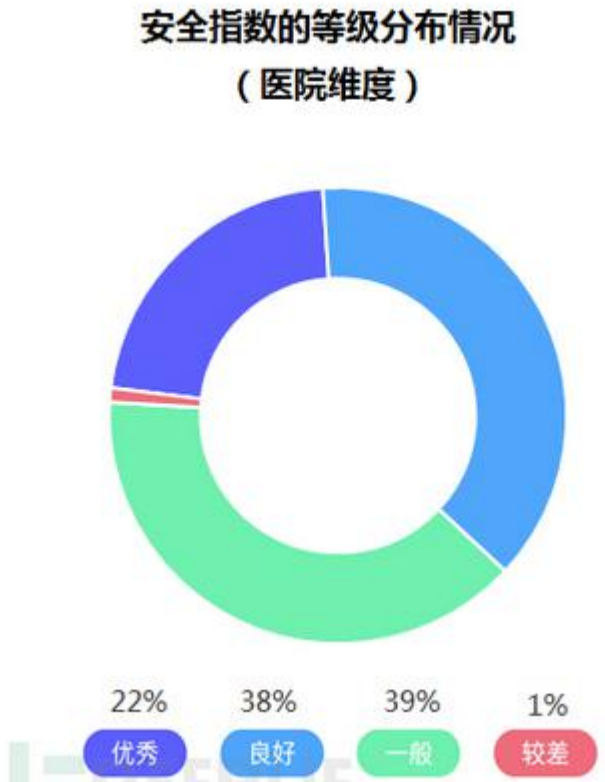


图2-7 医院数据安全措施

医疗行业安全指数报告

医疗行业风险分析

➢ 医疗行业成黑客攻击重要目标

患者预约信息

检查检验信息

就诊信息

医学数据

网络安全面临严峻的威胁

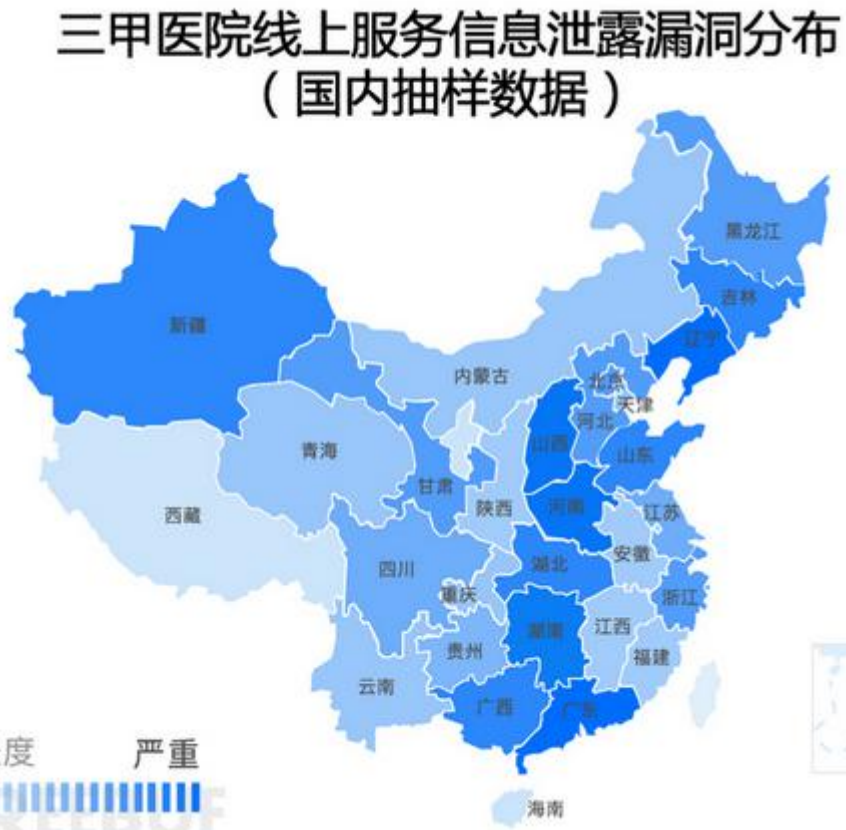
2017年以来，医疗行业已成为攻击者实施勒索的最主要目标，有29%的勒索软件的攻击目标是各类医疗相关机构。勒索、挖矿已经成为影响医疗业务连续性的主要威胁。

医疗行业风险分析

应用安全脆弱性凸显

全国大中型医院中，有87.4%的医院提供线上服务，73%的医院提供线上预约挂号服务，51.7%的医院提供线上缴费服务，56.4%的医院提供线上检验化验报告查询服务。

但线上医疗服务带来了新的漏洞风险和数据泄露风险。



医疗行业风险分析

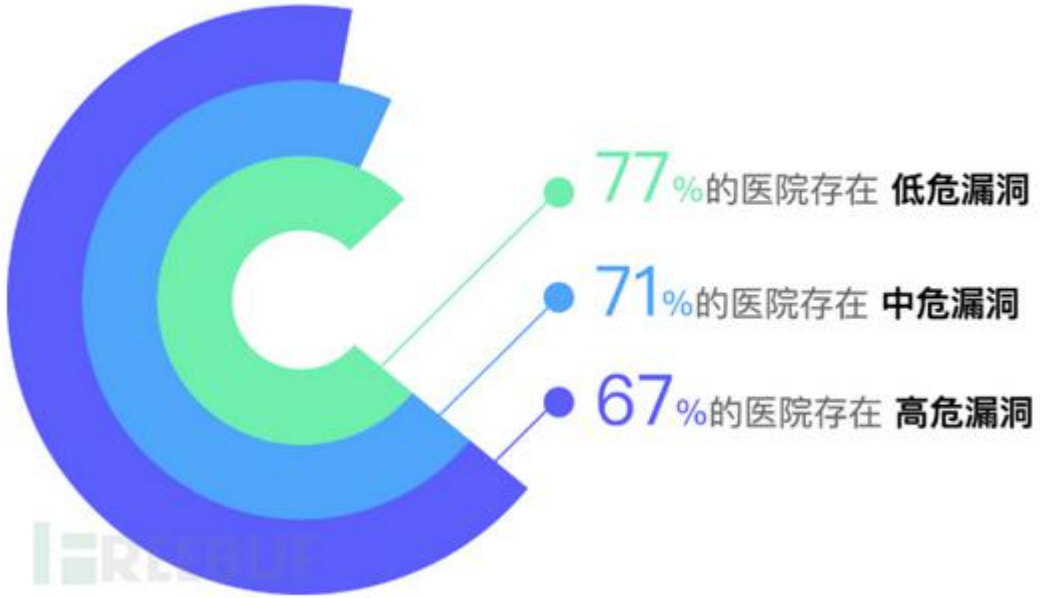
数据泄漏成主要风险

医疗数据泄露事件也呈逐年上升趋势。2015年地下黑市大约有1.1亿条医疗记录需要出售，几乎占据了全美国一半的医疗数据。2017年媒体报道的医疗数据泄露事件就达到350多起。在中国，医疗信息泄露同样不可小觑。

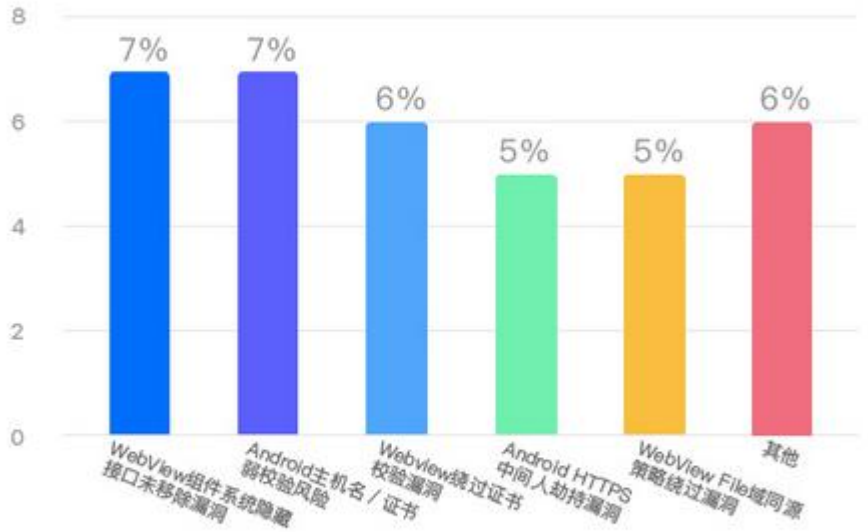
医疗行业风险分析

患者APP存在较多漏洞：对国内患者APP的抽样调查分析，80%左右的患者APP存在漏洞，其中有67%的患者APP存在可利用的高危漏洞。

患者APP存在的漏洞风险情况



高危漏洞分布情况



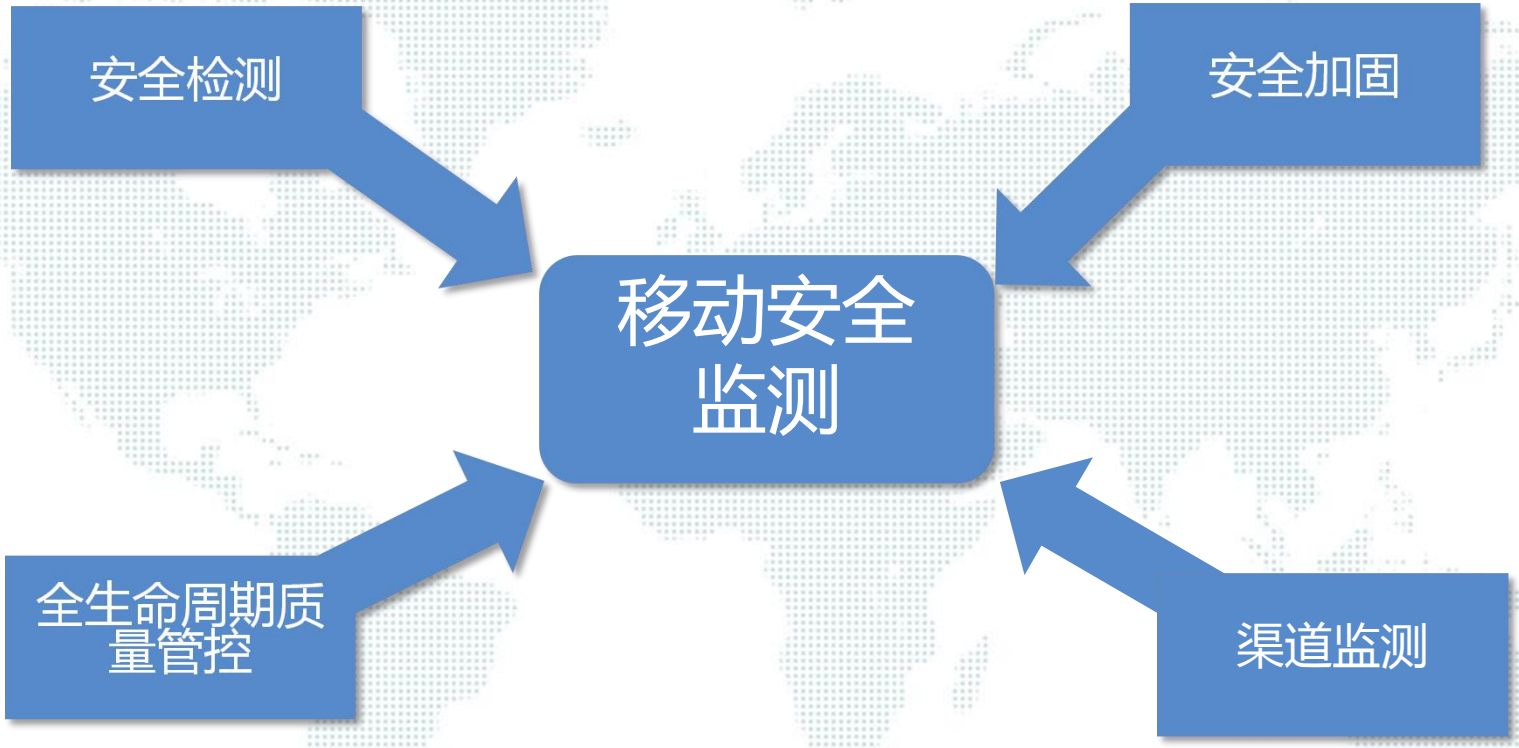
安全漏洞危害

经济损失

对用户造成不可逆的伤害

经济-》法律-》国家层面

移动安全监测解决方案

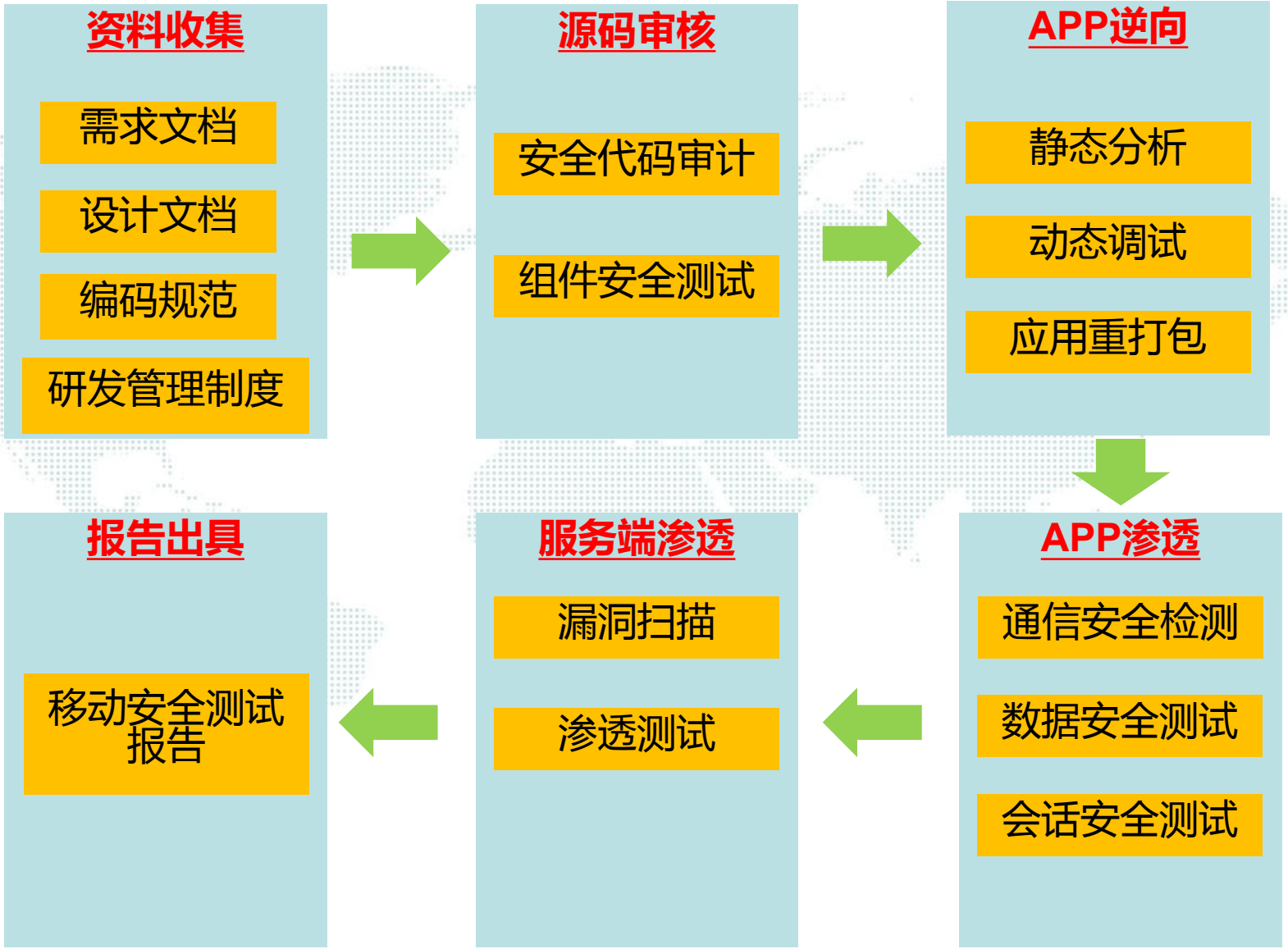


移动安全检测

移动安全测试内容

移动安全检测

移动安全测试步骤



安全检测

➢ **移动安全测试技术优势：**

1、采用静态反编译、动态分析、人工渗透等多种技术分析手段，立体式查找各种威胁。

2、模拟用户和手机交互行为，检测服务器的安全问题，全面、深层检测，保障系统整体的安全性。

3、提供针对性安全修复建议、权威、专业的第三方安全检测报告，符合监管、内审等的要求。

移动安全加固


防反编译保护
1
防篡改保护
2
签名校验
3
So加壳
4
反截屏
5
反调试保护
6
防进程注入
7
Lua保护
8
界面防劫持
9
等等。。。
10

移动安全加固

安全加固技术

1、核心代码加密，加密后无法静态分析关键文件的相关函数代码

2、关键指令转换，抽取指令并转换为机器码，有效抵抗黑客分析、反编译和破解

3、安全SDK加固，提供客户端软件的安全检测、清场和工具防护

移动安全加固

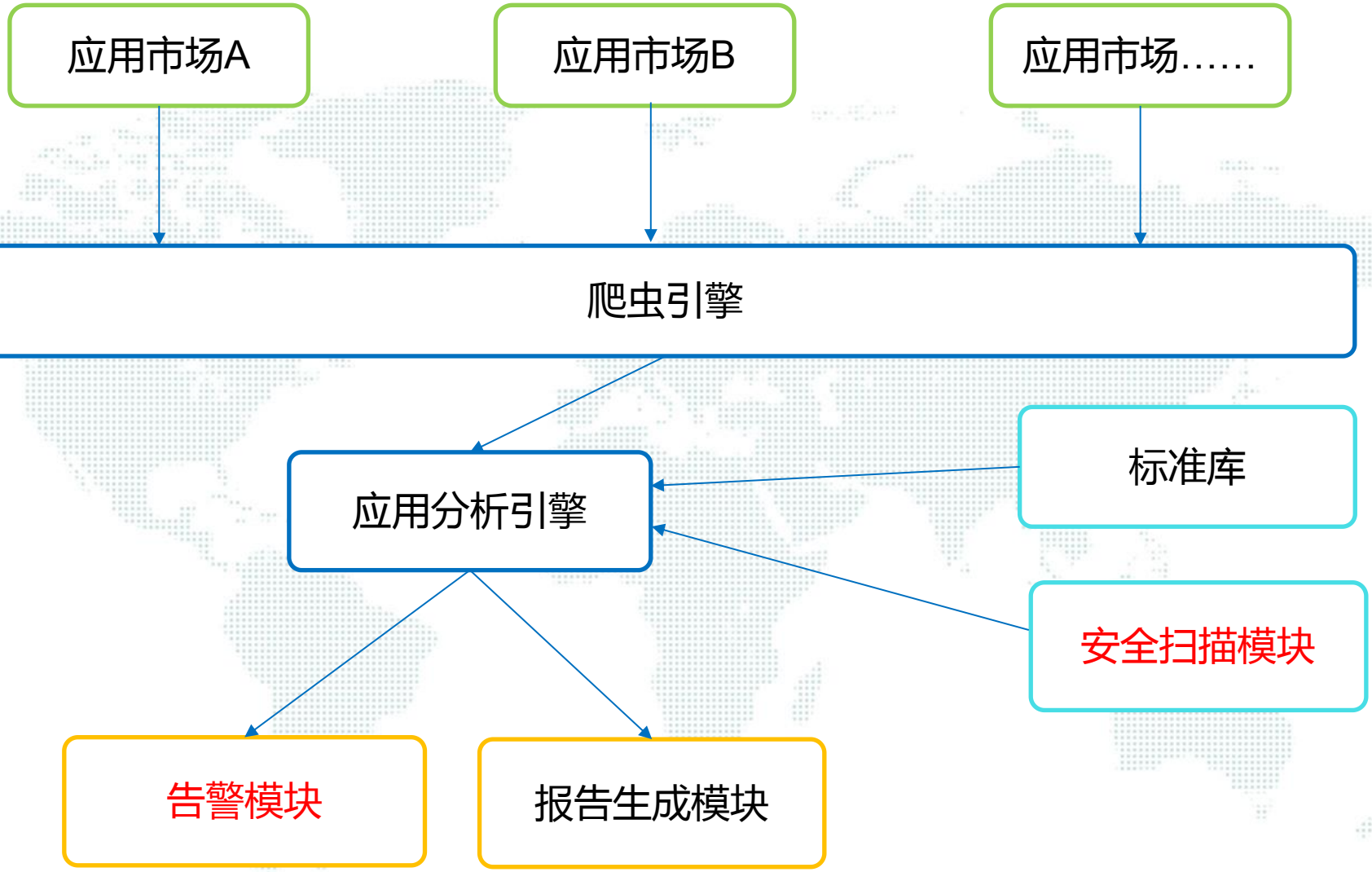
安全加固技术

4、加固后的代码已经被转换成机器码，不能再还原为原始JAVA代码，有效控制各类风险隐患

5、无法静态分析核心代码内容，运行时加固的核心代码不进行还原，有效防止核心代码泄露

6、加固后程序启动速度快，兼容性好

渠道检测



采用静态爬虫技术和基于WebKit动态爬虫技术结合收录700多个有效渠道。

渠道检测

实现原理

1、爬虫引擎从各个APP市场爬取APP应用。
2、APP应用通过应用分析引擎与标准库中的程序进行对比，检测文件是否发生改变。
3、同时安全扫描模块对APP进行扫描，检测是否存在漏洞。
4、标准库：正版APP的文件码。
5、将应用分析引擎的分析结果通过报告生成模块输出报告。
6、如果应用分析引擎发现APP存在问题通过告警模块通知相关人员。

渠道检测

技术优势

1、支持分布式部署，检测及时，可扩展。

2、支持精准识别、盗版分析、态势评估等功能，统一管理各发布渠道。

3、支持定时、随机检测各个应用市场。

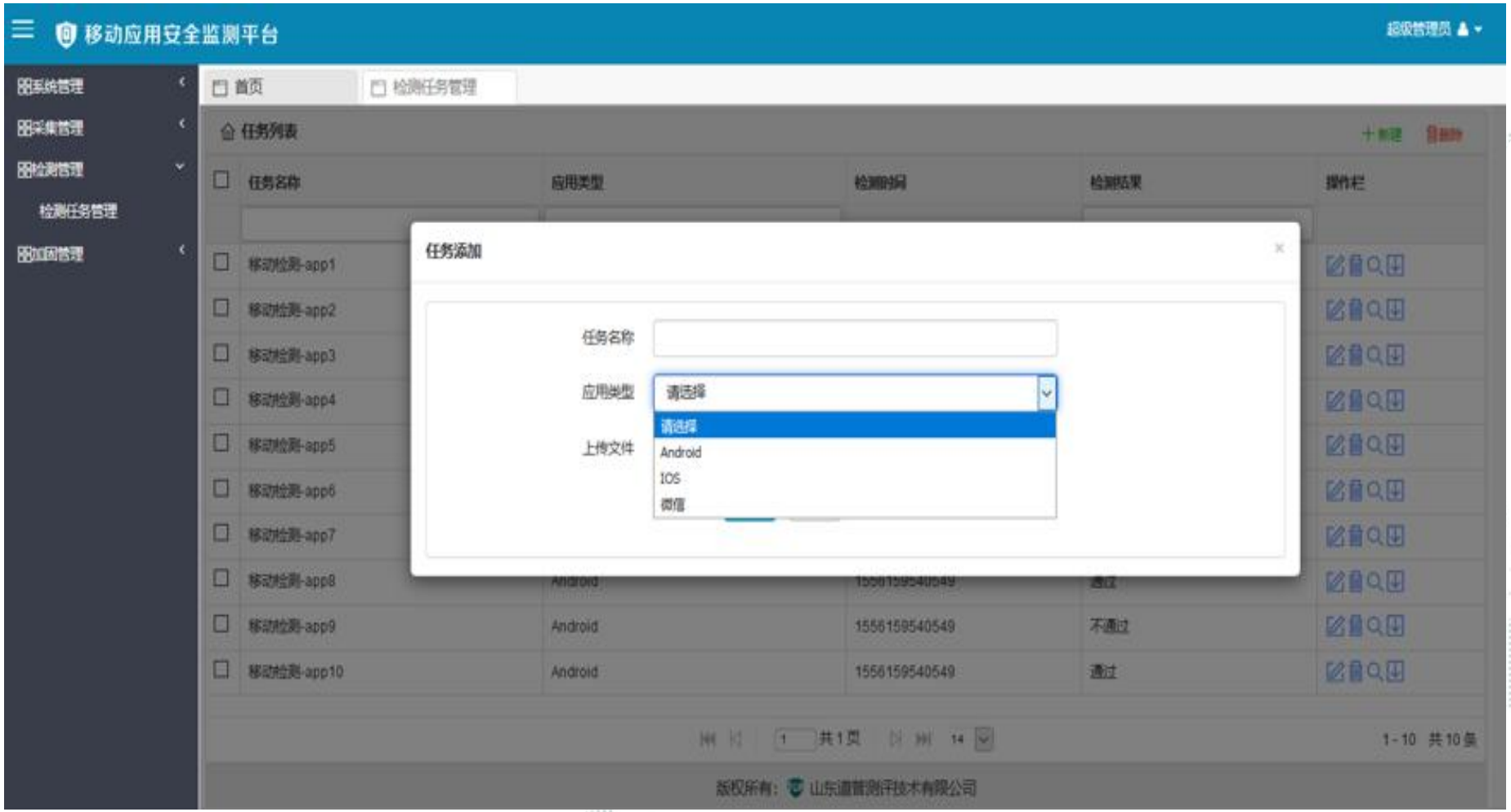
4、精准盗版大数据分析策略，支持多种报告格式。

5、支持短信、微信、邮件等多种告警方式。

道普移动安全监测平台

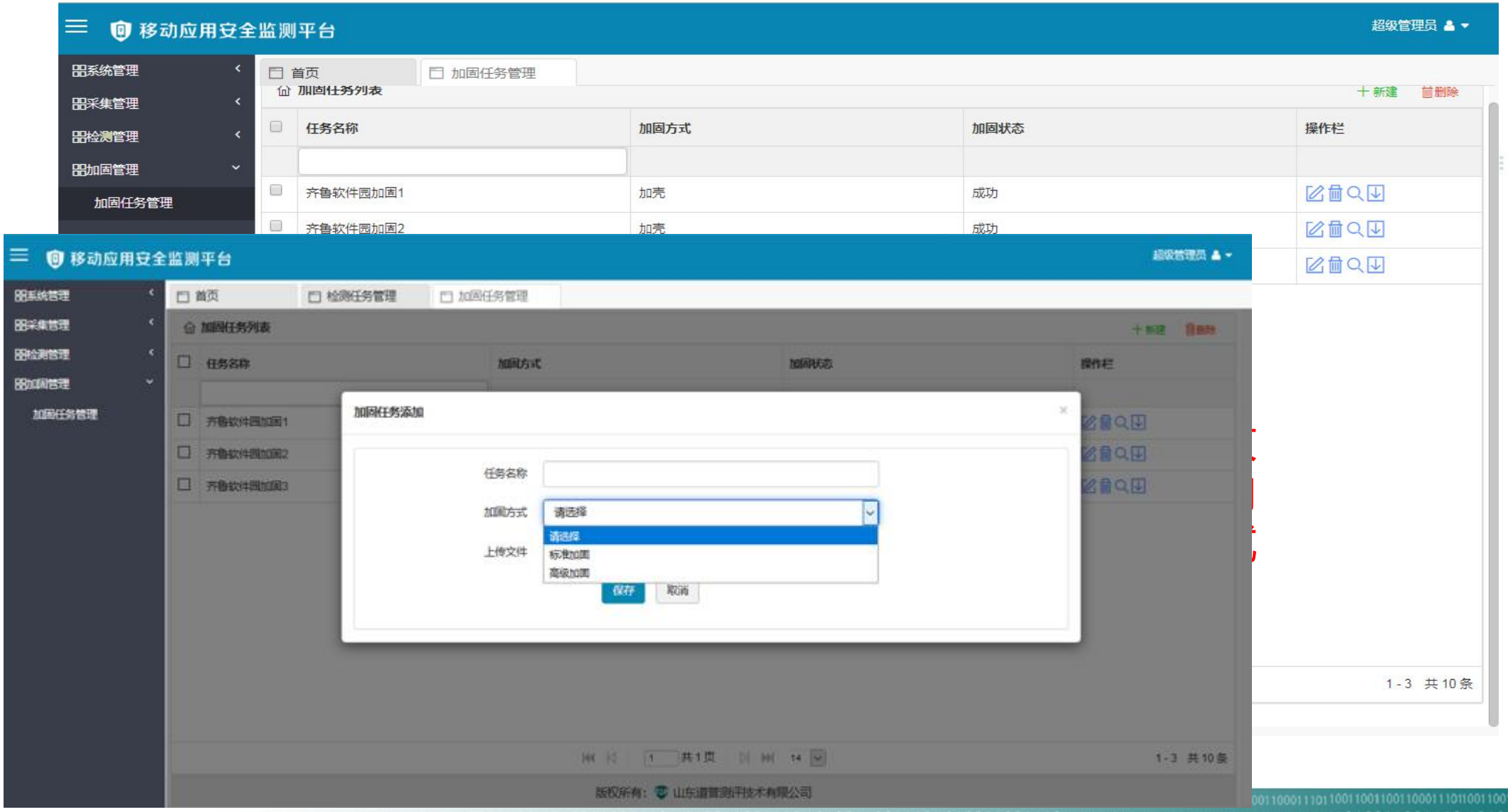
- 集移动安全检测、安全加固、渠道监测与一体

道普移动安全监测平台

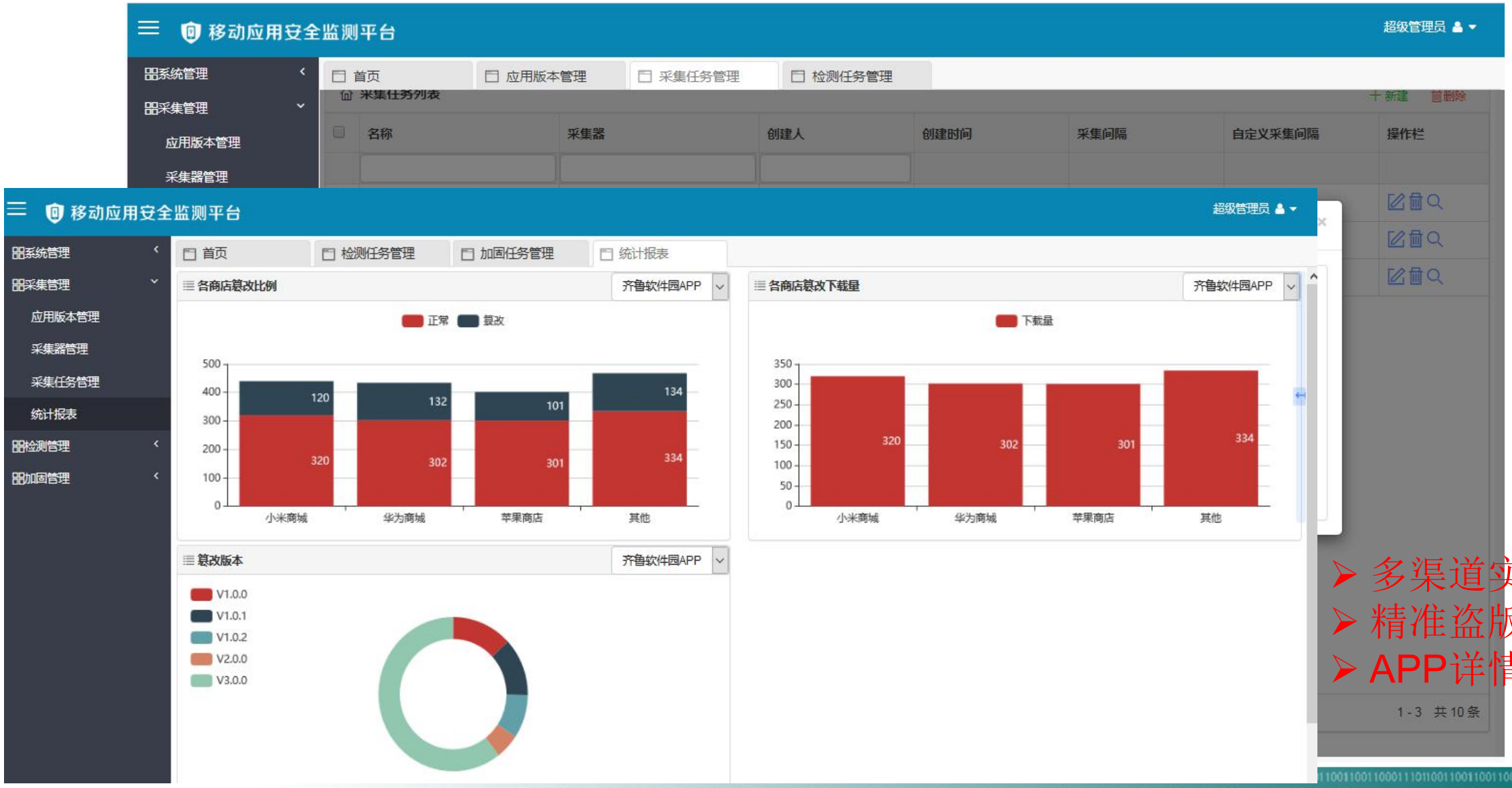


- 支持**APP**自动化安全检测
- 支持微信**公众号**自动化安全检测
- 支持微信**小程序**自动化安全检测

道普移动安全监测平台


移动应用安全监测平台
超级管理员
系统管理
采集管理
检测管理
加固管理
加固任务管理
首页
加固任务管理
加固任务列表
新建
删除
任务名称
加固方式
加固状态
操作栏
齐鲁软件园加固1
加壳
成功
齐鲁软件园加固2
加壳
成功
1 - 3 共 10 条
检测任务管理
加固任务添加
任务名称
加固方式
请选择
上传文件
标准加固
高级加固
保存
取消
共 1 页
1 - 3 共 10 条
版权所有：山东道普测评技术有限公司

道普移动安全监测平台



- 多渠道实时监测
- 精准盗版识别
- APP详情分析

全生命周期质量管理

➢ 四、交付阶段
1.渠道监测
2.应急响应
3.安全运维

➢ 三、实现阶段
1.移动安全检测
2.人工渗透测试
3.安全加固

➢ 一、需求阶段
1.明确移动安全需求
2.安全需求评审

➢ 二、设计阶段
1.采用安全SDK（安全键盘、数据库保护、缓存文件保护、通讯加固等）、APP运行环境监测、敏感信息隔离沙箱、安全编译器
2. 安全设计评审

全生命周期质量管理

技术优势

1、提升质量：全过程的软件质量保障措施，提高项目管理水平，保证系统的建设质量。

2、降低风险：全过程的管控，可以及时发现、解决系统建设过程中的问题和风险，加强APP管理（7*24小时监控发布渠道）。

3、降低成本：全程管控，保证系统质量，降低系统运维成本。

服务价值

服务价值

- 提前发现版本的安全漏洞，避免安全风险引起的经济损失和影响
- 保护知识产权，增加系统安全性，防止APP被调试、分析，增加抗逆向、抗汇编的防护能力
- 监控商城版本盗版情况，进行应用篡改风险监测
- 前期识别设计或实现上的安全缺陷，降低漏洞维护成本

典型案例

某医院的掌上APP安全检测、加固、渠道监测为例：

--为提高医疗行业的能力和服务水平，某医疗主管单位着手建设该医院的诊疗服务、个人中心、医健通等APP系统，整个系统包括预约挂号、专家出诊、门诊费用、报告查询、院内导航、住院服务、个人中心等多项功能。

--系统建设方面临的问题：

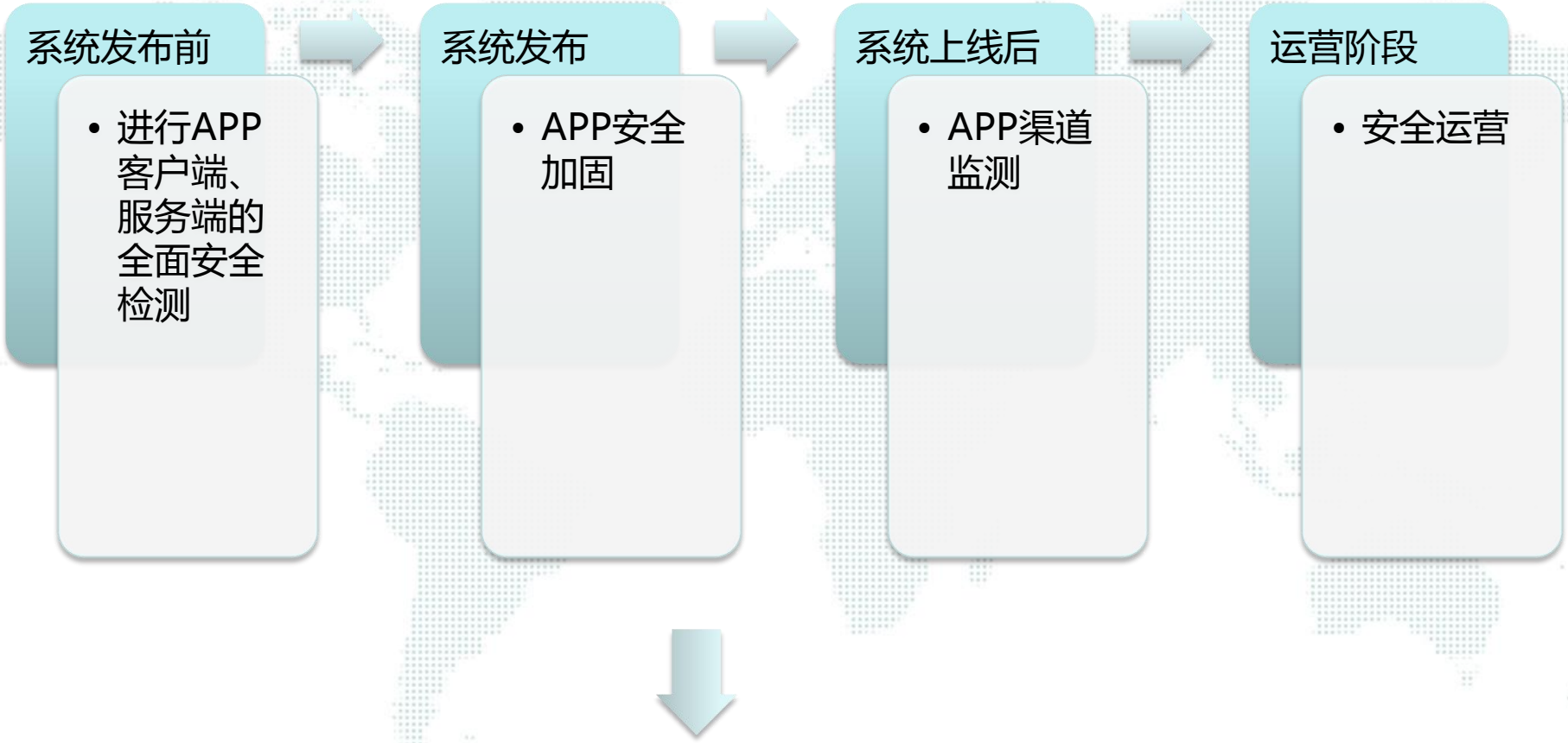
--由于医疗行业的特殊性，患者预约信息、检查检验信息、就诊信息、医学数据等医疗信息都是属于需要紧急使用的、敏感的信息，一旦泄露或被利用将造成严重的影响；

--针对APP应用，存在版本等恶意破解等行为，给用户带来严重危害；

--APP商城杂乱，版本较多，对盗版软件的管理困难，渠道监测薄弱；

典型案例

- 解决方案


系统发布前
进行APP客户端、服务端的全面安全检测
系统发布
APP安全加固
系统上线后
APP渠道监测
运营阶段
安全运营
全生命周期质量管理

典型案例

- 价值：
  - **检测**：提前发现并修改了系统中存在的APP组件使用不安全、安全支付漏洞、广告插入风险、文件任意读写、二次打包攻击等安全缺陷；
  - **加固**：规避APP存在易被反编译、反调试等问题；
  - **监测**：有效识别应用商店、技术网站、论坛、 网盘等各个商城的APP版本，发现篡改、 仿冒应用、盗版等风险；
  - 提前发现遗漏的安全需求，相关安全威胁，并设计相关安全模块，节约了后期维护成本；
  - 通过第三方专业测试，系统安全问题得到明显改善，没有出现由安全漏洞引起的问题，得到上级单位领导认可赞扬。

目录 CONTENTS

安全运营模型介绍

- 感知

感知是预测并发现网络威胁的能力。需要通过网络威胁情报和主动防御来预测向其逼近的威胁或攻击，在攻击成功实施前将其发现。必须知道可能会发生的事，同时采取精确复杂的分析来获取针对中断事件的风险预警。

- 抵御

简单地说抵御机制就是护盾。建立防御机制首先需要了解整个生态系统所能承受的风险，然后在此基础上建立三道防线：

第一道防线：在日常操作中采取控制措施

第二道防线：部署监控职能，如内部控制、法务控制、风险管理与网络安全

第三道防线：实施强有力的内部审计

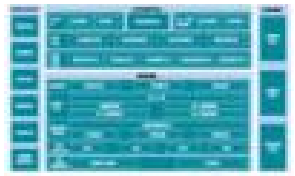
- 响应

如果识别失效（没能察觉逼近的威胁），抵御机制也出现问题（控制措施的效力不足），便需要为相关中断事件、故障响应措施以及危机管理做好准备。同时，也需要开始保留有力的法律证据，并对安全事件进行调查以安抚关键利益失联方----客户、监管机构、投资者、执法机关及公众，因为其中任意一方都可能发起诉讼，要求对其损失或不合规行为进行赔偿，而攻击的责任主体一经确认，则可以对之进行诉讼索赔。最后，需要以最快的速度恢复日常业务，从中学习经验，并调整与重塑以逐步加强网络弹性。

关注网络风险，而不仅仅是网络安全

五大能力建设

输入

- 业务发展规划 
- 业务发展规划 
- 网络安全风险 
- 安全技术趋势 
- 合规管理要求 

安全目标

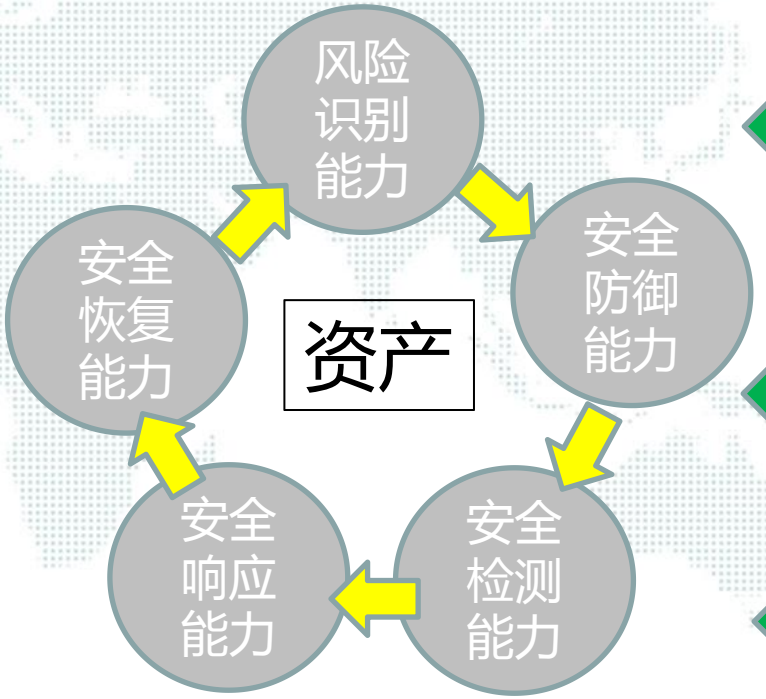
- 风险可见化
- 防御主动化
- 运行自动化

指导

支撑

安全能力

网络空间安全体系框架



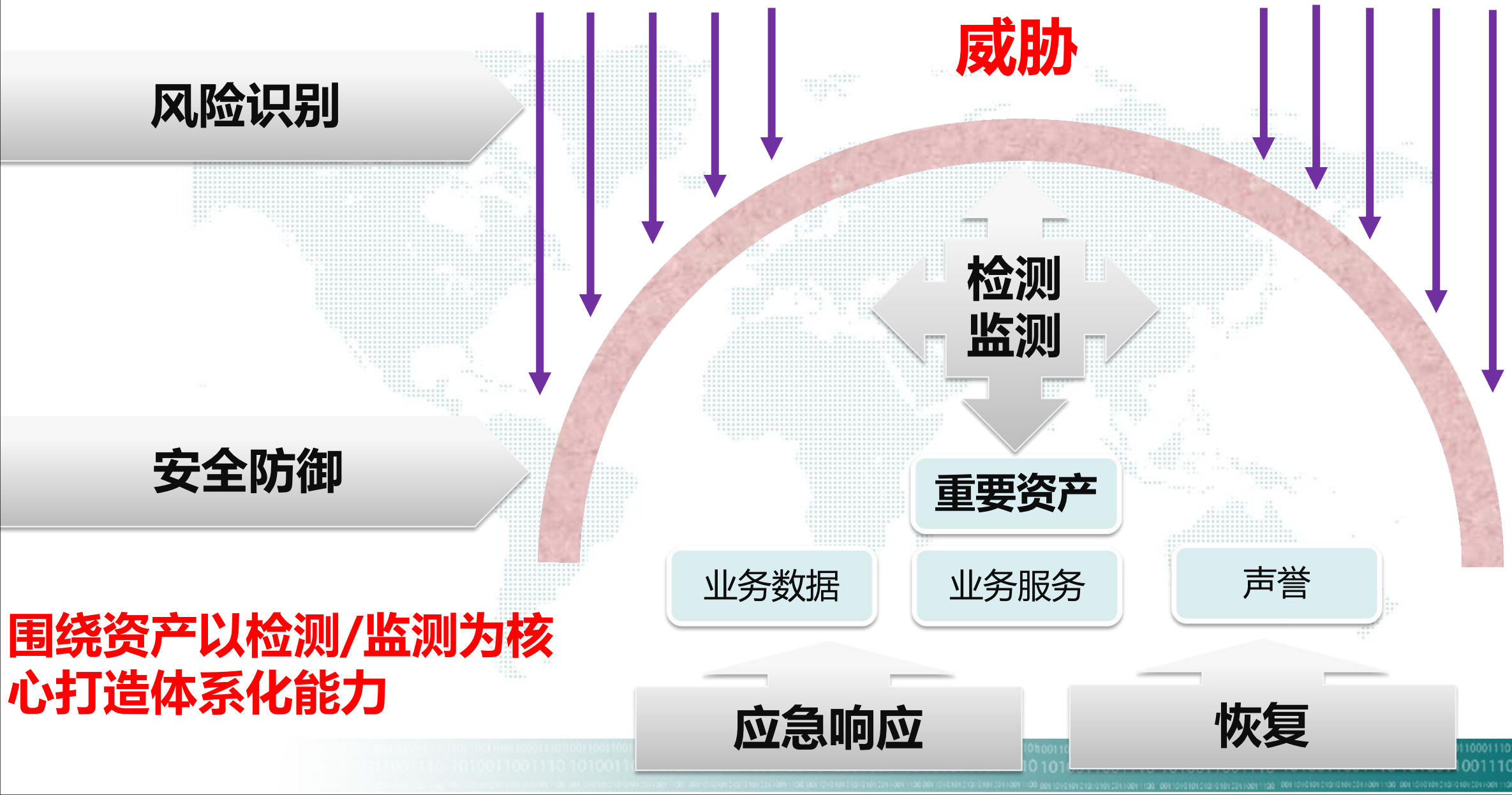
识别并建立防护对象框架

支撑体系

- 组织体系
- 管理体系
- 技术体系

围绕安全目标构建主动安全能力

安全赋能



围绕资产以检测/监测为核心打造体系化能力

目录 CONTENTS

公司介绍

山东道普测评技术有限公司（山东省软件评测中心）是一家综合性IT服务机构，是山东省内唯一 一家具备信息化建设全程服务能力的第三方IT服务机构，致力于第三方信息化风险管控

公司架构

公司作为山东省计算中心在软件工程、信息安全等多领域科研成果应用与服务载体，以多年的科研成果积累和雄厚的技术能力为基础，面向社会提供**智能系统、软件质量、信息安全等相关的检测、咨询服务**，致力于让用户的信息化更简单更安全

山东省科学院

山东省计算中心

山东道普测评技术有限公司

山东省软件评测中心

山东省计算机网络质量监督检验站

国家保密科技测评中心山东分中心

公司服务定位、价值、优势

使　命： 让信息化更简单更安全

愿　景： 第三方信息化风险管控领导者，成为共创事业的平台

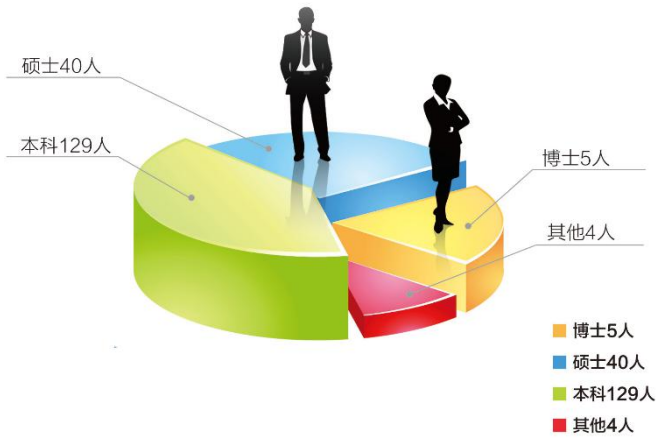
价值观： 让每个人成为创意精英

企业文化： 创新、求是、精进、利人

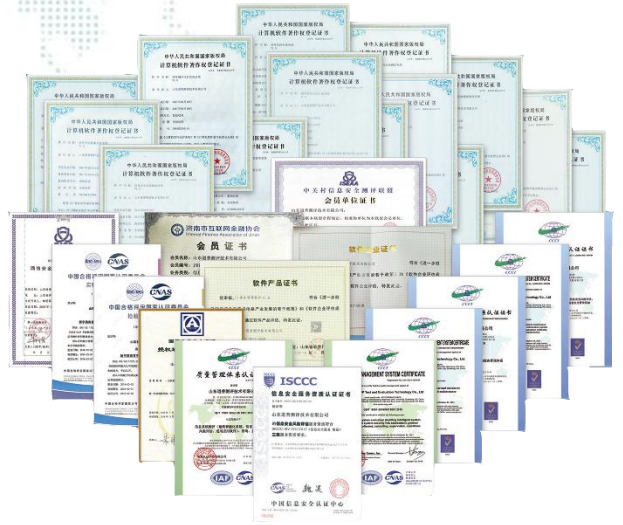
平台：山东省科学院计算中心在信息化战略、软件工程、信息安全、涉密工程、智能交通、智能建筑等多领域科研成果转化平台

服务：针对风险，提供规划咨询、过程管控、检测验收、应用评估等服务，充分发挥第三方的作用和价值

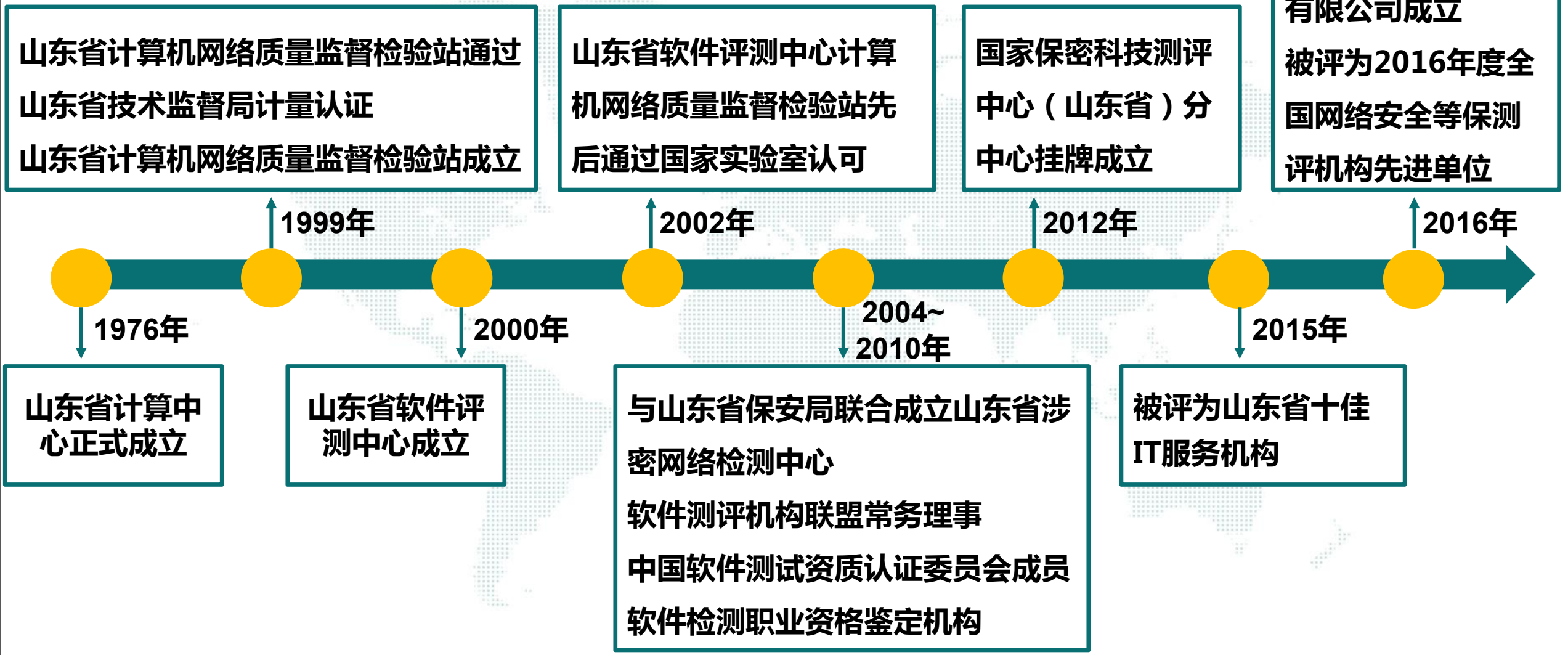
博士领军 硕士为主体的中高端人才队伍



人才　专业



发展历程


1976年
山东省计算中心正式成立
1999年
山东省计算机网络质量监督检验站通过山东省技术监督局计量认证
山东省计算机网络质量监督检验站成立
2000年
山东省软件评测中心成立
2002年
山东省软件评测中心计算机网络质量监督检验站先后通过国家实验室认可
2004~2010年
与山东省保安局联合成立山东省涉密网络检测中心
软件测评机构联盟常务理事
中国软件测试资质认证委员会成员
软件检测职业资格鉴定机构
2012年
国家保密科技测评中心（山东省）分中心挂牌成立
2015年
被评为山东省十佳IT服务机构
2016年
山东道普测评技术有限公司成立
被评为2016年度全国网络安全等保测评机构先进单位

资质荣誉

- 中国合格评定国家认可委员会 认可实验室（CNAS）
- 中国信息安全认证中心 信息安全风险评估服务资质
- 中国信息安全认证中心 信息安全应急处理服务资质
- 山东省质量技术监督局 计量认证（CMA）
- 工信部首批推荐两化融合管理体系贯标咨询服务资质
- 中国软件测评机构联盟常务理事单位
- 中国软件测试资质认证委员会会员单位
- 中国系统与软件过程改进分会理事单位
- 国家保密科技测评中心（山东省）分中心
- 山东省经信委 唯一的软件产品登记测试机构
- 山东省司法厅 计算机司法鉴定机构
- 公安部 信息安全等级保护测评机构
- 山东省科技厅 信息系统测评工程技术研究中心
- 山东省建设厅 智能建筑检测机构
- 承担国家863、自然基金多项科研课题
- 参与制定多项国家标准

资质荣誉

2016等保先进单位

软件协会理事单位

计量认证

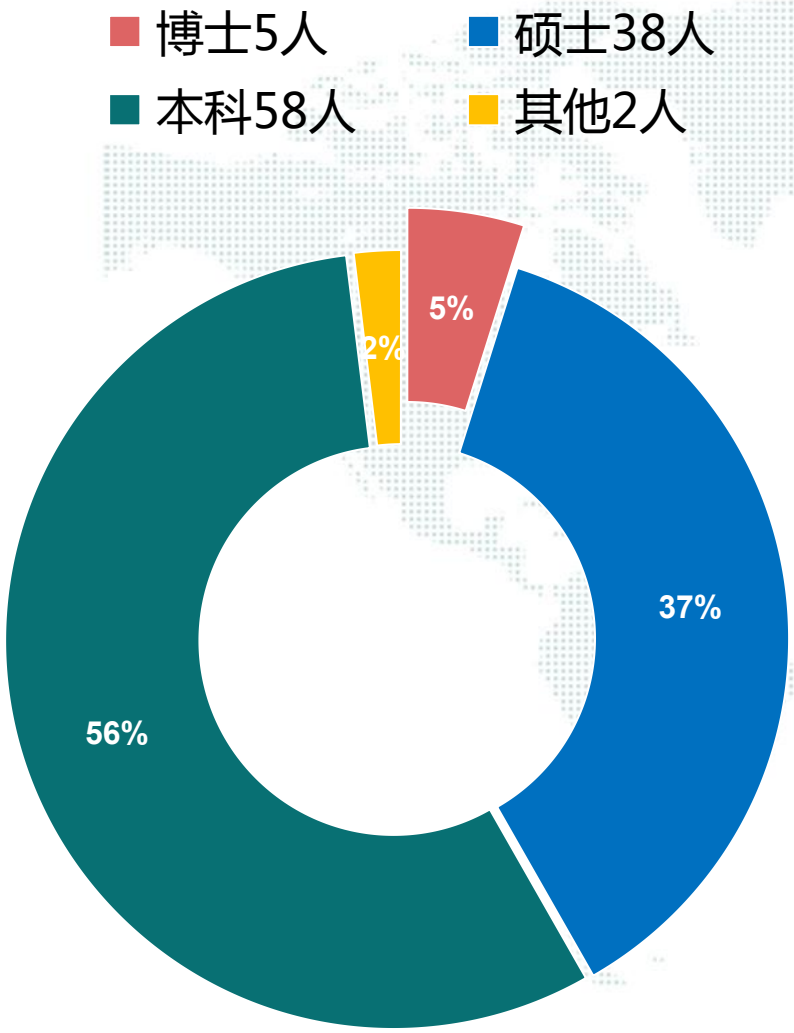
司法鉴定许可证

软件测评常务理事单位

保密测评分中心

服务团队

博士领军、硕士为主的高端人才队伍



我中心现有工程咨询师、系统分析员、软件测试工程师、信息安全等级测评师、网路规划设计师、安全工程师、质量工程师等人员超过80人,其中有多人通过:

- NCSE（国家信息安全技术水平考试）
- RHCA（红帽认证工程师）
- CCIE（思科认证互联网专家）
- OCP（Oracle数据库认证专家）
- CISSP（国际注册信息系统安全专家）
- CISA（国际信息系统审计师）
- PMP（国际项目管理工程师）
- Prince2（项目管理工程师）
- Cobit5 （IT治理实施认证）、ITIL（IT运维专家级认证）

大纲

1

风险来源

迎合数字化时代，把脉转型重点

风险识别

识别新常态风险，认清潜在后果

风险管控

护航信息化建设，管控全程风险

风险化解

驾驭信息化风险，实现组织价值

服务客户

山东省交警总队
山东省商务厅
山东省国资委
省人民检察院
山东省环保厅
河北高速
山东省公安厅
山东省国税局
山东省国土资源局
山东省质量监督局
山东省畜牧局
山东电力集团
山东交通运输厅
山东高速
中国石化
中国建设银行
中国农业银行
中国人民银行
中国光大银行
中国工商银行
山东钢铁
山东交运集团
山东齐鲁医院
中国黄金集团
山东盐业集团
山东远洋集团
鲁商集团
山东黄金集团有限公司
山东省立医院
中国航空工业集团公司

服务客户

党政机关

山东省纪委	山东省财政厅	山东省国税局	山东省总工会	山东省审计厅	山东省国资委	山东省委办公厅	山东省民政厅	山东省渔业厅
山东省公安厅	山东省经信委	山东省府办公厅	济南市中级法院	山东省水利厅	山东省林业厅	山东省农业厅	山东省政法委	山东省环保厅
山东省卫计委	山东省武警总队	山东省检察院	济南市检察院	山东省地税	山东省安监局	海南省国税局	山东省人社厅	山东省人防办

公路交通

山东交运集团	山东省交通运输厅	齐鲁交通发展集团	青岛交通工程质量监督站	青岛远洋集团	青岛市公路管理局
山东省高速集团	山东省交通质监站	山东省公安交警总队	山东交通厅机关服务中心	烟台市公路管理局	济南历下市政工程管理局

金融机构

齐鲁银行	齐商银行	中国光大银行	中国工商银行山东分行	烟台银行	中行济南分行
广发银行	中国民生银行	山东省金融办	山东省金融资产交易中心	泰安银行	山东省农村信用社联合社

服务客户

电力能源

焦家金矿	聊城供电公司	聊城国土局	中石化山东分公司	山东黄金集团	重庆电力公司
山东能源集团	山东电力集团	山东钢铁集团	中国电力科学研究院	贵州电网公司	枣庄市资源局

医疗卫生

山东省立三院	山东医科院附院	青岛市妇幼保健院	山东海王银河医药	山东省血液中心	山东省疾病预防控制中心
山东省眼科医院	滨州医学院附属医院	济南市急救中心	兖矿总医院	泰安中医院	肥城中医院

金融机构

北京大学	济南大学	山东省科技馆	山东省教育招生考试院	山东大学	山东省图书馆
南京大学	山东省教育厅	淄博市教育局	山东省青干院	山东政法学院	齐鲁工业大学

其他行业

鲁商集团	日照日报社	兖矿集团	浪潮集团	北京软通动力	济南二机床
山东省烟草	中电兴发	海康威视	恒通物流	山东中创	山东盐业集团

谢谢

山东省计算中心
山东省软件评测中心
山东道普测评技术有限公司

山东省两化融合促进中心
山东省计算机网络质量监督检验站
国家保密科技测评中心（山东省）分中心

济南总部：
电话：+86-531-86515189
传真：+86-531-82605299
邮编：250101
地址：济南市高新区银荷大厦D座5层

青岛办事处：
电话：+86-532-58628342
传真：+86-532-58628342
邮编：266100
地址：青岛市苗岭路37号省科院海仪所13层