御安信息
YU AN INFORMATION

APP应用安全合规解决方案

浙江御安信息技术有限公司

摄御四方 安如泰山

目录

CONTENTS

企业荣誉资质

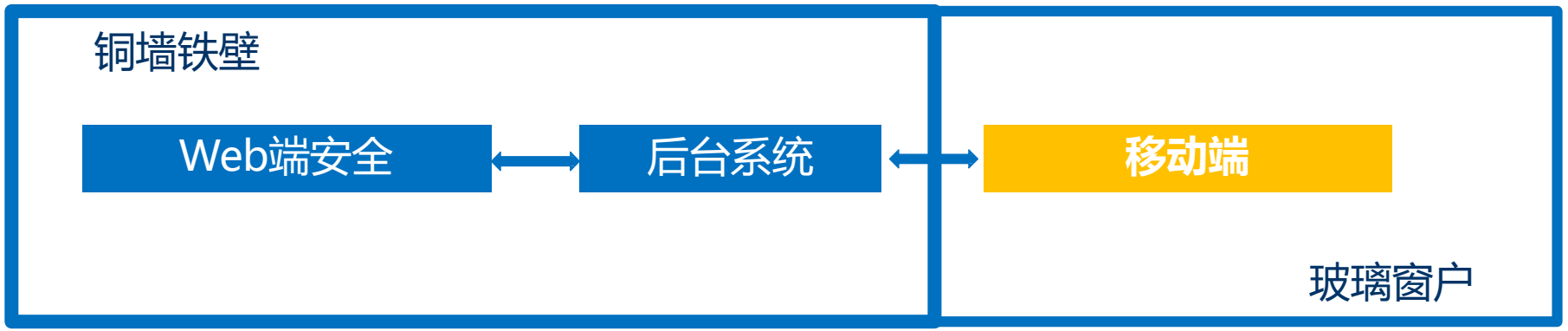
御安信息入选**首批中国互联网协会App数据安全测评服务工作组成员**，浙江省互联网协会个人信息保护专委会成员，同时也入选**工信部移动互联网APP产品安全漏洞库技术支撑单位**。从2019年以来，一直支撑多省省通信管理局进行全省的App个人信息保护专项工作，协助管局进行个人信息合规检测监管工作支撑。

目录

CONTENTS

安全背景-移动应用安全防护意识匮乏

同一个后台（互联网接入/移动接入），不同的安全策略,多终端安全策略的严重不统一性

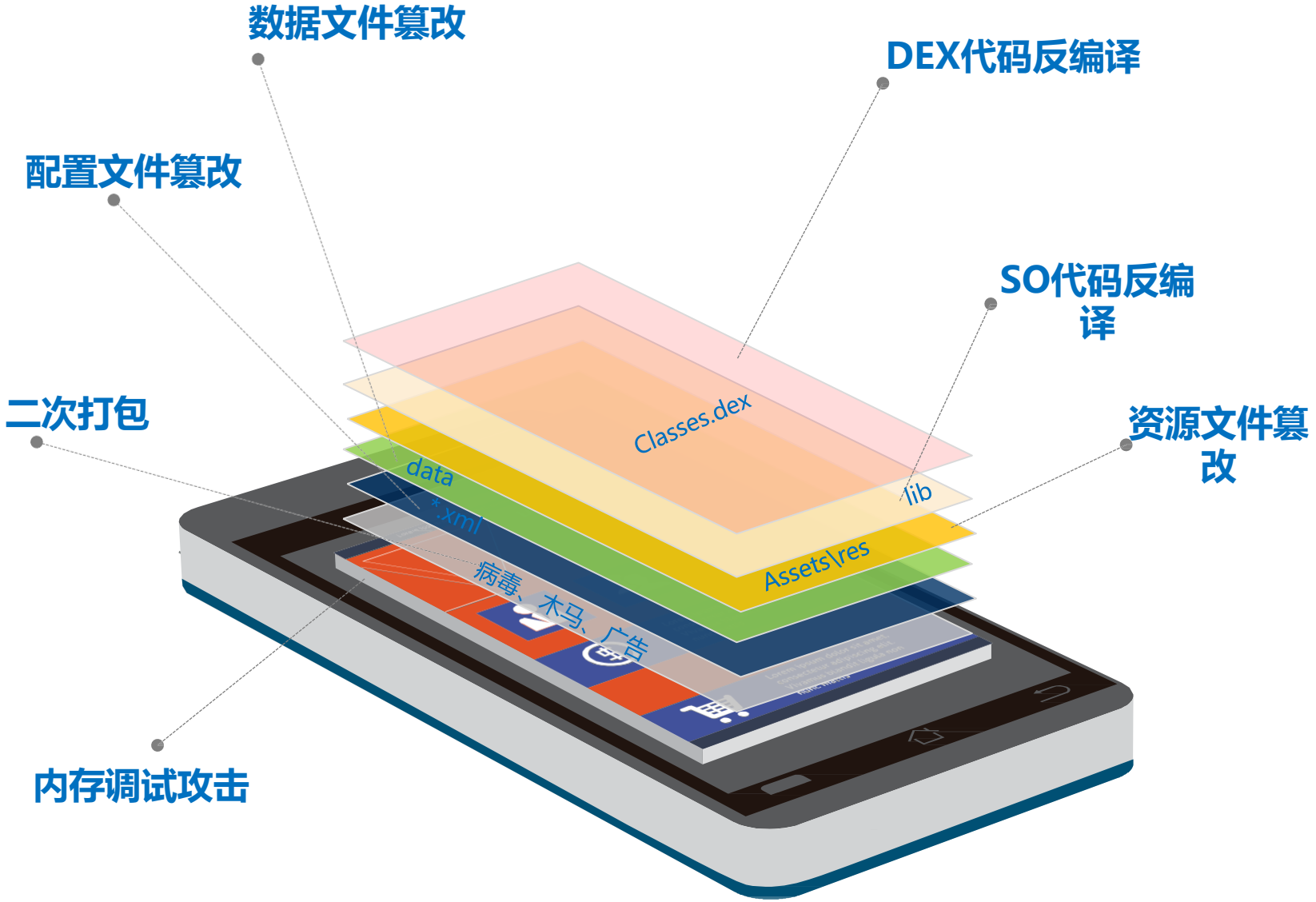


安全意识尚未从互联网时代进入移动互联网时代

安全背景-Android应用安全威胁

御安信息 YU AN INFORMATION

应用的破解是移动侧攻击的必然路径



针对安卓常见的威胁实例

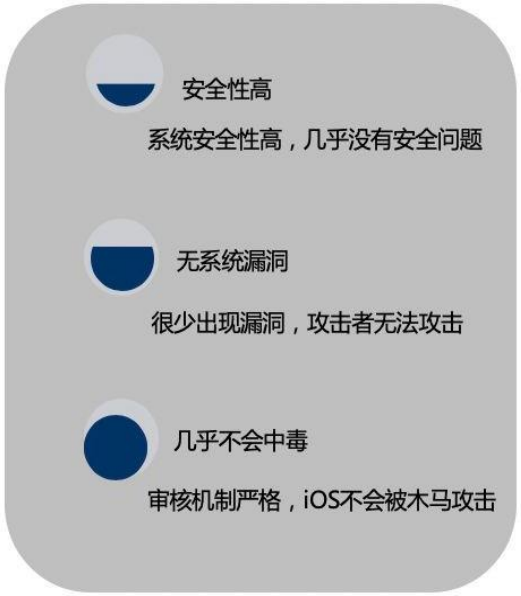
- 植入病毒、植入木马、植入广告
- 截屏录屏、信息窃取、交易篡改、刷单刷量、付费拦截
- 内购破解、支付屏蔽、权限破解
- IP窃取、仿冒、山寨

摄御四方 安如泰山

安全背景-iOS应用安全威胁

iOS App天然的低防御模式

由于苹果iOS系统的封闭性，一直以来开发者普遍认为iOS应用更安全。正是因为iOS开发者的这种心态，很少有开发者对iOS应用进行混淆、加密等加固处理，结果导致App惨遭破解。根据国外安全机构的最新调查，App Store前100名应用中87%均遭受黑客的不同破解攻击，涵盖了游戏、商业、生成、金融、社交、娱乐、教育、医疗等各个行业的应用，给开发者造成了非常大的损失。



理想很丰满
（用户认为的）

现实很残酷
（实际的情况）

安全背景-供应链安全风险

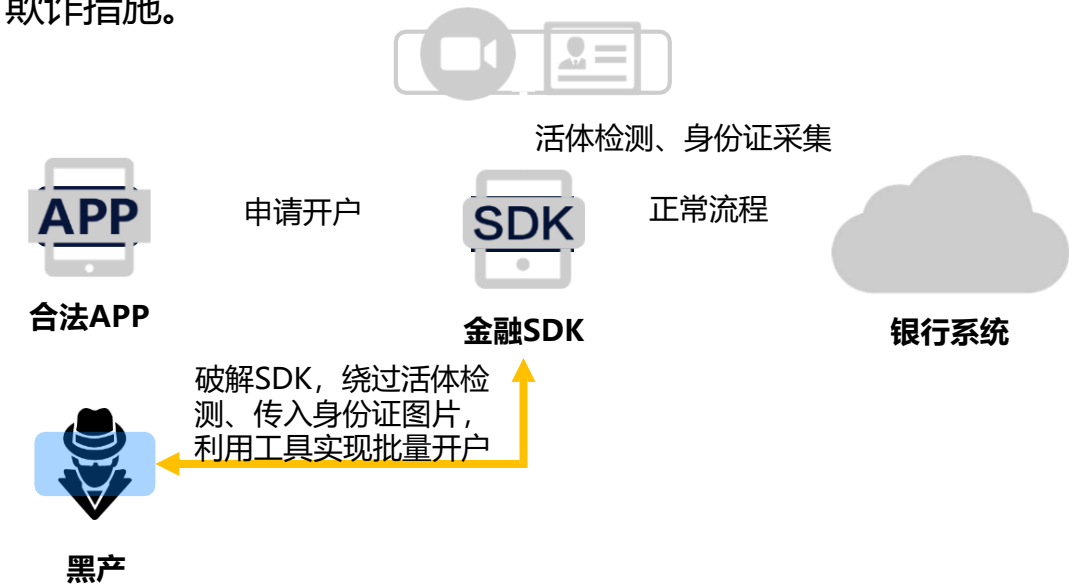
01 集成三方SDK

2018年4月，在“寄生推”漏洞事件里，第三方SDK可通过预留的“后门”云控开启恶意功能，进行恶意广告行为和应用推广以牟取灰色收益。

2019年3月，杭州某科技公司利用其对外提供的SDK非法搜集用户的电话联系人列表、地理位置和QQ登录信息。

02 外发SDK

2018年以来，不法分子利用银行的网络安全漏洞批量开立个人二三类虚假账户。主要问题包括：身份核验措施不足、系统存在安全漏洞、鉴权通道应用不规范、缺乏有效的交易反欺诈措施。



安全背景-渠道安全风险

御安信息 YU AN INFORMATION

钓鱼APP：从应用的图标、界面、名称等方面来伪装成合法或原版应用的APP，再通过第三方应用商店或钓鱼信息的方式诱使用户点击下载并安装。

山寨仿冒、恶意木马应用：山寨黄、赌、毒传播应用；手机木马伪装成官方应用、系统文件。


恶意软件假冒“个税”APP 税务总局:官方的没问题

2018年12月31日 08:26 中国新闻网

原标题：恶意软件假冒“个税”APP 税务总局：官方的没问题

图标	应用名称	版本号	应用 MD5	渠道市场
	云南红塔银行	v3.1	e7f63f62fe474f240898a521d9b0c6fe	安智市场、跑跑车市场、当易网
	农行手机银行	v1.0.0	fb3f7d6a64f53c8e4f5f8c2d3ded3770	安卓软件园、安卓乐园
	兰银个人版	v2.1	24d3d96d0fc240488d746d02dd71c838	雷电市场
	焦作中旅银行	v1.1.1	ed048668fd3c3bff109b0eaf6788115e	56 手机游戏
	中国工商银行	v3.0.0.0	91824bab0cdce01e735208bbcf59cf64	56 手机游戏
	光大银行	v3.1.5	d18caace9bd9dd7a11ebd62157d91eaa	56 手机游戏
	江西农信	v2.2	55d4c52360bd1be50b14c9e59ac8f5c3	统一下载站
	湖州银行	v1.4	a3f40b3a019b87e32de8274b0f9f3360	风暴数码、360 手机助手,爱奇艺应用商店
	兰银企业版	v2.2	a37b05f49495c83a459d7d4aed1efd30	搞趣网、免费市场,狐狸助手、爱奇艺应用商
	辽阳银行	v1.0	2260890b66f1f554df79fb8b4806e32e	应用酷,历趣市场
	广西农信	v1.6.5	9c61ed7e74d828bfa1c78f72e8b3d226	应用酷、OPPO 软件商店、安心市场

安全背景-运行环境安全风险

御安信息
YU AN INFORMATION

终端设备不可控

真机还是模拟器、多开器？
设备信息是真是假？
地理位置信息是真是假？

操作手段不可控

真人还是机器？
是否有人正在渗透测试？
是否在使用外挂等工具？

运行环境不可控

应用是否被破解？
静态加固保护机制是否被攻击？
运行环境是否有攻击框架？
系统是否被Root/越狱？

三方代码不可控

第三方SDK是否热更新代码？
是否偷偷搜集用户敏感信息？
是否有恶意安装应用等行为？

安全背景-四部委联合治理个人信息违规收集现象

御安信息 YU AN INFORMATION

四部委联合治理个人信息违规收集现象

2019年1月25日上午，中央网信办、工信部、公安部、市场监管总局等四部门召开新闻发布会，联合发布《关于开展APP违法违规收集使用个人信息专项治理的公告》。

2019年3月1日，App专项治理工作组依据《网络安全法》、《消费者权益保护法》、《信息安全技术个人信息安全规范》 等法律法规和国家标准，编制了《App违法违规收集使用个人信息自评估指南》。

法规政策指引

- 国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定了《App违法违规收集使用个人信息行为认定方法》，从6大方面对APP及其运营商收集个人信息作出法律要求。
- 《电信和互联网行业提升网络数据安全保护能力专项行动方案》要求企业加强APP数据防攻击、防窃取、防泄漏、数据备份和恢复等安全技术保障措施，对存在安全漏洞和非法采集个人信息的APP责令整改等严厉措施。

目录

CONTENTS

APP安全服务体系

御安信息 YU AN INFORMATION

四大服务能力全方位保证APP安全

产品介绍-应用安全测评平台

御安信息 YU AN INFORMATION

收集并分析活跃App上的安全威胁信息

威胁数据

设备复用检测、模拟器检测、加速器检测、攻击框架检测、修改器检测、地理位置造假检测、本地域名劫持检测、应用崩溃检测信息。

属性数据

硬件信息、系统信息、应用 安装信息、应用启动信息、 位置信息、函数劫持信息、 配置信息、Zygote信息、内 存信息、文件信息等。

安全指数判定

检查分析所有攻击的必然技术节点，从基础技术原理上检测各类交易欺诈信息。

威胁信息管控与展示

基于从威胁情报贡献的安全指数；基于不断训练提升的系统可信度，对接威胁指数到其他控制体系实现管控。

01 采集安全数据

02 建立威胁模型

03 分析安全指数

04 生成威胁情报

05 制定安全策略

建立威胁模型

结合业务特点，一方面通过自定义规则建立自有判定体系，另一方面利用大数据技术利用决策链分析、图论分析等技术手段对复杂场景进行威胁建模。

基于威胁模型关联威胁情报

关联设备威胁库、应用威胁库、账户威胁库和IP威胁库生成可信安全情报。

产品介绍-应用安全测评平台

01.静态防御闭环感知

针对加固、渗透测试、兼容性测试等静态保护措施的闭环验证，及时发现静态防御机制的不足。

02.第三方代码行为感知

实时感知在运行过程中的第三方SDK行为，针对非授权的行为进行拦截、审计。

03.应用运行时威胁感知

针对应用运行时威胁进行实时感知，感知应用运行时攻击威胁发生的时间、威胁类型、地点、手机信息、登录账号等多维度信息。

04.应用运行时风险感知

针对应用运行时的风险进行感知，及时掌握系统风险状况，针对高风险设备进行持续关注，溯源攻击准备过程。

产品介绍-Android应用安全加固

御安信息 YU AN INFORMATION

让您的Android应用在不安全不可控的环境里安全运行

DEX防逆向分析

- DEX文件整体加密，防逆向分析
- DEX函数抽取加密，动态加解密
- DEX混合加密
- Java 转 C
- 基于虚拟机指令保护（VMP）的DEX加密

SO库加密

- SO库文件加壳保护
- SO库文件代码压缩
- SO防dump保护
- SO防篡改保护
- SO防盗用保护

资源文件加密

- assets资源文件加密
- res资源文件加密
- raw资源文件加密
- XML配置文件防篡改

数据文件加密

- SharedPreferences数据文件加密
- 数据库文件加密
- 运行过程缓存文件加密
- SSL证书文件防篡改
- 动态加解密
- 数据透明加密

防篡改及二次打包

- 完整性保护
- 开发者签名校验

防日志泄露

- Error错误日志信息防泄漏
- Warning警告日志信息防泄漏
- Information提示日志信息防泄漏
- Debug调试日志信息防泄漏
- Verbose冗余日志信息防泄漏

防调试

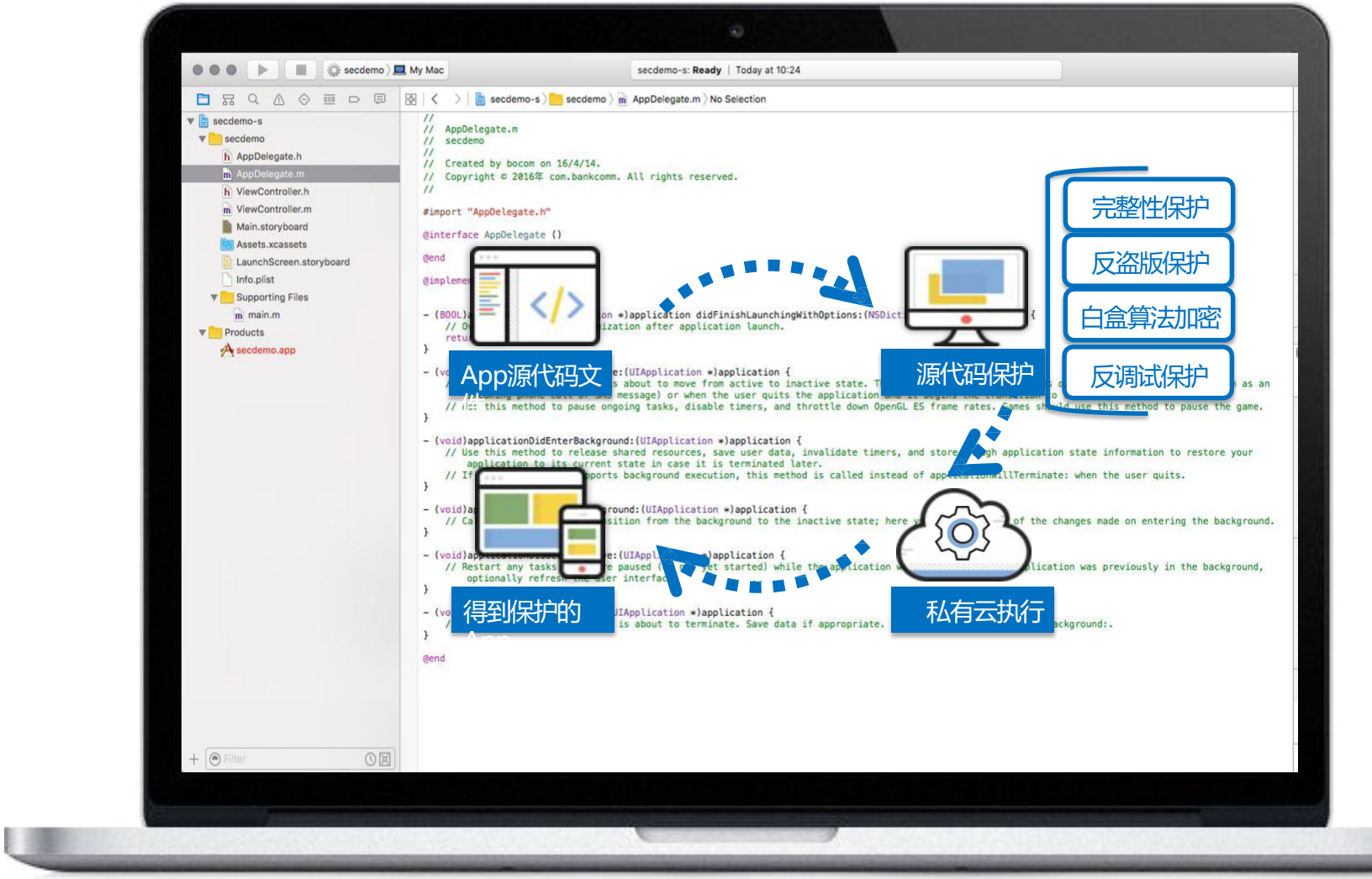
- 防动态调试
- 防内存修改
- 防动态注入

产品介绍-源代码安全加固

御安信息 YU AN INFORMATION

直接对源代码进行深度保护

御安源代码加固系统基于源代码层面，利用白盒保护技术构建一个人工有限时间无法分析的复杂逻辑，把**真实的代码逻辑隐藏到逻辑阵列中**，实现了**源代码的不可阅读及不可分析**从而达到保护代码的目的。在**加密代码**的同时，通过在源代码中**插入海量的交叉完整性检查，反调试及越狱检查分支**实现了对代码的多层面保护。



服务介绍-移动应用个人信息保护合规咨询

御安信息 YU AN INFORMATION

基于自评估指南等要求对企业App的合规情况进行快速评估，让企业能够快速了解当前在个人信息保护合规方面的实际情况，为后续开展个人信息合规工作提供支撑。

App个人信息保护 现状快速评估服务

通过对App的产品功能、业务流程进行梳理、信息安全技术，同时对企业在个人信息保护管理、安全开发管理流程规范方面进行全面的梳理，基于标准及法规要求，评估当前企业在个人信息保护技术与管理方面与国标的差距。提供合规整改方案。

App个人信息保护 合规咨询服务

根据整改方案以及企业现状，向企业提供合规整改服务，整改内容包括：

1、构建个人信息保护治理框架、构建企业安全开发管理体系提供整个咨询服务；

2、提供个人信息保护技术、信息安全技术 的合规整改咨询服务；

3、提供信息安全产品；

App个人信息保护 合规整改服务

服务介绍-移动应用渗透测试

御安信息
YU AN INFORMATION

Android移动应用渗透性测试
iOS移动应用渗透性测试

渗透测试

挖掘发现现有技术和业务风险漏洞

01
渗透测试
人工远程/人工现场开展的渗透性测试，挖掘发现安全漏洞。

02
漏洞讲解
人工远程/人工现场沟通移动应用漏洞，讲解漏洞原理，演示漏洞危害。

03
修复咨询
针对开发人员，远程提供针对漏洞的修复咨询。

04
漏洞复测
人工远程/人工现场提供开展的渗透测试风险漏洞复查。

浙江省通管局APP安全检测案例

配 合 开展网络和信息安全检查，对宁波、舟山等地区APP服务提供者开展APP侵害用户权益专项检查，重点针对未公开收集使用规则、未明示收集使用个人信息的目的、方式和范围、未经用户同意收集使用个人信息等四个方面10类问题开展检测，并对检测结果进行验证和分析。

在2022年支撑浙江管局完成**4万余个APP个人隐私合规检测**等，并提交**漏洞报告1228个**。

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

其他案例简介

御安信息 YU AN INFORMATION

配合监管部门进行APP检测

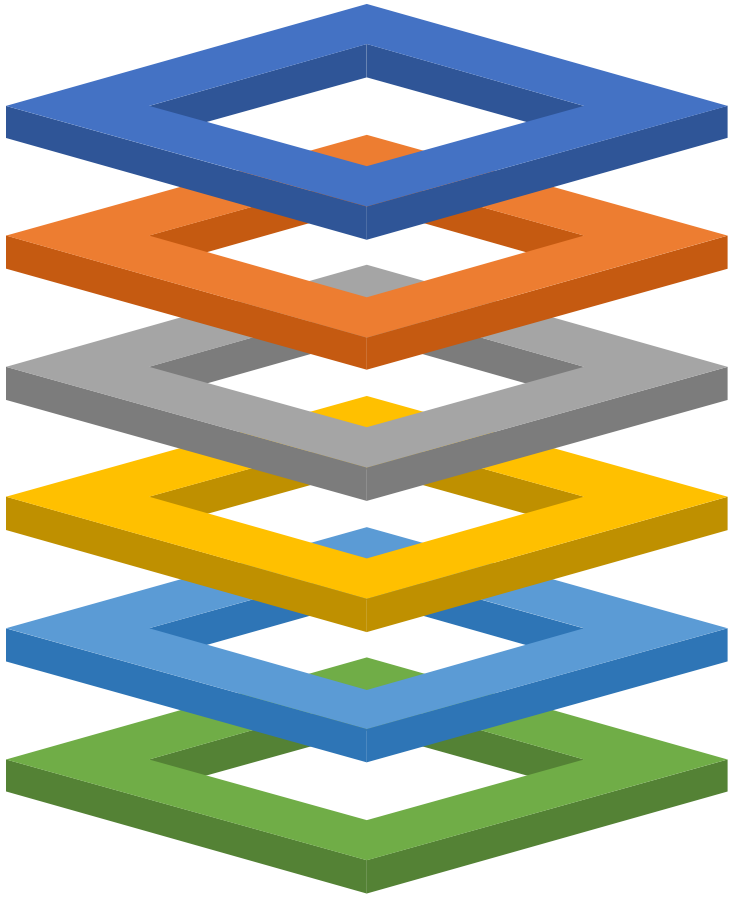
2022年配合其他省份省通管局进行3W+个APP侵害用户权益、个人信息保护等网络信息安全检查，不合规率95%

广电行业APP检测

2021年为华数数字电视传媒集团有限公司提供APP安全检测服务

互联网行业APP检测

为阿里巴巴、腾讯等互联网企业提供移动互联网应用（APP）网络安全评测服务



游戏行业APP检测

医疗行业APP检测

为杭州联科美讯生物医药技术有限公司（丁香医生）等医疗行业公司提供移动互联网安全等级保护测评服务

金融行业APP检测

为某省证券公司提供APP安全检测服务

御安信息
YU AN INFORMATION

Thanks for watching!

浙江御安信息技术有限公司