OWASP

Open Web Application Security Project

下一代移动应用安全

江苏通付盾信息安全技术有限公司

移动应用发展

5G时代的到来？

GDPR对国内关于在移动应用数据方面未来的影响？

OWASP
Open Web Application Security Project

攻防不对等导致黑客屡屡得手

问题不再是是否被黑，

而是什么时候被黑和你什么时候发现被黑

OWASP
Open Web Application Security Project

防护对象与防护边界的变化

互联网

从专业安全转向互联网+安全

从内向外

互联网+

业务驱动安全

外网 | 内网 | 业务专网

数据，传输

从边界安全转向IT生态安全

从一向多

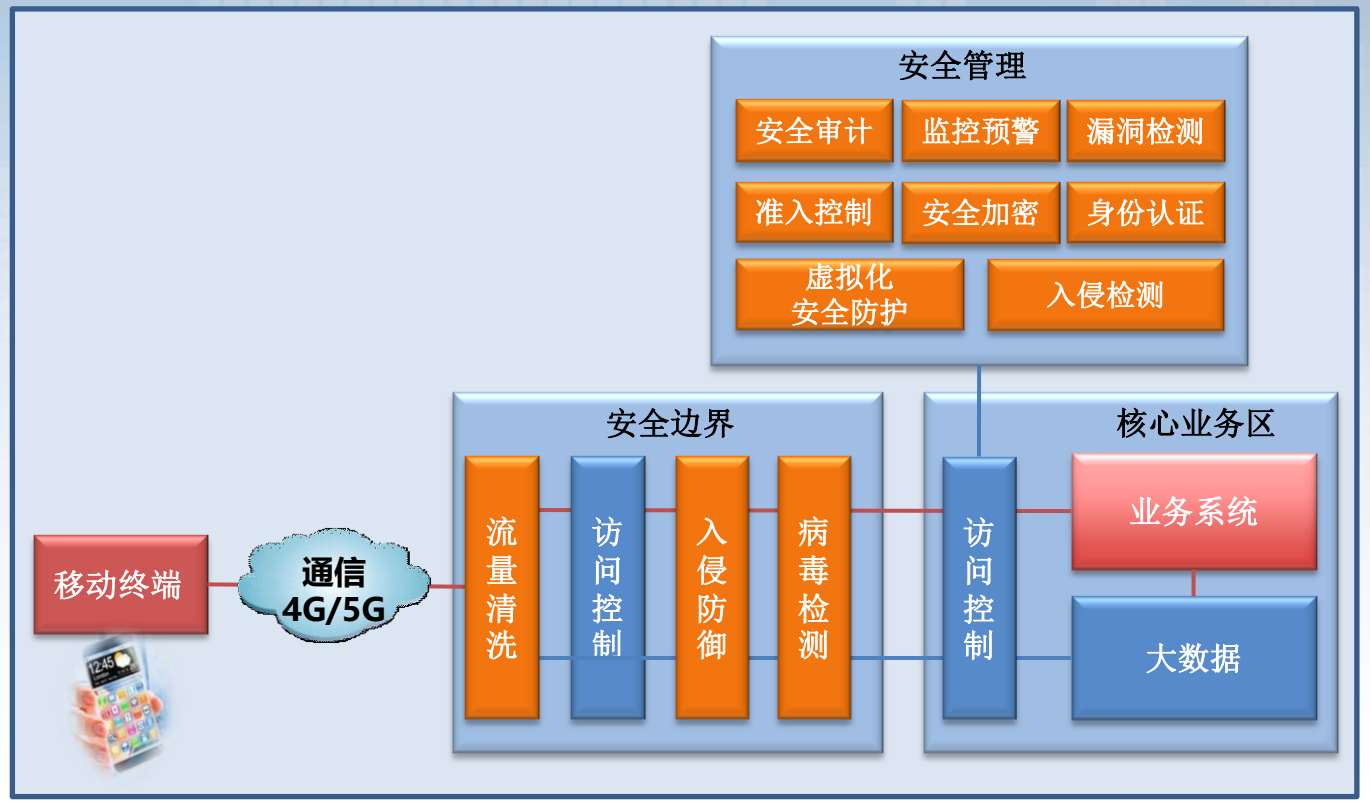
现今移动安全架构

终端应用：
实名认证
APP加固
不存储业务数据等

通信：
应用协议传输加密通道
抗DDoS攻击
蜜罐诱导攻击
APT攻击检测等

后台服务：
业务系统
大数据
云平台

安全管控：
安全审计
监控预警



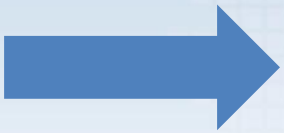
OWASP
Open Web Application Security Project

防御能力与业务发展不匹配

移动业务

移动办公

移动作业



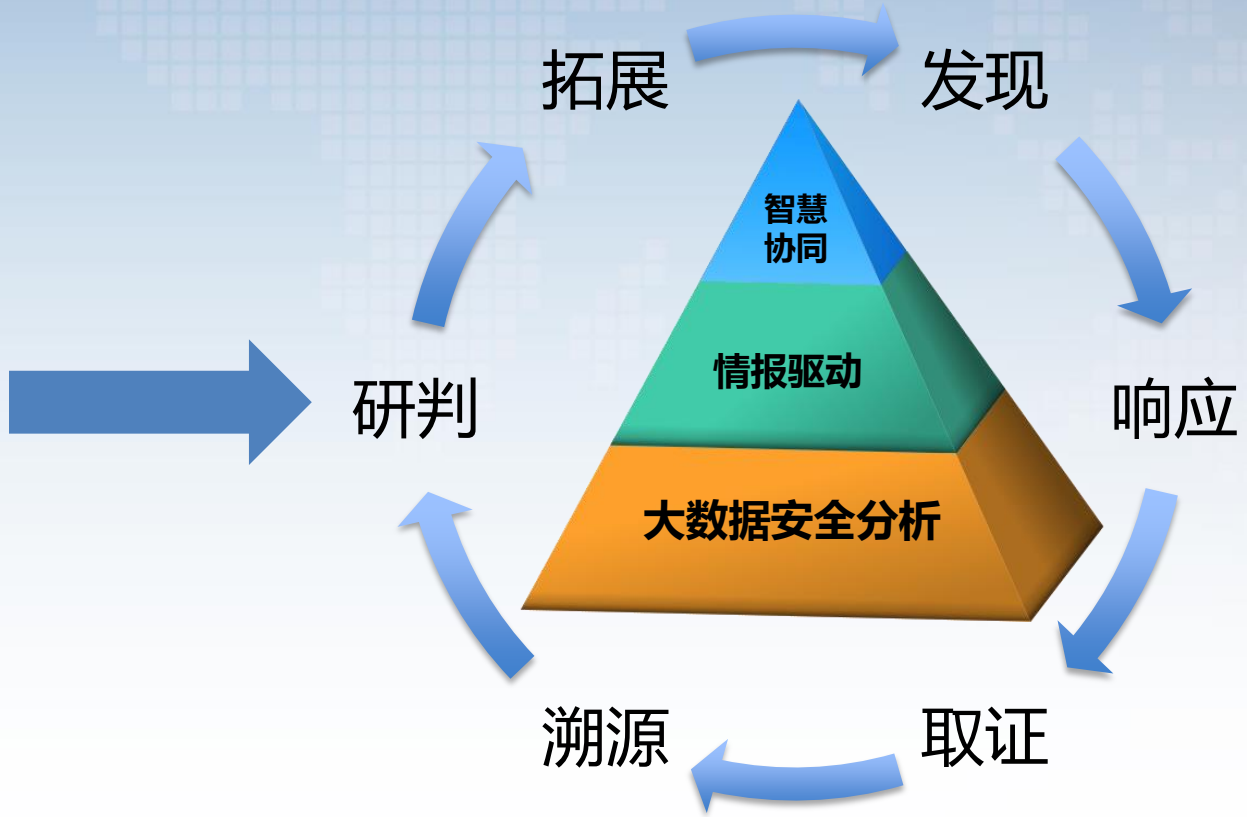
规划阶段 → 建设阶段 → 运行阶段

从静态防御到动态防御的趋势

部署、维护困难

数据标准不统一

计算能力弱



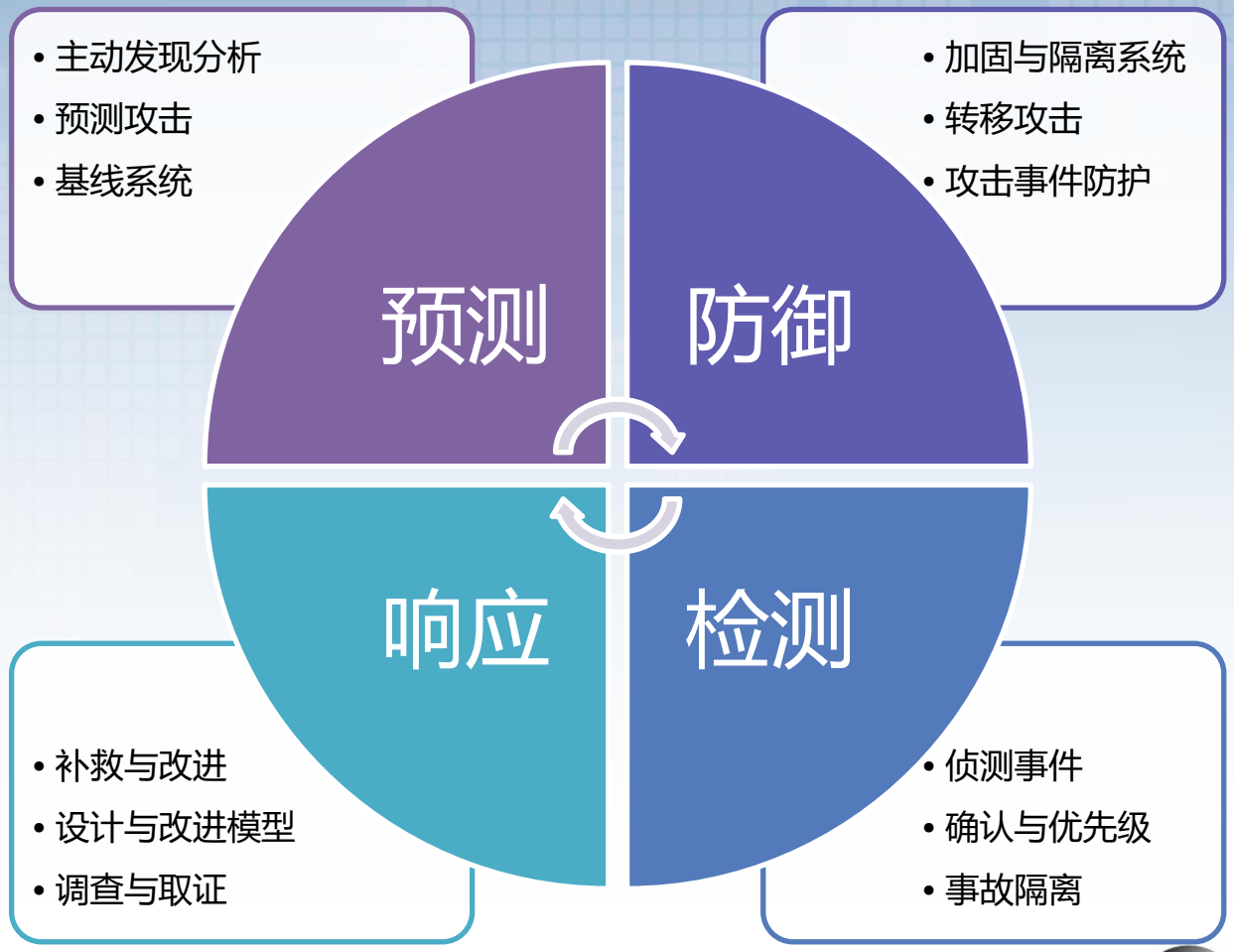
从S-SDLC和DevSecOps相结合

移动应用开发安全全生命周期

- 安全功能的服务化、自动化工具
- 响应的时间可控制在一个很短的时间内
- 减少产品研发过程中的安全投入，增强安全效果

OWASP
Open Web Application Security Project

下一代移动应用安全



OWASP
Open Web Application Security Project

立体化拟态防御体系

移动应用全业务流程

移动应用安全防护

联动防御

大数据学习和分析

1 发起攻击

2 发现攻击

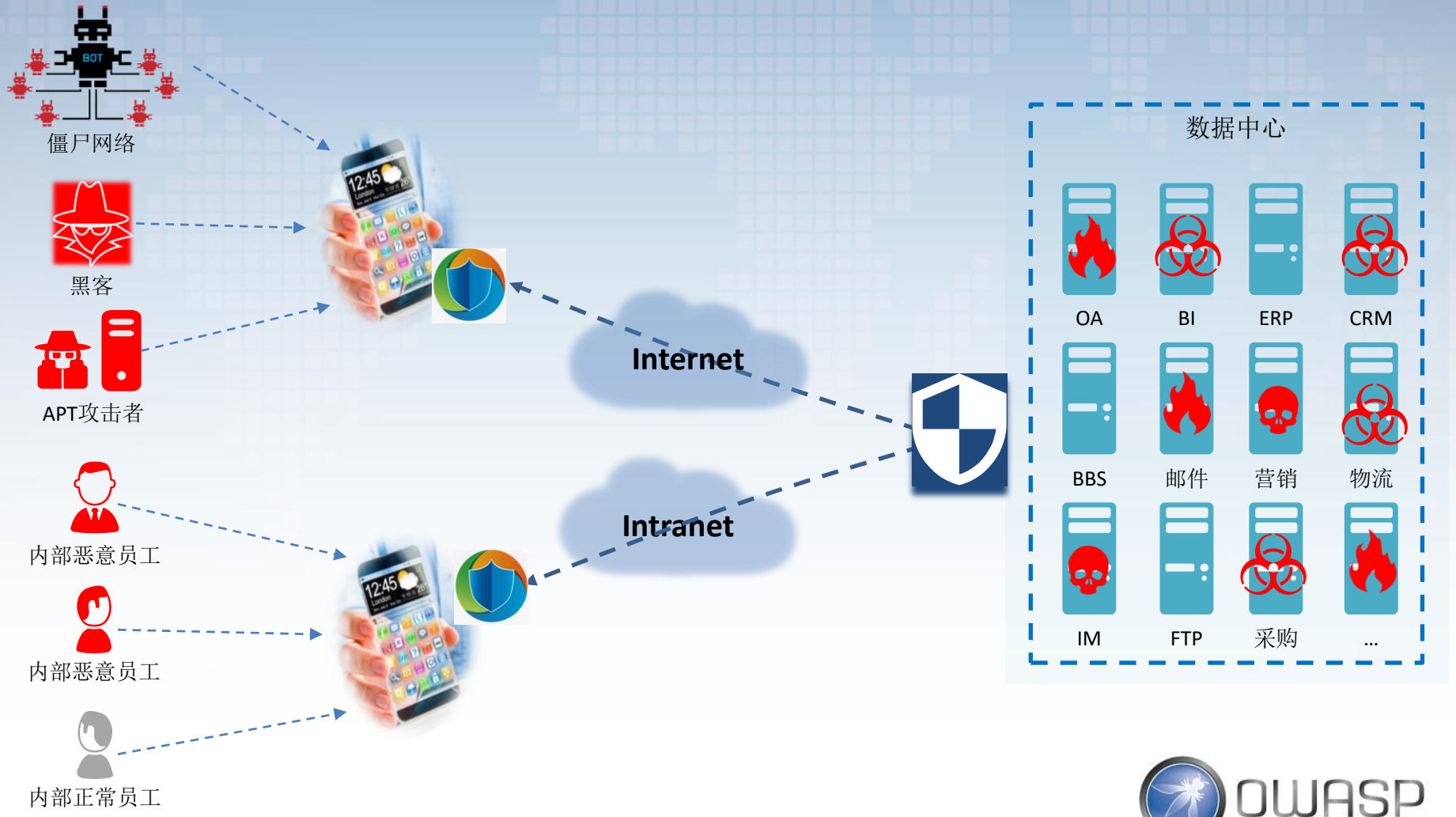
3 拦截攻击

4 威胁感知

5 精准溯源

OWASP
Open Web Application Security Project

下一代移动应用安全示意图



OWASP
Open Web Application Security Project

移动应用安全威胁感知

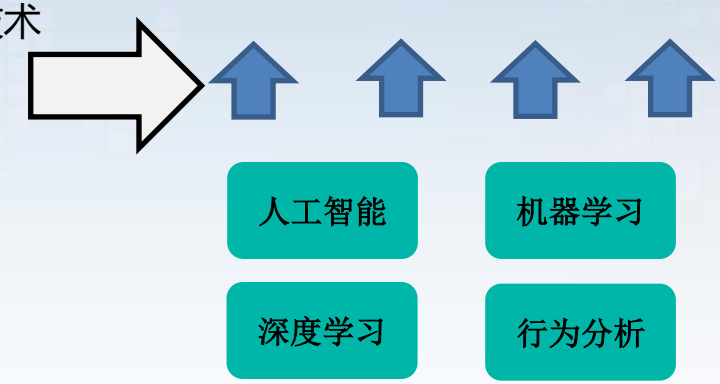
安全数据采集	威胁建模	威胁情报	安全策略及展示
硬件信息采集： 设备指纹、硬件信息、系统信息、应用信息、归属地、网络类型、行为信息等 **环境信息采集：** root/越狱、是否使用修改器框架、是否模拟器、是否存在病毒木马	针对已知威胁建模 自定义规则建模 利用大数据技术和人工智能技术进行自学习建模	全面分析设备、系统、移动应用等基本信息及程序运行、运行环境、攻击行为等威胁信息，对攻击时间、攻击来源、攻击目标、攻击手段等进行全面的统计分析、生成威胁情报	对恶意攻击行为的安全防御策略配置 采用可视化技术，形成威胁情报的态势图，借助态势可视化为安全管理人员提供辅助决策信息。

OWASP
Open Web Application Security Project

借鉴Gartner理念

1. CASB
2. 终端检测与响应（EDR）
3. 基于非签名方法的终端防御技术
4. 用户和实体行为分析（UEBA）技术
5. 微隔离和流可视性
6. DevOps安全
7. 情报驱动的安全运营中心
8.远程浏览器技术
9.伪装技术
10.普适信任服务

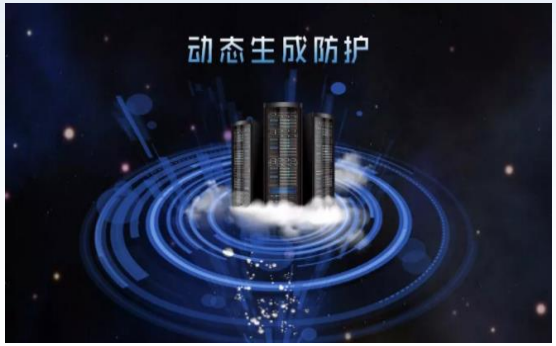
安全检测技术需要升级换代



OWASP
Open Web Application Security Project

下一代移动应用技术优势

- **纠缠感知**：实现了终端与服务端无地域、无边界、实时态势感知。
- **动态生成防护**：在收到威胁信号后，智能判定结果，自动生成防护方案。
- **自适应防护**：面对不同的场景，采用灵活的自适应安全防护方案。



挑战：移动应用安全+神经网络

手动挡

自动挡

自动驾驶

汽车的发展历史：“把人解放出来，自适应环境降低操作的故障”

自动驾驶汽车发展的挑战：“机器学习训练，但依赖于可信的、广覆盖的环境数据”

手工命令行部署

图形化界面部署

人工智能+深度学习
“自适应、自学习、自优化”

客服电话：400-831-8116

官方网址：www.tongfudun.com

商务合作：info@tongfudun.com

售后服务：service@tongfudun.com