0DAY与APT攻防

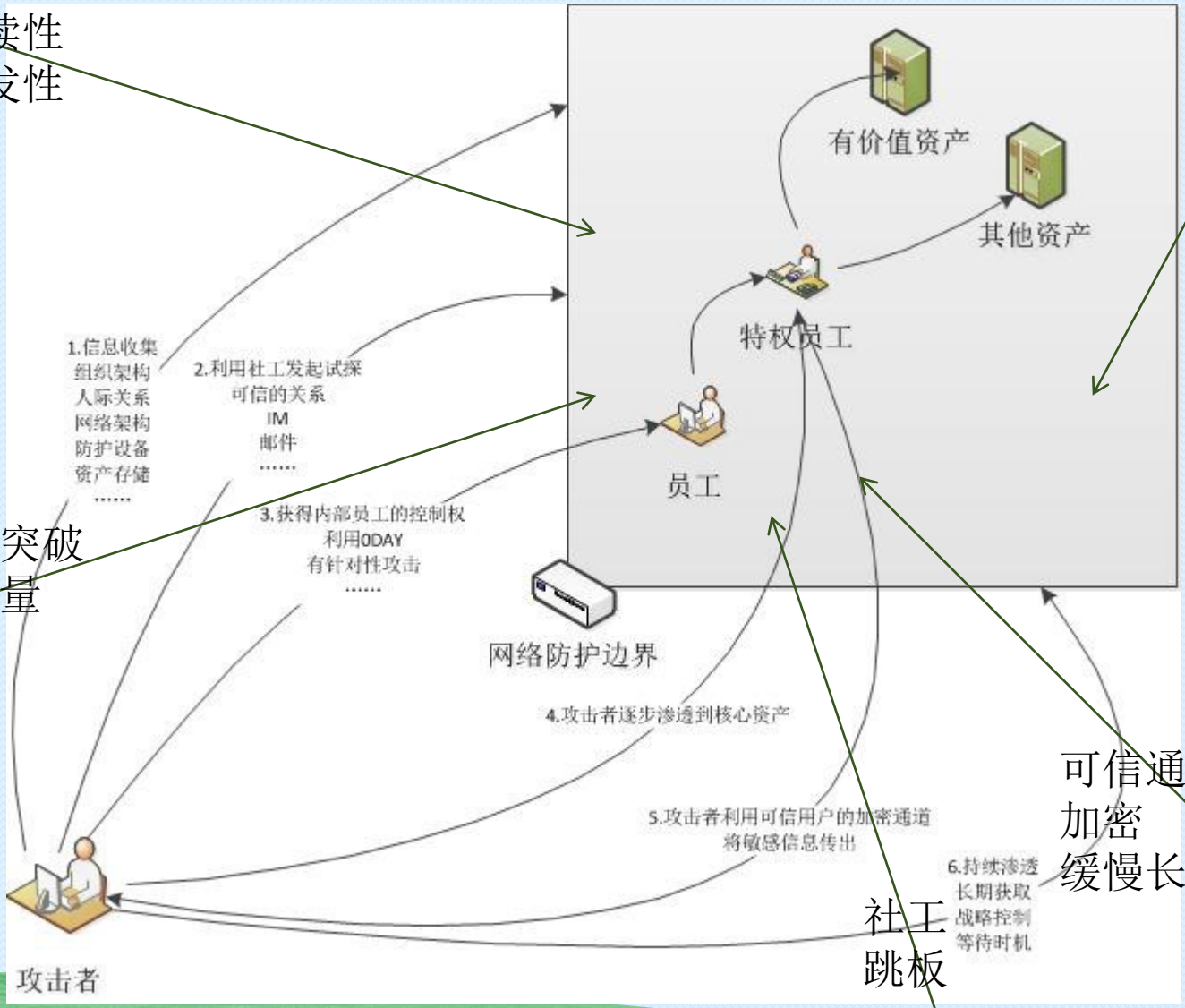
南京翰海源信息技术有限公司

APT攻击特性

持续性
同发性

长期窃取
战略控制
深度渗透

个人终端突破
多攻击向量
社工
0DAY



可信通道
加密
缓慢长期

社工
跳板

APT攻击的A分析

- 技术上的高级
  - oDAY漏洞
  - oDAY木马
  - 通道加密
- 投入上的高级
  - 全面信息的收集与获取
  - 针对的目标和工作分工
  - 多种手段的结合：社工+物理

0DAY漏洞利用

- 了解对方使用软件和环境
- 有针对性的寻找只有攻击者知道的漏洞
- 绕过现有的保护体系实现利用

0DAY特马

- 绕过现有防护
  - 了解环境下使用专门的对抗
  - 关闭防护
  - 绕过防护
  - 合法逃逸
- 云托管模式
  - 远程恶意模块

通道加密

- 模拟合法用户行为
  - 协议与软件端口
  - 配合用户行为同步
- 使用加密通道
  - 常见必开的协议如DNS
  - 合法加密的协议如HTTPS

社工

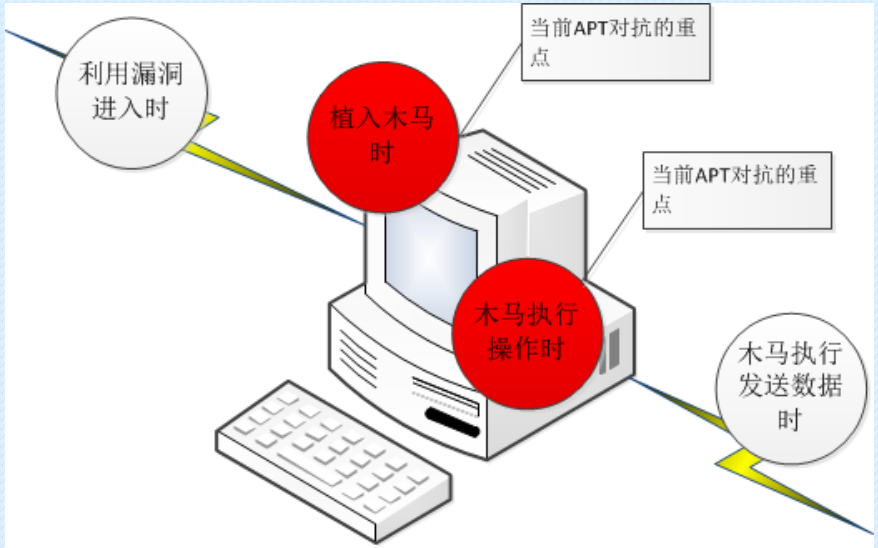
- 针对人的薄弱缓解与信任体系
- 攻击人的终端，利用人的权限获取
- 常见人的信息流通道的深度检测缺乏
  - 邮件
  - WEB访问
  - IM

APT防御：当前安全之痛

- 当前防御体系的问题
  - 基于已知知识
  - 基于规则
  - 基于信任
  - 缺乏对未知威胁的感知能力

  - 对抗点滞后
  - 缺乏关联分析能力

APT提出的挑战

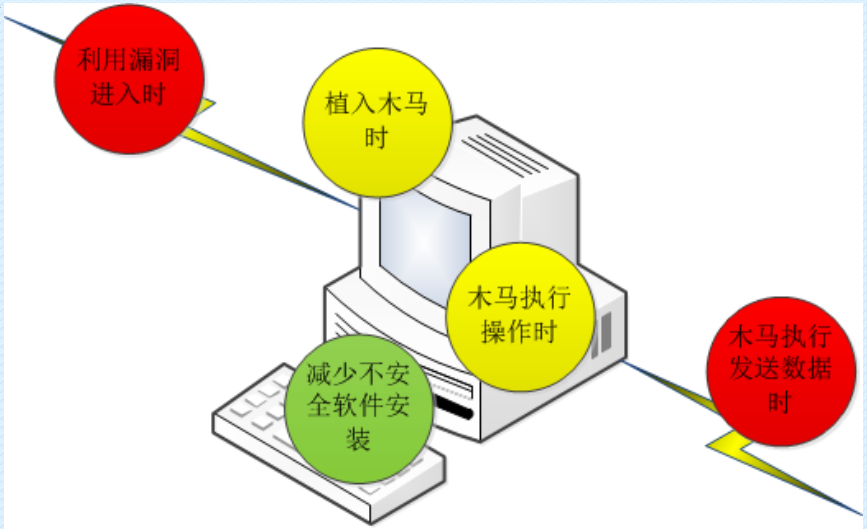


APT 检测与防御

- 降低应用自身漏洞
  - SDL
- 增强漏洞利用时实施检测
- 增强加密数据可信分析检测
- 形成纵深防线
  - 漏洞利用
  - 木马执行
  - 数据传输

思考：APT攻击的应对之道

- **加强漏洞进入时检测**
  - 攻击者唯一无力代码级对抗的检测点
  - 可以准确确定恶意行为的点
  - 挑战：如何检测未知漏洞利用？
- **加强木马执行发送数据点检测**
  - 窃密类木马的必然行为
  - 从链路可信级别分析
  - 挑战：识别加密链路可信性？
- **配合其他两个检测点，形成完整的纵深防御链条**



加强国外不可信软件与设备的安全检测与准入制度

让安全成为IT系统基础属性

- 现代IT系统是复合的
  - 自身可控部分的安全
    - 意识与能力
    - 安全开发
    - 安全验证
  - 自身依赖不可控部分的安全
    - 供应链安全保证：准入、保证、追责
    - 未知危害感知能力
  - 整体
    - 纵深的安全防御与监控体系
    - IT教育与培训体系

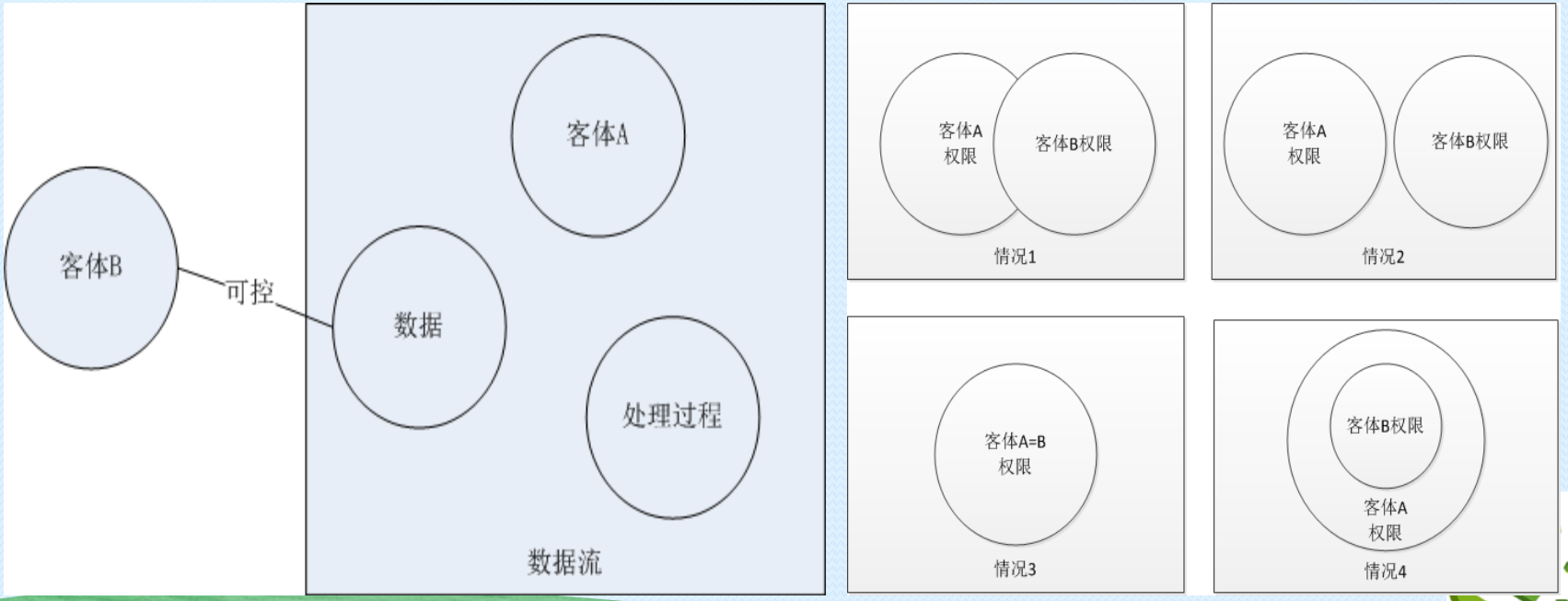
事前预防：安全测试&安全检测

- 以漏洞挖掘之手段，在系统上线或产品交付前，尽量保证其安全性的系统化行为
  - 覆盖性
  - 完备性
  - 可度量性

- 当前安全测试困境
  - 测试理论很难适用于安全领域
  - 安全测试基础理论薄弱,当前测试方法缺少理论指导，也缺乏技术产品工具

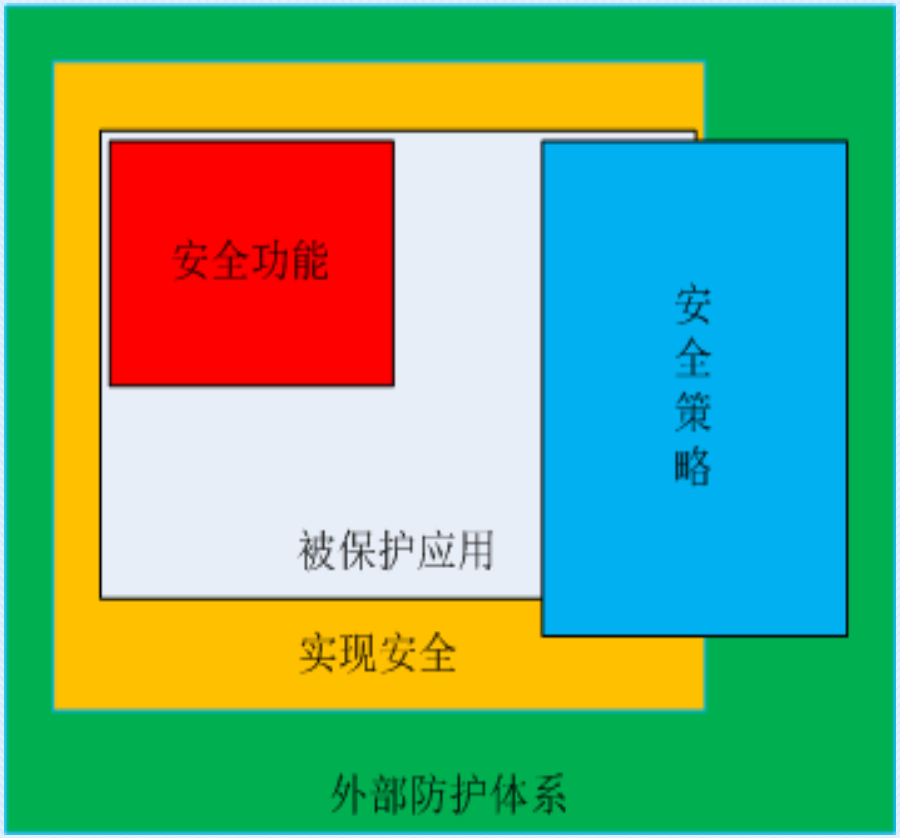
宏观安全分析的本质要素

- 宏观
  - 不同权限或能力的对象之间存在着对同一数据流的处理和控制权限
  - 权限的提升



安全语义分析的本质要素

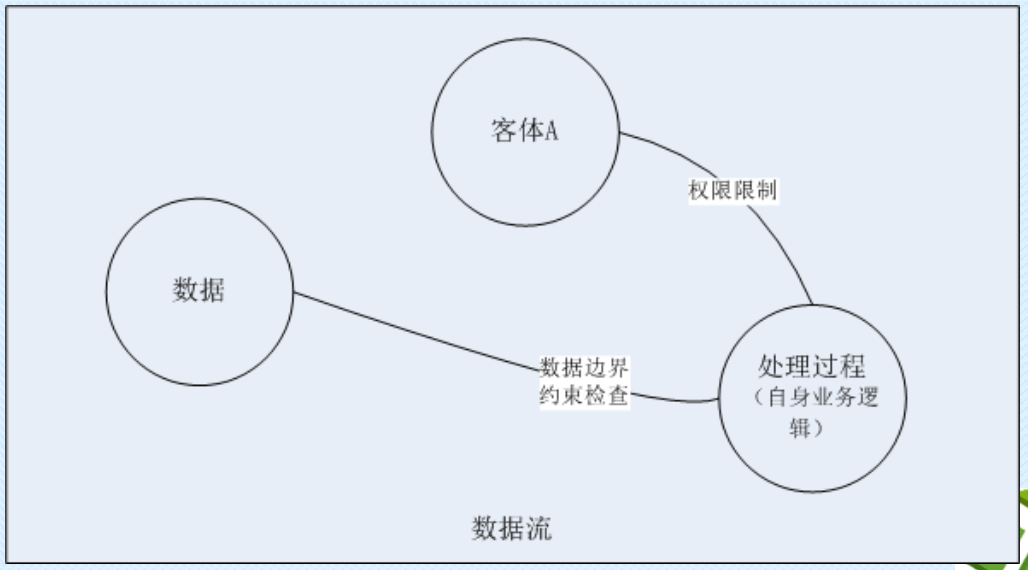
- 安全包括了三个层次
  - 安全功能（特性）
  - 安全策略（部署，配置，全局设计准则）
  - 安全实现



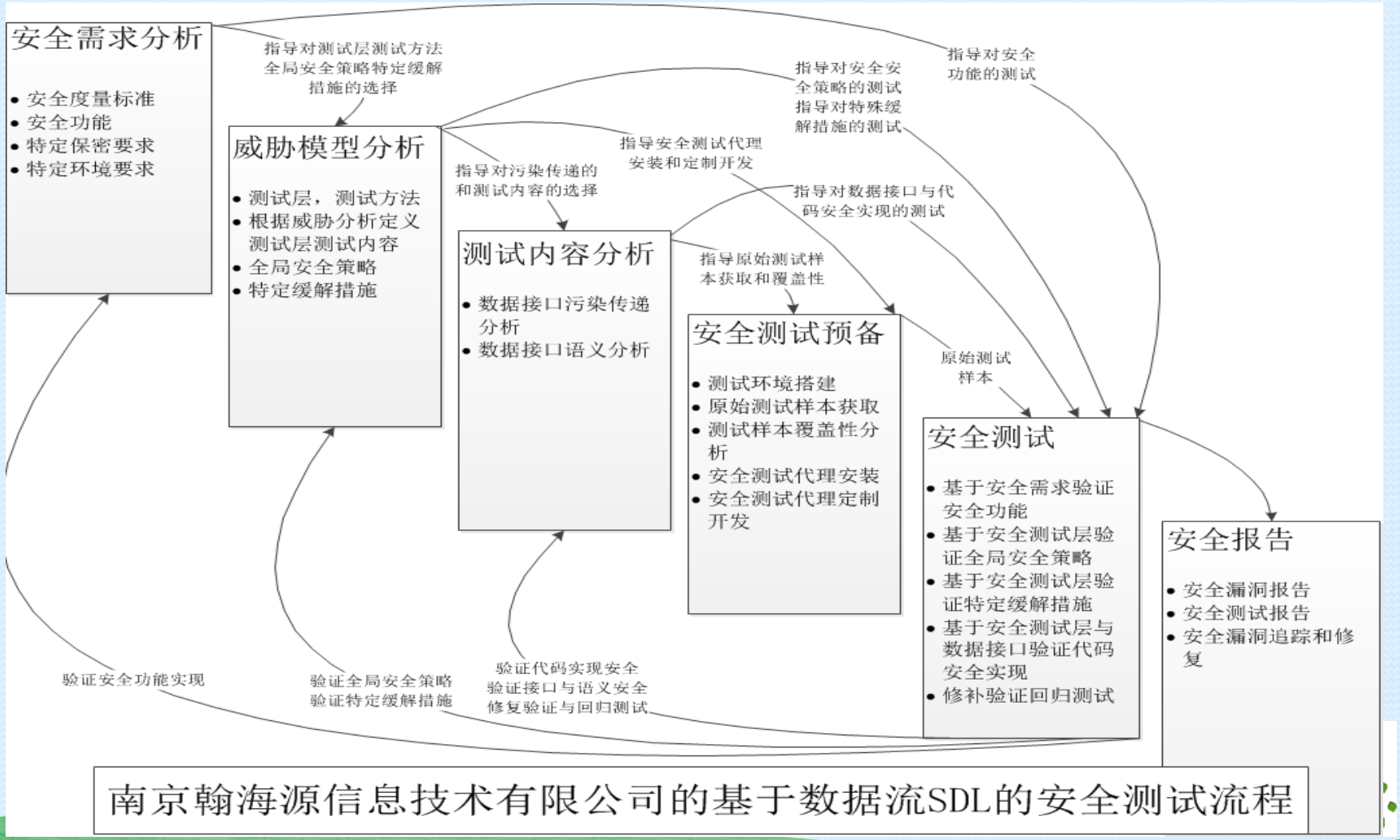
- 安全测试是对以上几个层次的验证和度量
- 外部防护系统是一种补充保护

安全微观分析的本质要素

- 程序本质是什么？
- 程序=数据流+数据处理+权限对象
  - 对数据流上的数据边界缺乏检查
  - 对客体权限本身缺乏限制
  - 逻辑处理错误



综合的安全测试方法论



APT攻击防御核心技术

- 基于漏洞（包括oDAY）攻击检测技术
  - 沙盒行为分析技术
  - 前置检测技术
    - 特征识别
    - 轻量虚拟机
  - NDAY漏洞识别引擎
- oDAY病毒木马检测技术
  - 沙盒行为分析引擎
  - 行为类似对比引擎
  - 智能学习与关联获取补丁

APT攻击防御核心技术

- 加密数据的可信性识别
  - 未加密协议通道
  - 加密协议通道
- 纵深防御体系
  - oDAY漏洞触发：进入点，对抗好，可判性强
  - oDAY特马检测：对抗性高，自动化学习
  - 加密链路识别：
  - 智能事件关联与分析

演示

Q/A