新型媒体建设中的信息安全管控

演讲人：谭晓生

职务：奇虎360 副总裁，首席隐私官

日期：2015年6月17日

媒体被黑客攻击事件


Warning
We've aire
We contin
We've obt
If you dor
Determin
Data Lin
ht
ht
ht
ht
http://
2

攻击的目标

- 个人计算机
- 个人移动终端（手机、平板电脑、电子阅读器）
- 服务器
- 工业控制系统/嵌入式系统
- 物联网传感器/智能机器
- 网络设备/信息传输装置
- 云计算系统

为什么这些目标会被攻破？

- 计算机体系结构的天然缺陷
- 网络通信协议的缺陷
- 管理制度的缺陷
- 人的缺陷

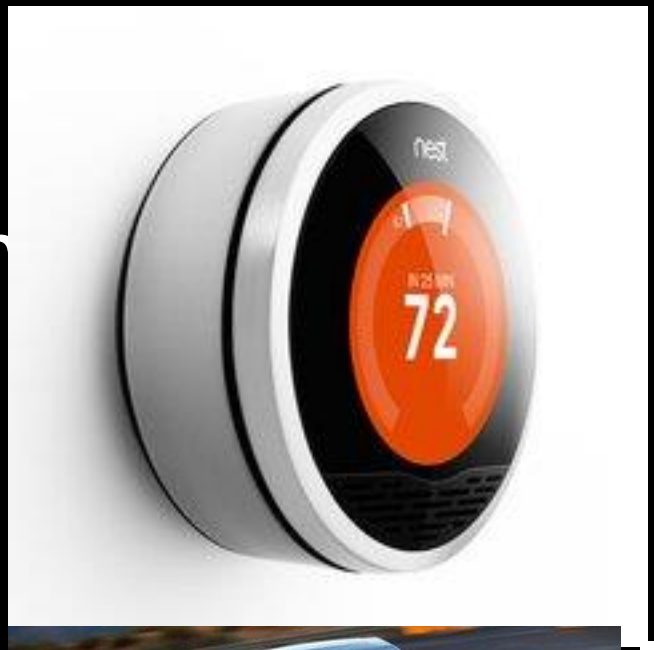
系统漏洞现状

终端 办公系统	操作系统	Windows XP、Windows Vista、Windows7、Windows8、IOS 等
	应用系统	Office、WPS、Acrobat、浏览器、即时通讯工具、下载工具、播放器 图片处理工具、邮箱客户端、在线炒股客户端、在线游戏客户端等
	BYOD	iPhone、iPad、HTC、三星、Nokia、Microsoft 等
业务 支撑系统	操作系统	Windows Server 2003、Windows Server 2008、WinCE AIX、HP-UNIX、Solaris、FreeBSD、Linux系列
	应用系统	Oracle、SQL Server、Web Logic、ERP、BPM、OA 工业控制系统、其他业务软硬件系统
网络 基础设施	网络设备	交换路由设备、网络运维设备、网络安全设备
	Wifi	AP、AC

- 每年会发现数千个**0DAY**漏洞

万物互联的后移动互联网时代

- Google收购Nest
- Apple推出iWatch
- Jawbone
- 小米路由器
- Tesla电动车
- 能上网的电冰箱
- 智能医疗设备
- ……



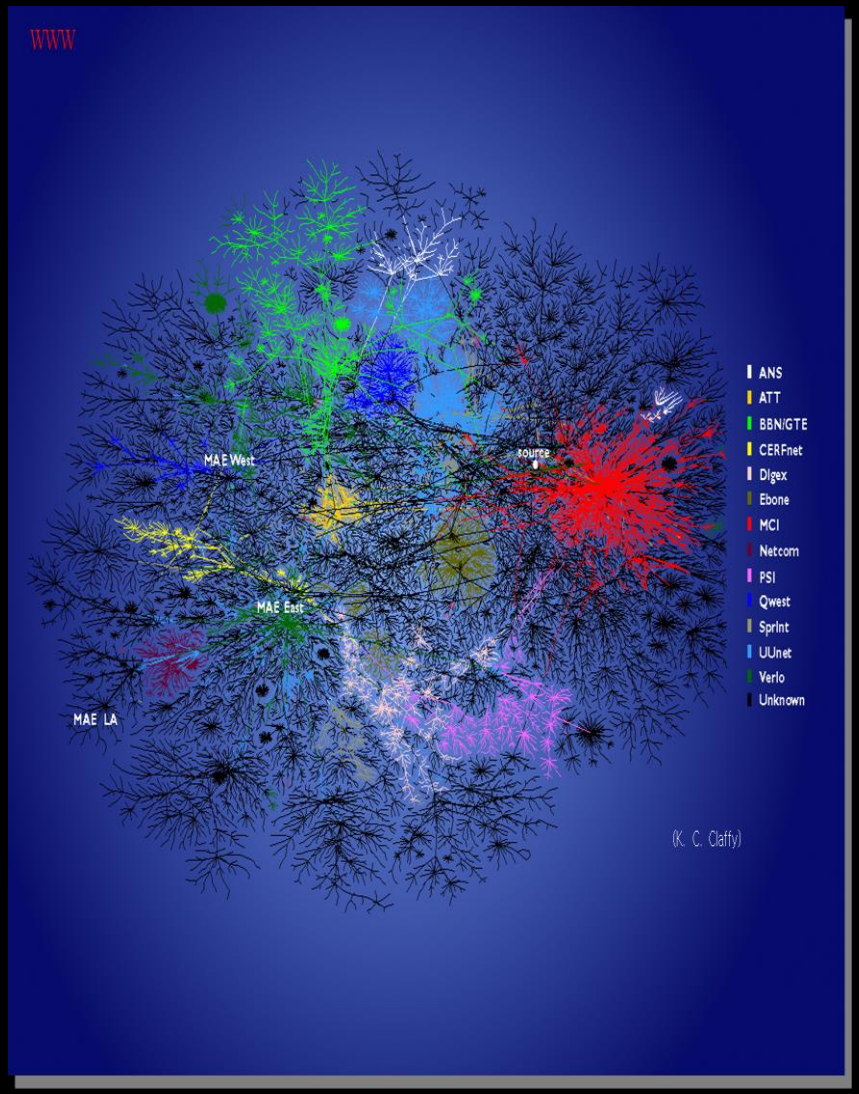
万物皆成为黑客破解的对象

- 2014Defcon上黑客演示45分钟破解2种硬件设备
- SyScan360上黑客破解Tesla电动车
- 2013年家用路由器被黑风波
- USB Firmware被重写的问题

传统的意识：安全即边界

- 防火墙
- IPS
- IDS
- UTM
- VPN
- ……

传统的意识：安全即边界



- 互联网的本质是什么？
- 云计算对网络边界的冲击
- 移动应用对网络边界的影响
- 智能硬件对网络边界的影响
- 现在的世界是一个无边界网络。
- 随着网络的泛化和无边界化
- 边界思想越来越不适应整个网络发展的现状

企业信息安全边界在哪里？

- 企业网站
- 企业Wifi
- BYOD
- 智能硬件设备
- 供应链
- 互联网路由
- ……

安全体系的演化

早期的P2DR安全模型

本质：安全就是响应+防护的安全运维体系

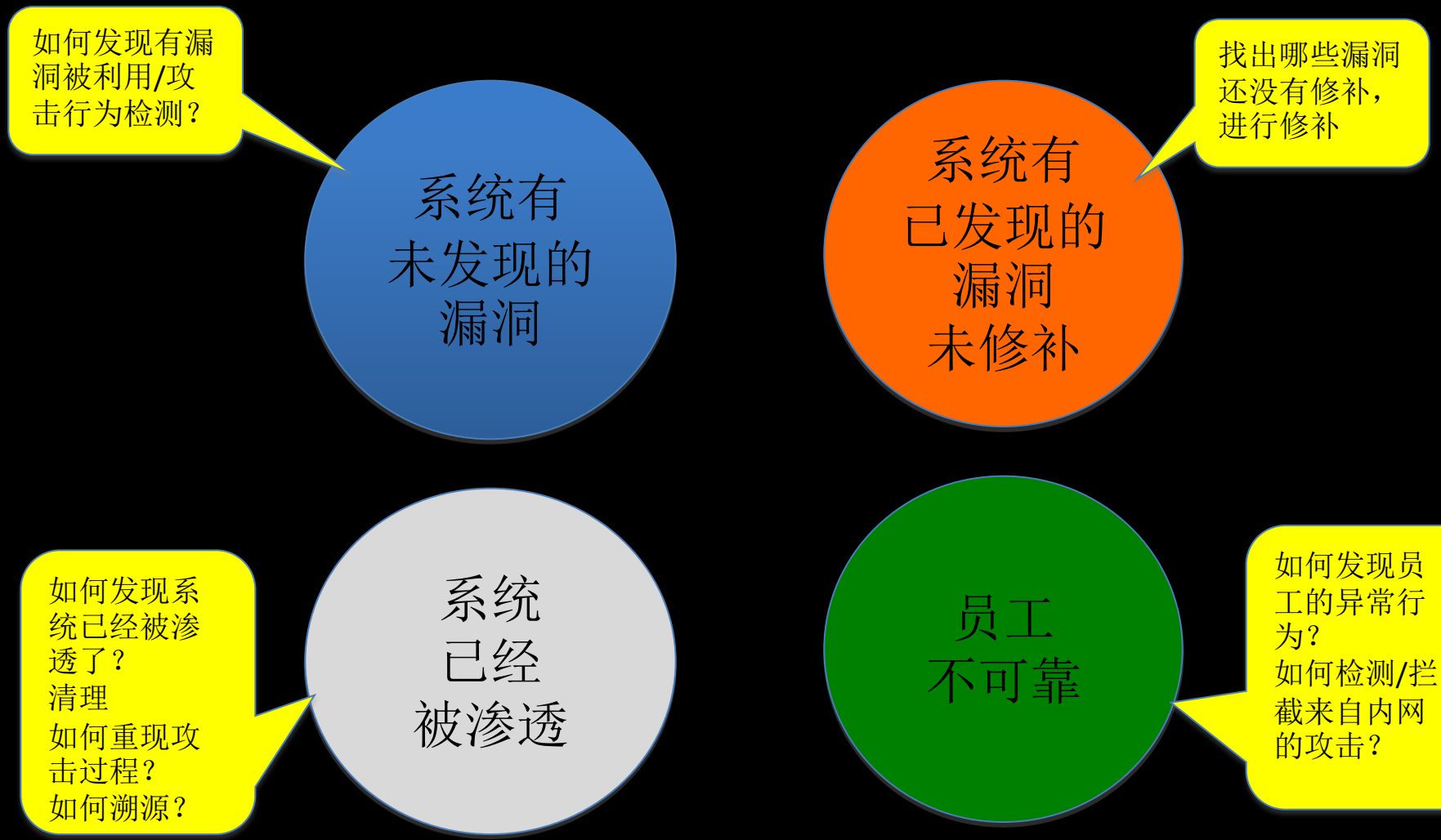
后来的安全木桶理论

本质：安全就是用安全产品堆砌出来的线式防御体系

流行的立体防御体系

本质：安全就是分层的、分级的多层次防护体系

安全——4个重要假设


如何发现有漏洞被利用/攻击行为检测？
系统有未发现的漏洞
找出哪些漏洞还没有修补，进行修补
系统有已发现的漏洞未修补
如何发现系统已经被渗透了？
清理
如何重现攻击过程？
如何溯源？
系统已经被渗透
员工不可靠
如何发现员工的异常行为？
如何检测/拦截来自内网的攻击？

安全理念：三个阵地


• 产品
• 对外服务
• 员工
争夺边境线
• 重要服务器
• 重要业务系统
• 重要数据
保卫大城市
• 监控
• 审计
• 大数据分析
反潜伏
第一道防线
第二道防线
第三道防线

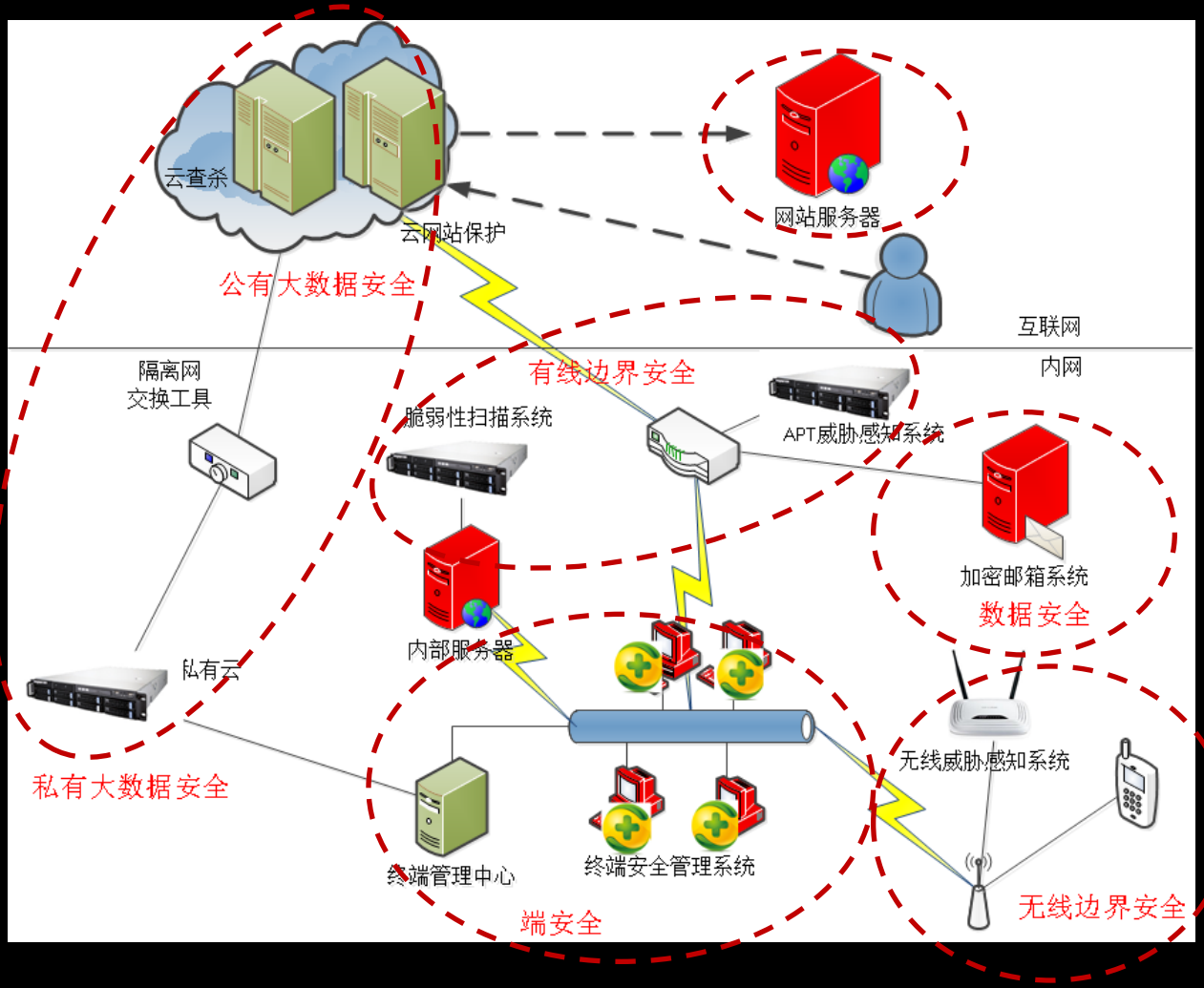
新安全模型：云+管+端

云端
- 攻击行为学习
- 攻击模型提取
- 漏洞检测
- 攻击行为鉴定

终端
- 统一管控
- 多维信息提取
- 软件准入
  非白即黑
- 主动防御

管道
- 网关防护
- 准入控制
- 流量侦听

新的安全边界在哪里？


云查杀
云网站保护
网站服务器
公有大数据安全
互联网
内网
隔离网
交换工具
有线边界安全
脆弱性扫描系统
APT威胁感知系统
加密邮箱系统
数据安全
内部服务器
私有云
私有大数据安全
无线威胁感知系统
终端管理中心
终端安全管理系统
端安全
无线边界安全

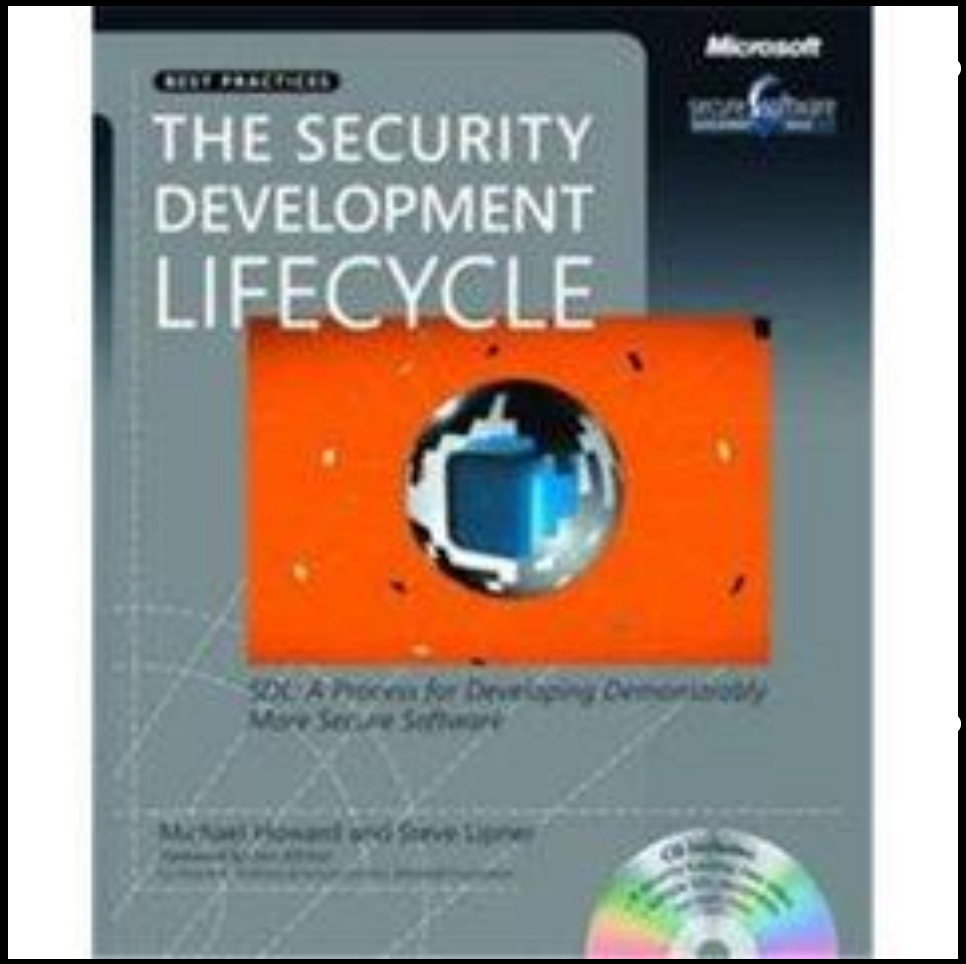
新的安全边界在哪里？

- 端
  - PC机
  - 手机
  - 智能终端
- 网络（边界、管道）
  - 出口路由器
  - 核心交换机
  - 各种网络安全设备
- 云计算基础架构

可供借鉴的历史—漏洞披露

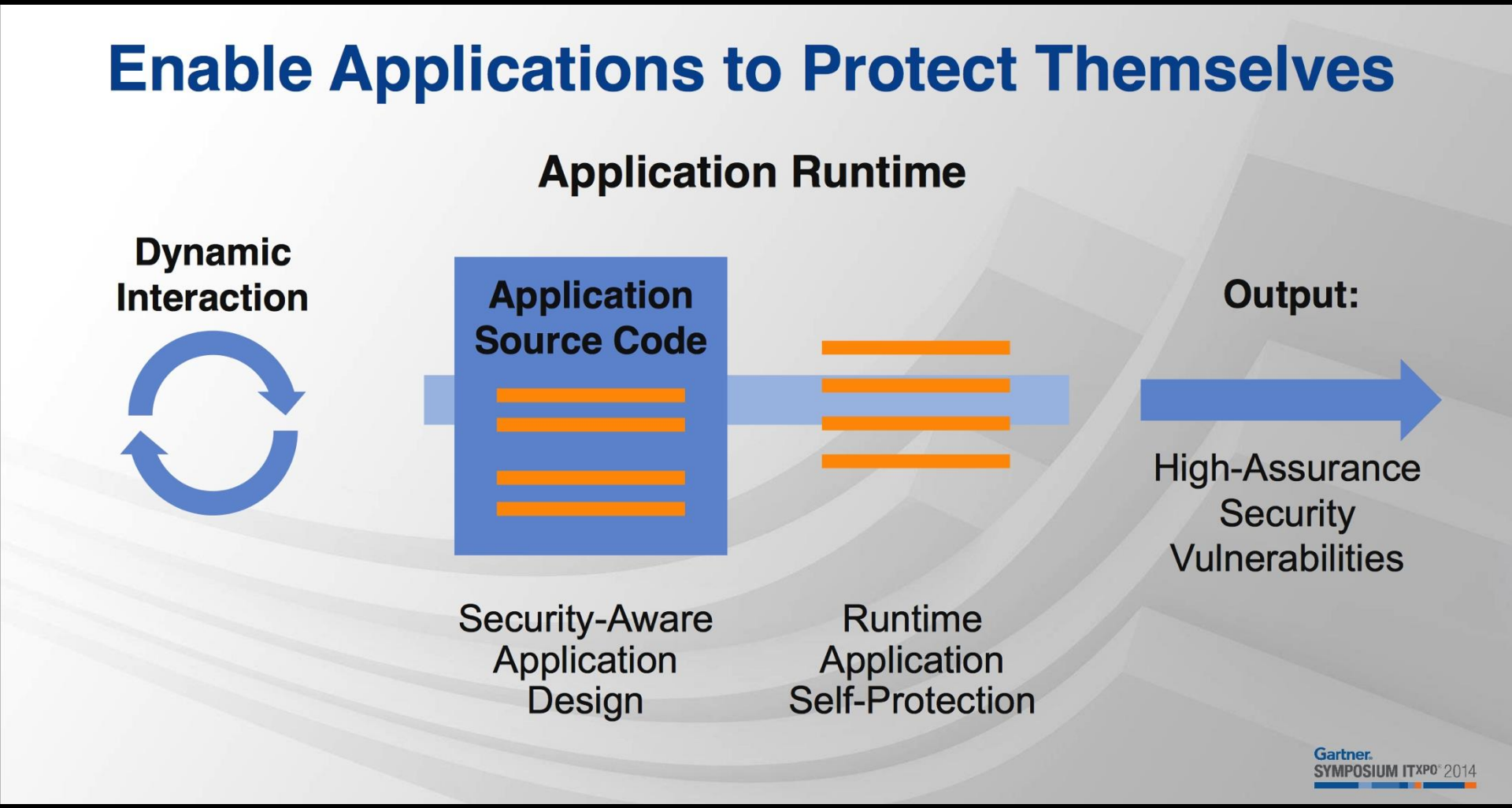
- 国家信息安全测评中心
- 乌云漏洞报告平台
- 360库带计划

可供借鉴的历史



- 软件的脆弱性是如何改进的？
  - 安全开发周期，即Security Development Lifecycle (SDL)
- Web安全的脆弱性是如何改进的？

系统应该可以自我保护


Enable Applications to Protect Themselves
Application Runtime
Dynamic Interaction
Application Source Code
Output:
High-Assurance Security Vulnerabilities
Security-Aware Application Design
Runtime Application Self-Protection
Gartner SYMPOSIUM ITXPO 2014

Thanks!