对企业面临安全挑战的思考

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- About Me
  - 杨黎
  - 用友软件股份有限公司 集团UAP中心
  - yanglih@yonyou.com

用友
yonyou

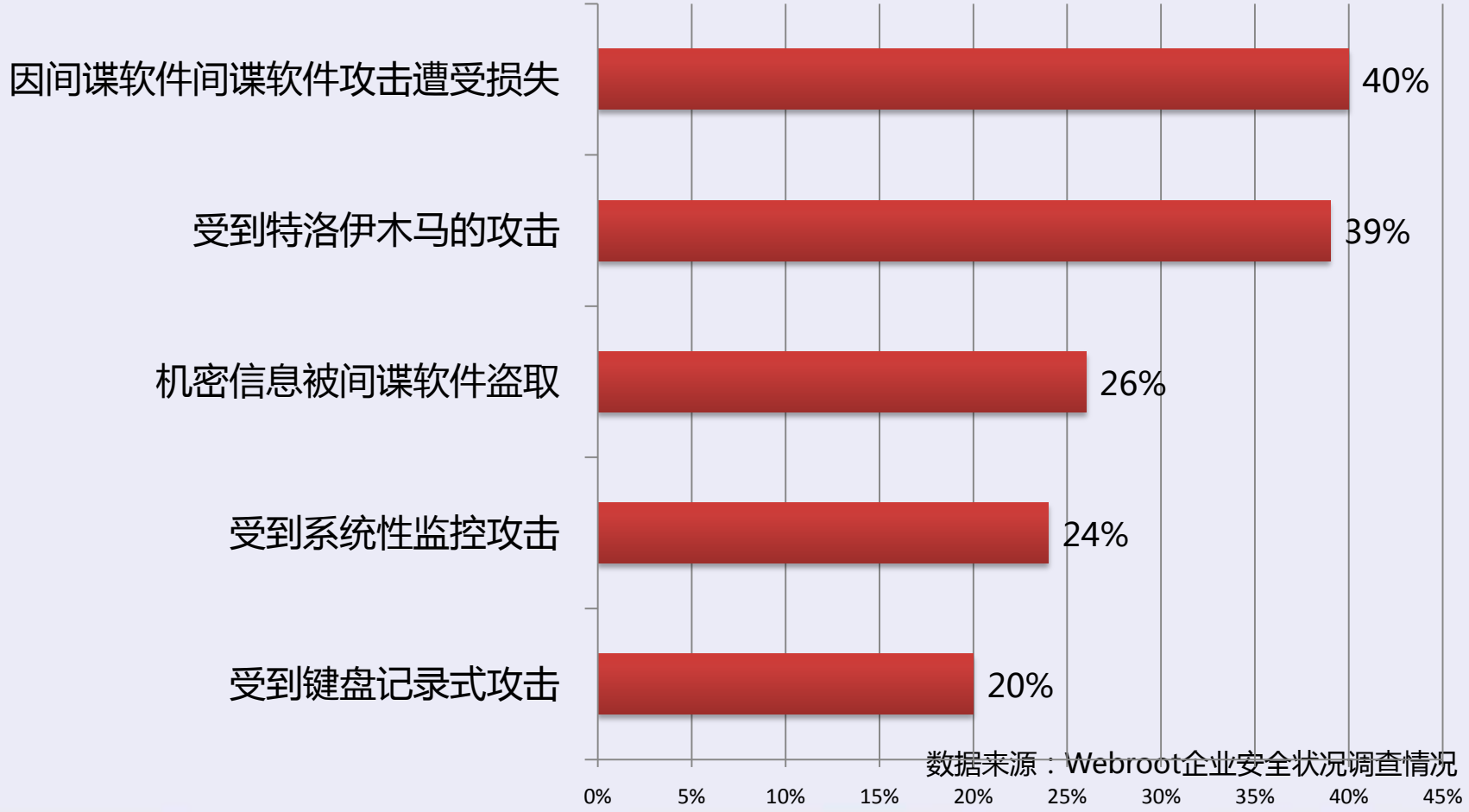
OWASP 中国
The Open Web Application Security Project

企业面临哪些安全挑战?

企业面临的安全挑战

OWASP 中国
The Open Web Application Security Project

- 企业外部信息安全威胁

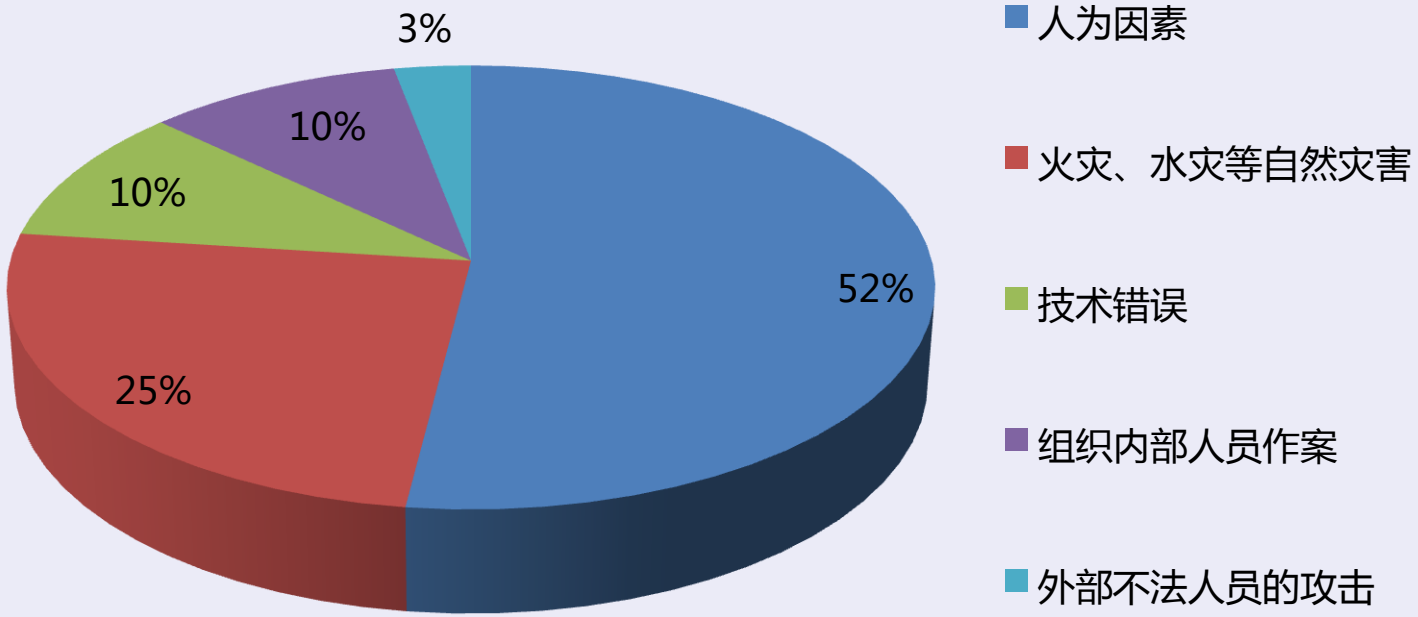


数据来源：Webroot企业安全状况调查情况

企业面临的安全挑战

OWASP 中国
The Open Web Application Security Project

- 企业内部信息安全威胁

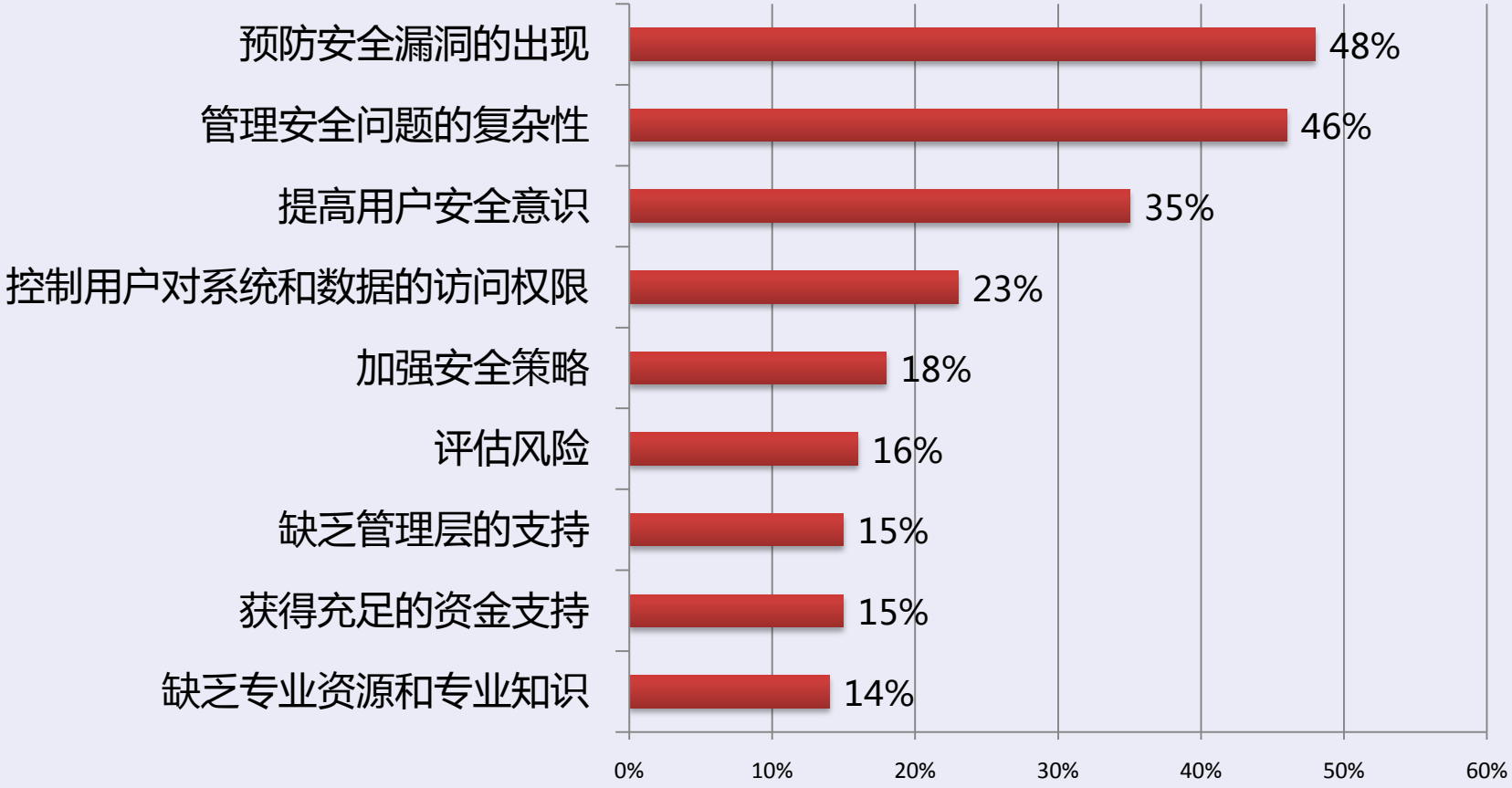


数据来源：国家计算机应急响应中心

企业面临的安全挑战

OWASP 中国
The Open Web Application Security Project

- 企业面临的最大安全挑战



数据来源：《InformationWeek》和埃森哲咨询公司合作进行的“全球信息安全调查”

企业面临的安全挑战

OWASP 中国
The Open Web Application Security Project

- 合规
- 新技术带来的安全问题
  - 提高生产力必须支持移动
  - 提高业务灵活性、降低成本寄望于云
  - 社交媒体

OWASP 中国

The Open Web Application Security Project

软件产品安全保证

软件产品安全保证

OWASP 中国
The Open Web Application Security Project

- 软件产品安全保证过程
  - 采用安全开发生命周期SDL

OWASP 中国
The Open Web Application Security Project

- 应用软件安全框架

合规

安全目标 OWASP	等级保护	审计

身份和访问管理

身份管理	访问控制	认证和单点登录

基础设施安全

通信安全	数据安全	前端安全	安全日志

软件生命周期安全

安全开发生命周期	安全交付	安全配置	安全服务

软件产品安全保证

OWASP 中国
The Open Web Application Security Project

- 应用软件安全特性

通信安全
- HTTPS
- 专有通信加密

访问控制

网络安全架构

移动设备安全

数据安全

会话管理

资源控制

安全策略

移动设备管理

移动应用管理

软件安全保证
- 编码安全
- 安全评估
- 安全标准
- 自动化代码扫描

认证和单点登录

授权和角色管理

日志和监控、审计

软件产品安全保证

OWASP 中国
The Open Web Application Security Project

- 开放的软件框架支持安全合作伙伴
  - 数字证书
  - 动态口令
  - 加密机
  - ……

软件产品安全保证

OWASP 中国
The Open Web Application Security Project

- 安全以企业业务为本
  - 提供以业务对象为中心的日志：记录对业务对象的操作；记录业务对象变化前和变化后的内容
  - 风险可管理
  - 合规支持
    - 信息安全等级保护
    - 企业内部控制基本规范
    - SOX
    - ISO 2700X
    - ……

企业做了什么?

企业做了什么

OWASP 中国
The Open Web Application Security Project

- 已经做了合理的安全域规划
  - 专用的防火墙
  - 严格的访问控制
  - 外网、内外、DMZ

企业做了什么

OWASP 中国
The Open Web Application Security Project

- 已经建立了有效的安全策略
  - 复杂的密码策略
  - 双因子认证
  - ……

企业做了什么

OWASP 中国
The Open Web Application Security Project

- 已经建立信息系统安全管理
  - 安全管理制度
  - 安全管理机构
  - 人员安全管理
  - 系统建设管理
  - 系统运维管理

- 为安全做了这么些事情是否足够了？

一个事例……

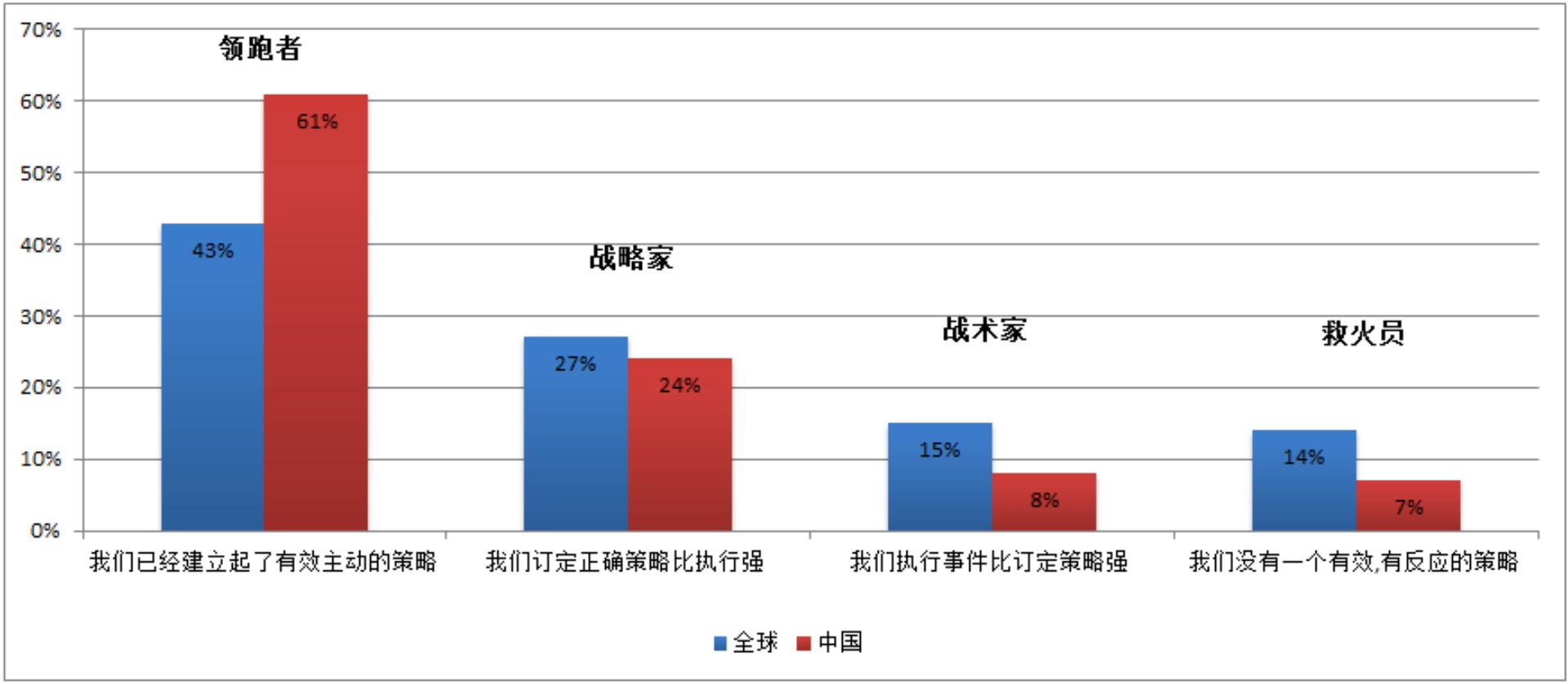
OWASP 中国
The Open Web Application Security Project

思考：企业的安全困境

思考：企业的安全困境

OWASP 中国
The Open Web Application Security Project

- 自信的企业



数据来源：普华永道2012年全球信息安全调查

思考：企业的安全困境

OWASP 中国
The Open Web Application Security Project

- 企业的现实问题
  - 人员、流程及技术在安全方面的结合
  - 安全专业人员
  - 安全投资
  - 维护成本
  - 业务增长与灵活性
  - ……

思考：企业的安全困境

OWASP 中国
The Open Web Application Security Project

- 没有安全意识很可怕
- 有了安全意识也会出现可怕的事情
  - 过于自信
  - 依赖工具
  - 知识匮乏
  - 经验不足
  - ……

因为有“人”就会有这样的问题

思考：企业的安全困境

OWASP 中国
The Open Web Application Security Project

所以我们思考如何减轻企业在安全上的负担。

如何让企业做安全时不再感觉是在买“保险”？

减轻企业安全负担

OWASP 中国
The Open Web Application Security Project

- 产品安全配置管理
  - 统一的安全配置管理
  - 提高默认安全配置的安全级别
  - 将一些可选项变为强制
  - 提供多种不同安全级别的预制配置供选择

企业评估目前的安全状态

OWASP 中国
The Open Web Application Security Project

- 安全检查
  - 安全配置检查
  - 补丁检查
  - 关键代码

提供企业提高自身安全的方法

OWASP 中国
The Open Web Application Security Project

- 安全知识库
- 安全工具
- 问题报告
- 漏洞修复
- 安全服务

用友提出的企业信息安全框架

安全管理

- 安全合规
- 安全策略管理
- 风险管理

安全运维

安全事件管理

- 安全事件监控
- 安全事件响应
- 安全事件审计

安全检查

合作和沟通

- 安全外包服务
- 安全问题报告

安全技术

物理安全

- 环境安全
- 设备安全

主机安全

- 安全配置
- 补丁管理
- 防病毒

网络安全

- 安全的网络架构
- 访问控制
- 入侵检测
- 防火墙
- 传输安全
- DOS防御

应用安全

- 身份管理
- 访问控制
- 日志和监控
- WEB应用安全
- 应用安全管理
- 安全开发生命周期
- 业务流程安全

数据安全

- 数据加密
- 数据泄露保护
- 抗抵赖
- 数据归档
- 灾难备份
- 数据安全删除

终端安全

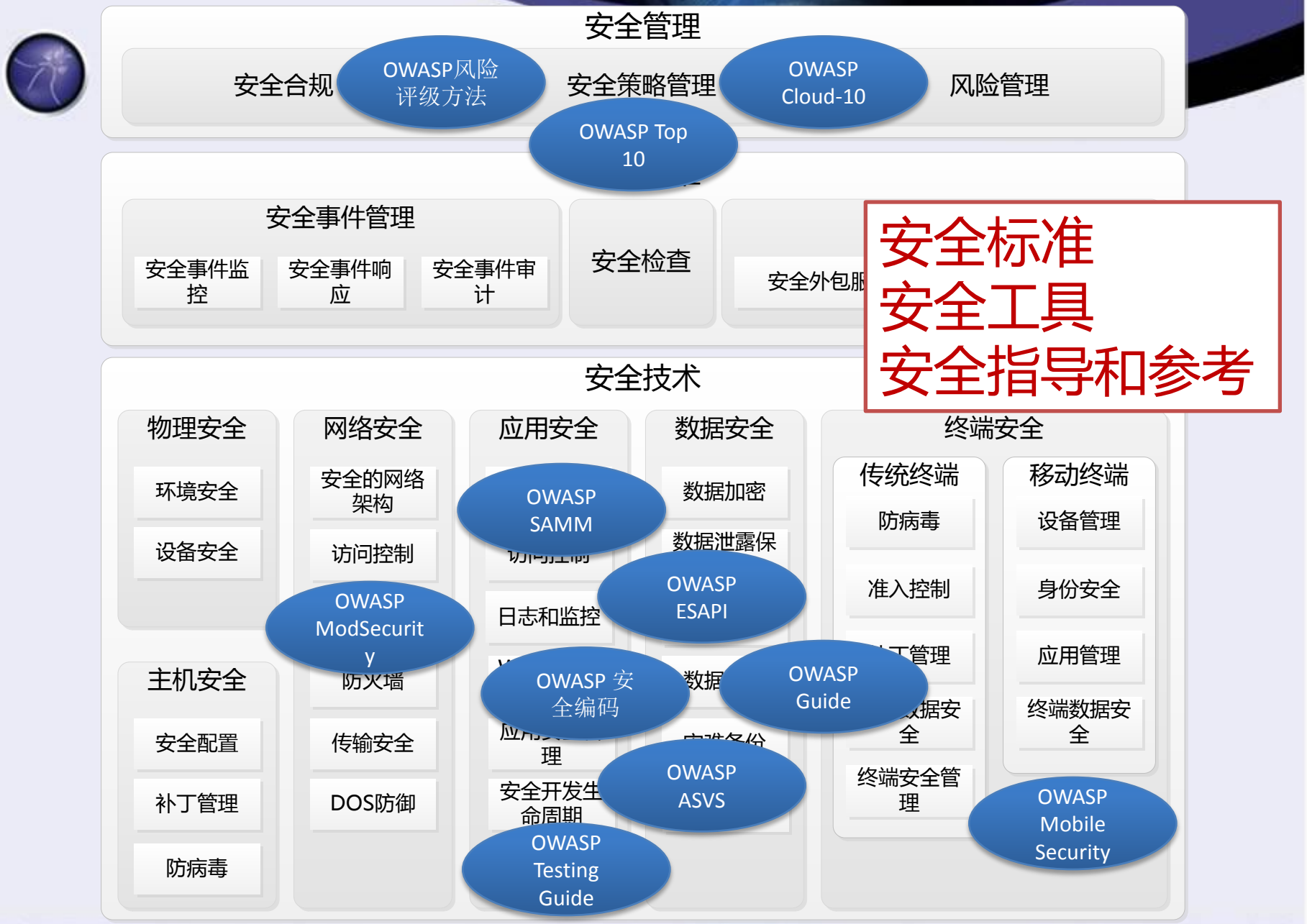
传统终端

- 防病毒
- 准入控制
- 补丁管理
- 终端数据安全
- 终端安全管理

移动终端

- 设备管理
- 身份安全
- 应用管理
- 终端数据安全

安全框架结合OWASP项目



未来

OWASP 中国
The Open Web Application Security Project

- 安全智能化？
- 支持SIEM？

OWASP 中国
The Open Web Application Security Project

感谢大家

期待与各位携手为企业共筑安全

www.yonyou.com

用友
yonyou