ThoughtWorks®

2016技术雷达峰会

技术雷达 之 构筑软件安全DNA

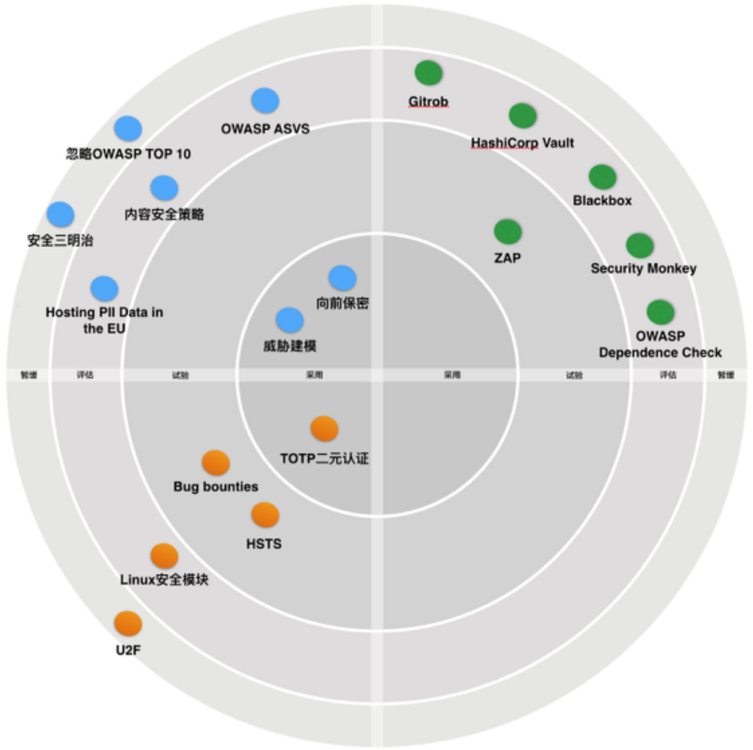
韩锴，ThoughtWorks Lead Consultant

安全风险与日俱增

3,930 次已知数据泄漏事件

736,000,000 条记录遭遇泄漏

技术雷达对安全领域的关注

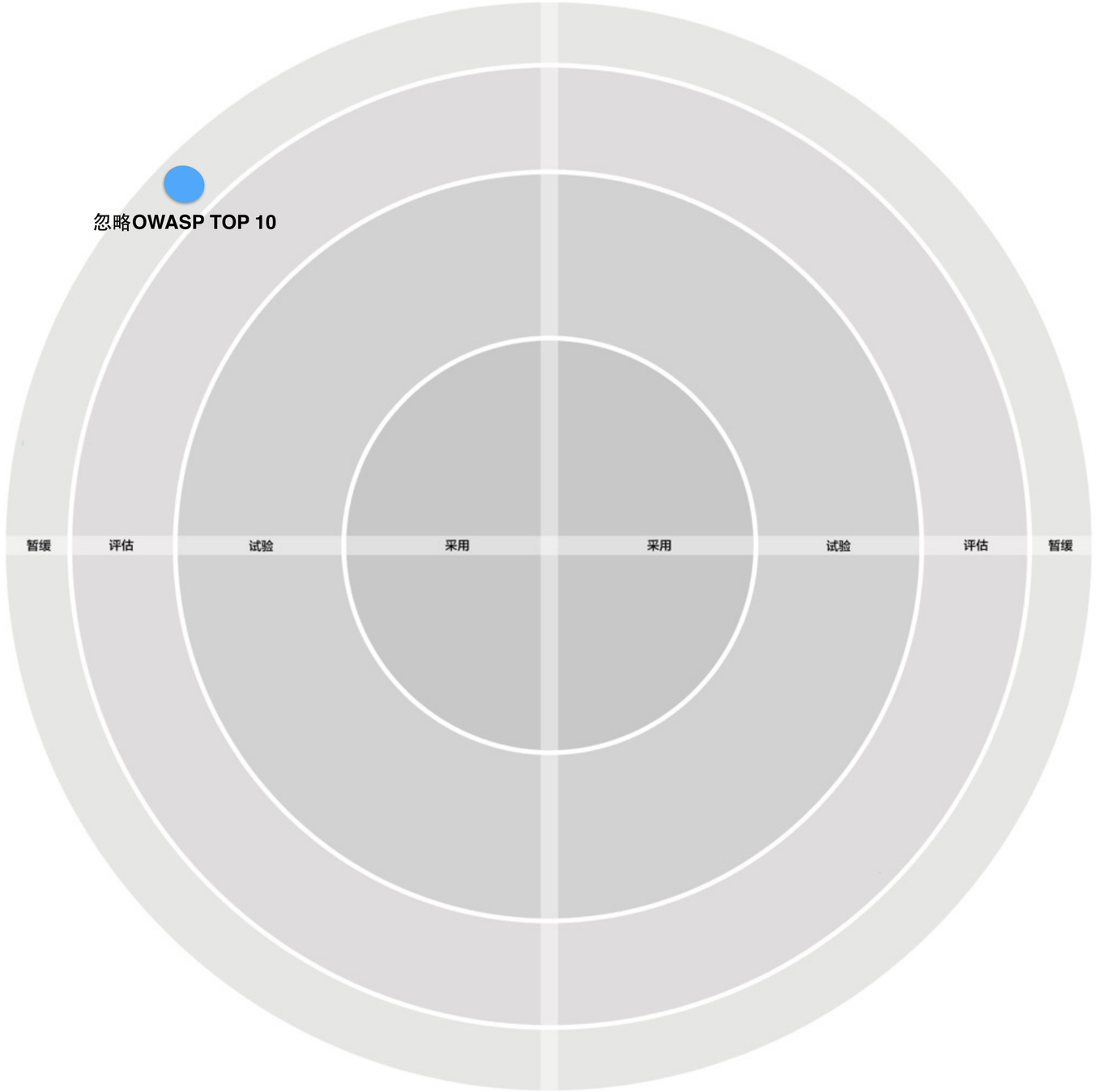


2015.05

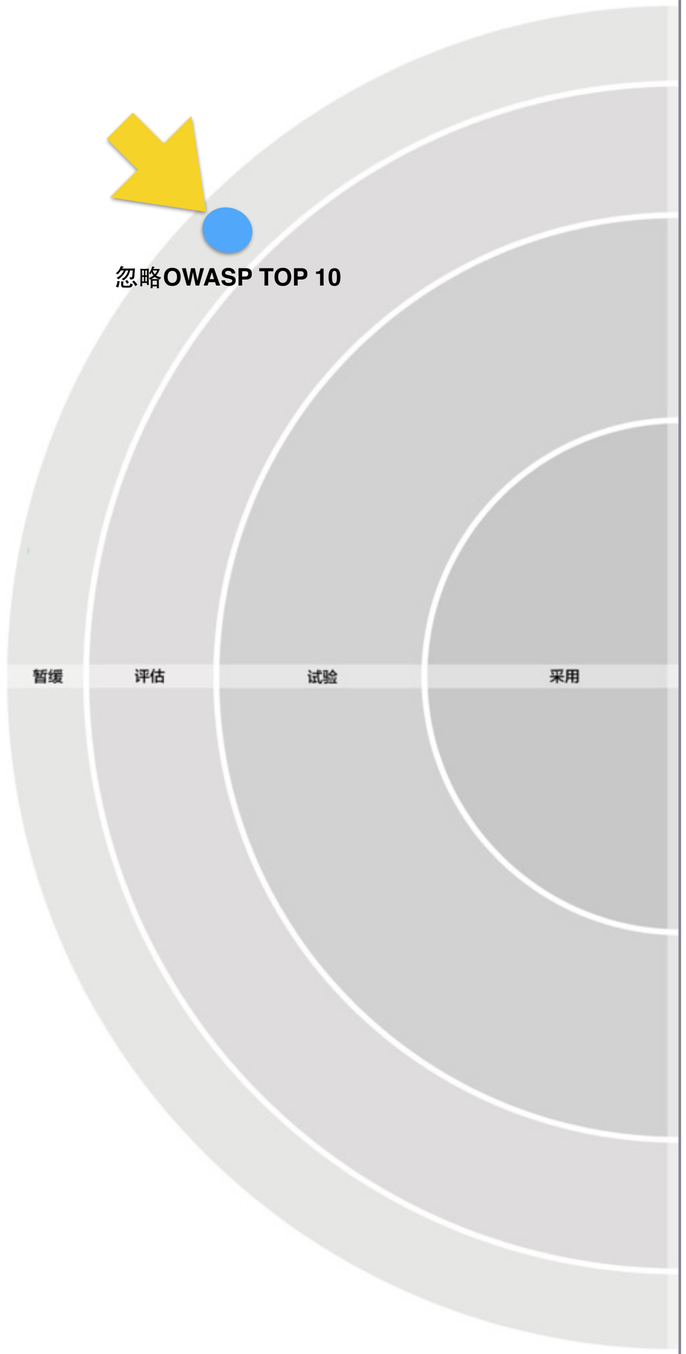
尽管在安全和隐私方面的关注度有所增加，但上次雷达发布之后业界在这个领域并没有多大进展，我们将继续强调这个问题。开发者方面有所响应，他们增强了安全基础设施和工具，把类似Zed Attack Prox之类的自动化测试工具构建到部署流水线中。当然这类工具只能算整个安全方案中的一部分，我们相信所有的企业组织都需要在这个领域提高水平。

2015.11

在软件开发生命周期中，安全是一个独一无二的会影响到所有角色的问题。我们在上一期雷达中着重指出了安全领域的一些改进，很高兴在很多团队中已经开始把安全实践结合在软件开发的生命周期中。这一期我们同样突出了这方面的创新，比如Bug bounties、安全建模、HSTS,TOTP和Let's Encript。我们希望这种提升的势头能够继续。



2014.01

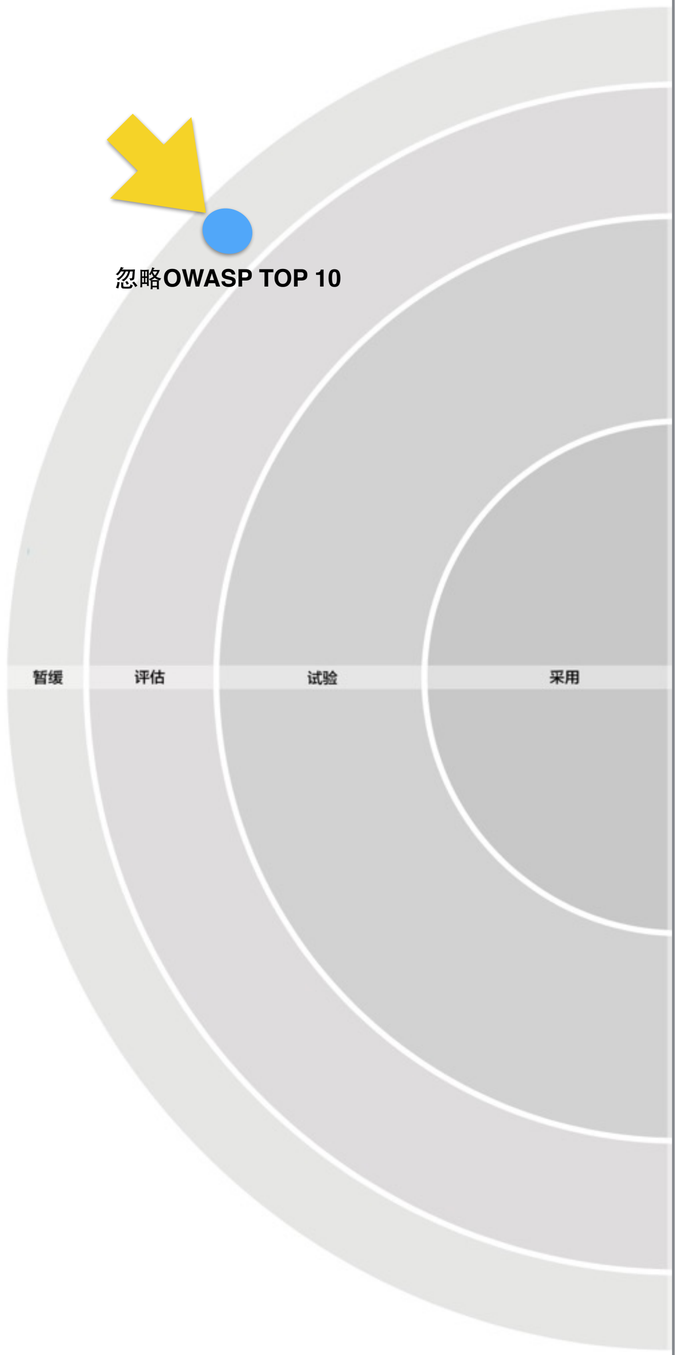


2014.01

OWASP
The Open Web Application Security Project

暂缓： 忽略OWASP TOP 10

OWASP Top 10 – 2010 （旧版）	OWASP Top 10 – 2013 （新版）
A1 – 注入	A1 – 注入
A3 –失效的身份认证和会话管理	A2 –失效的身份认证和会话管理
A2 – 跨站脚本（XSS）	A3 –跨站脚本（XSS）
A4 – 不安全的直接对象引用	A4 – 不安全的直接对象引用
A6 –安全配置错误	A5 –安全配置错误
A7 – 不安全的加密存储—与A9合并成为➔	A6 –敏感信息泄漏
A8 –没有限制URL访问—扩展成为➔	A7 – 功能级访问控制缺失
A5 – 跨站请求伪造 （CSRF）	A8 –跨站请求伪造 （CSRF）
<合并在A6 –安全配置错误 >	A9 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	A10 – 未验证的重定向和转发
A9 – 传输层保护不足	与2010年版中的A7合并成为2013年版中的A6

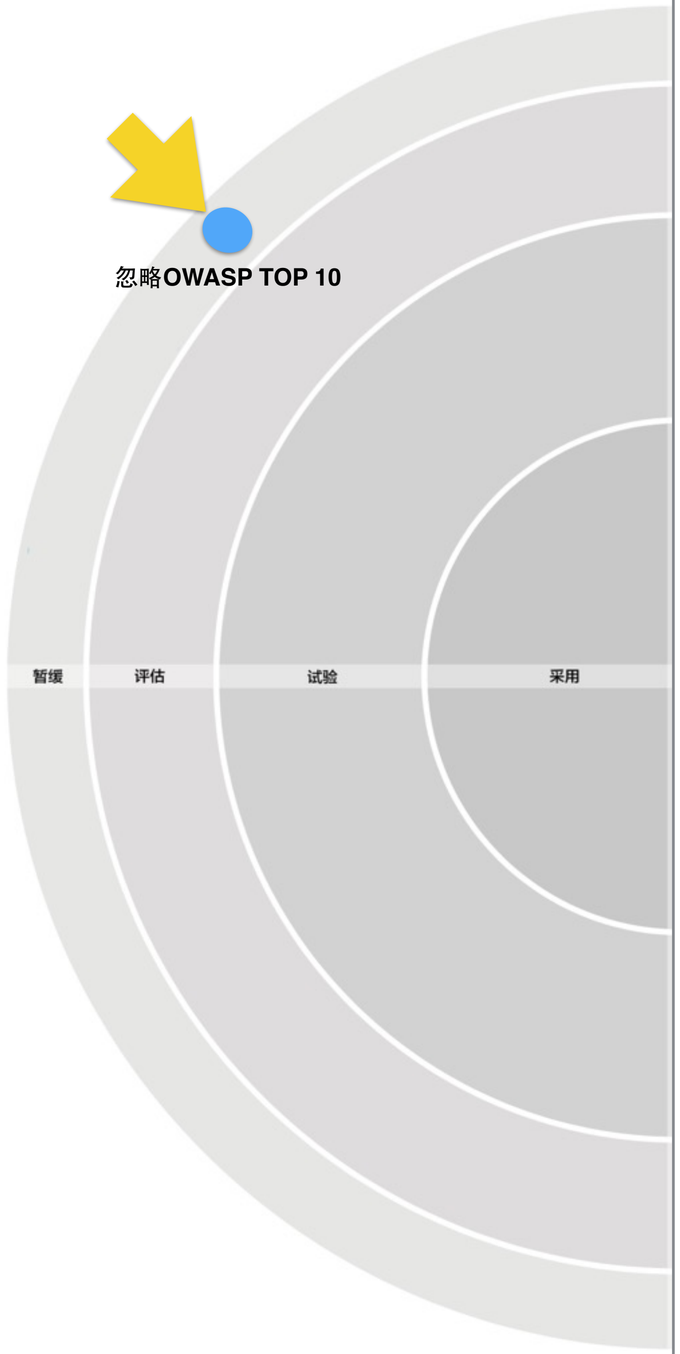


2014.01

OWASP
The Open Web Application Security Project

OWASP Top 10 – 2010 （旧版）	OWASP Top 10 – 2013 （新版）
A1 – 注入	A1 – 注入
A3 – 失效的身份认证和会话管理	A2 – 失效的身份认证和会话管理
A2 – 跨站脚本（XSS）	A3 – 跨站脚本（XSS）
A4 – 不安全的直接对象引用	A4 – 不安全的直接对象引用
A6 – 安全配置错误	A5 – 安全配置错误
A7 – 不安全的加密存储 – 与A9合并成为➔	A6 – 敏感信息泄漏
A8 – 没有限制URL访问 – 扩展成为➔	A7 – 功能级访问控制缺失
A5 – 跨站请求伪造 （CSRF）	A8 – 跨站请求伪造 （CSRF）
<合并在A6 – 安全配置错误 >	A9 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	A10 – 未验证的重定向和转发
A9 – 传输层保护不足	与2010年版中的A7合并成为2013年版中的A6

A2: 失效的身份认证和会话管理

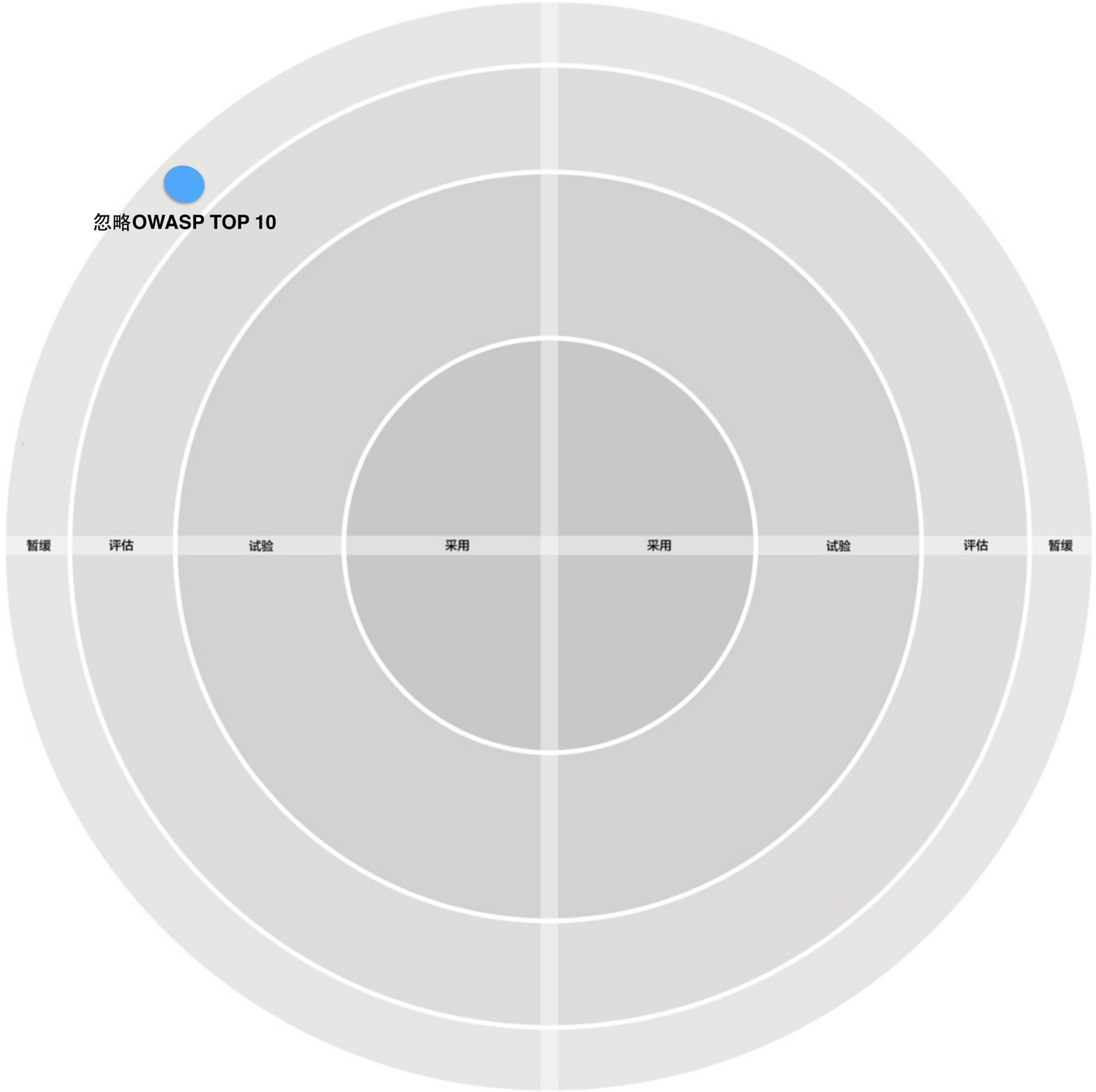


2014.01

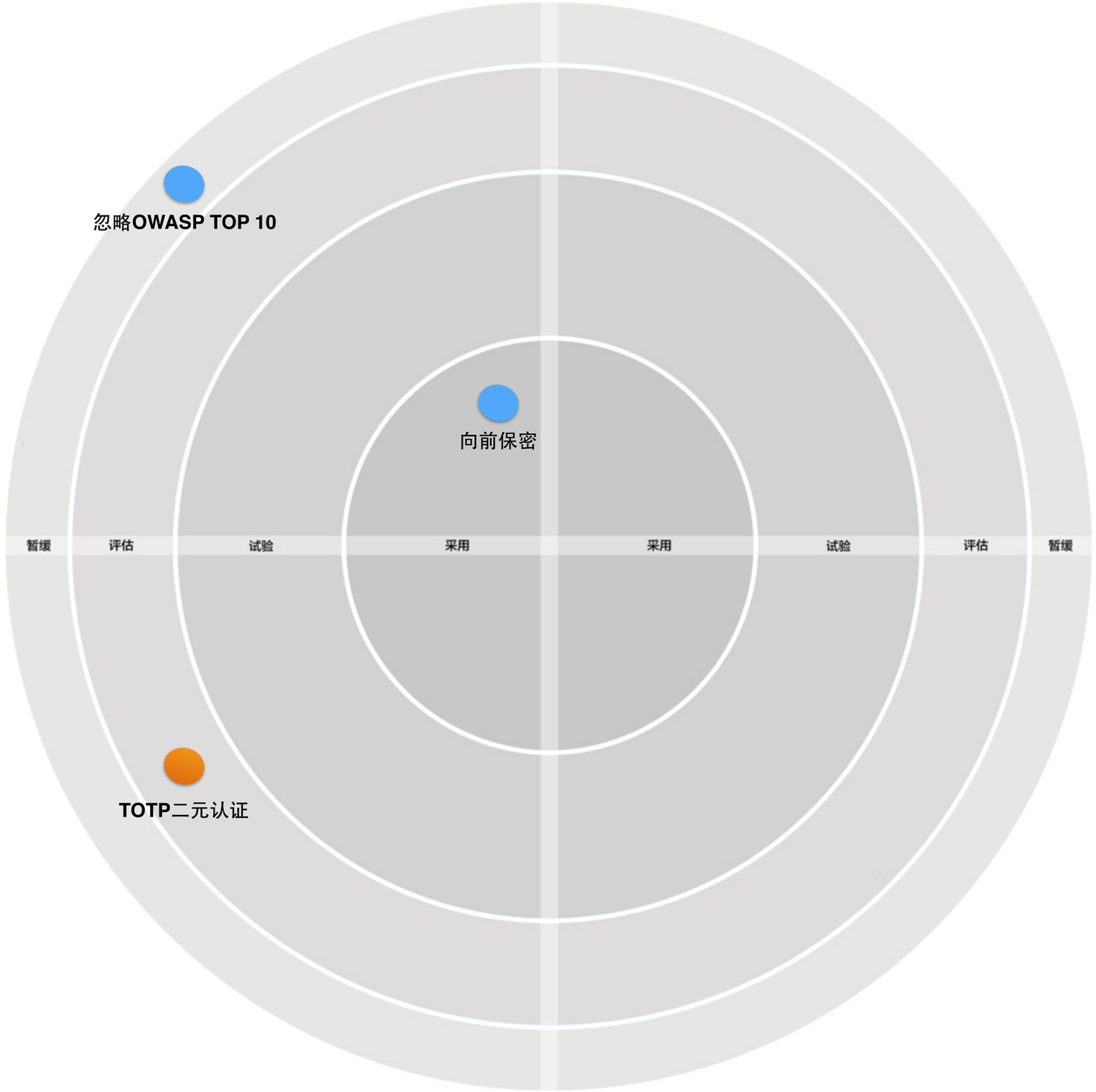
OWASP
The Open Web Application Security Project

OWASP Top 10 – 2010 （旧版）	OWASP Top 10 – 2013 （新版）
A1 – 注入	A1 – 注入
A3 – 失效的身份认证和会话管理	A2 – 失效的身份认证和会话管理
A2 – 跨站脚本（XSS）	A3 – 跨站脚本（XSS）
A4 – 不安全的直接对象引用	A4 – 不安全的直接对象引用
A6 – 安全配置错误	A5 – 安全配置错误
A7 – 不安全的加密存储 – 与A9合并成为➔	A6 – 敏感信息泄漏
A8 – 没有限制URL访问 – 扩展成为➔	A7 – 功能级访问控制缺失
A5 – 跨站请求伪造 （CSRF）	A8 – 跨站请求伪造 （CSRF）
<合并在A6 – 安全配置错误 >	A9 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	A10 – 未验证的重定向和转发
A9 – 传输层保护不足	与2010年版中的A7合并成为2013年版中的A6

A2: 失效的身份认证和会话管理

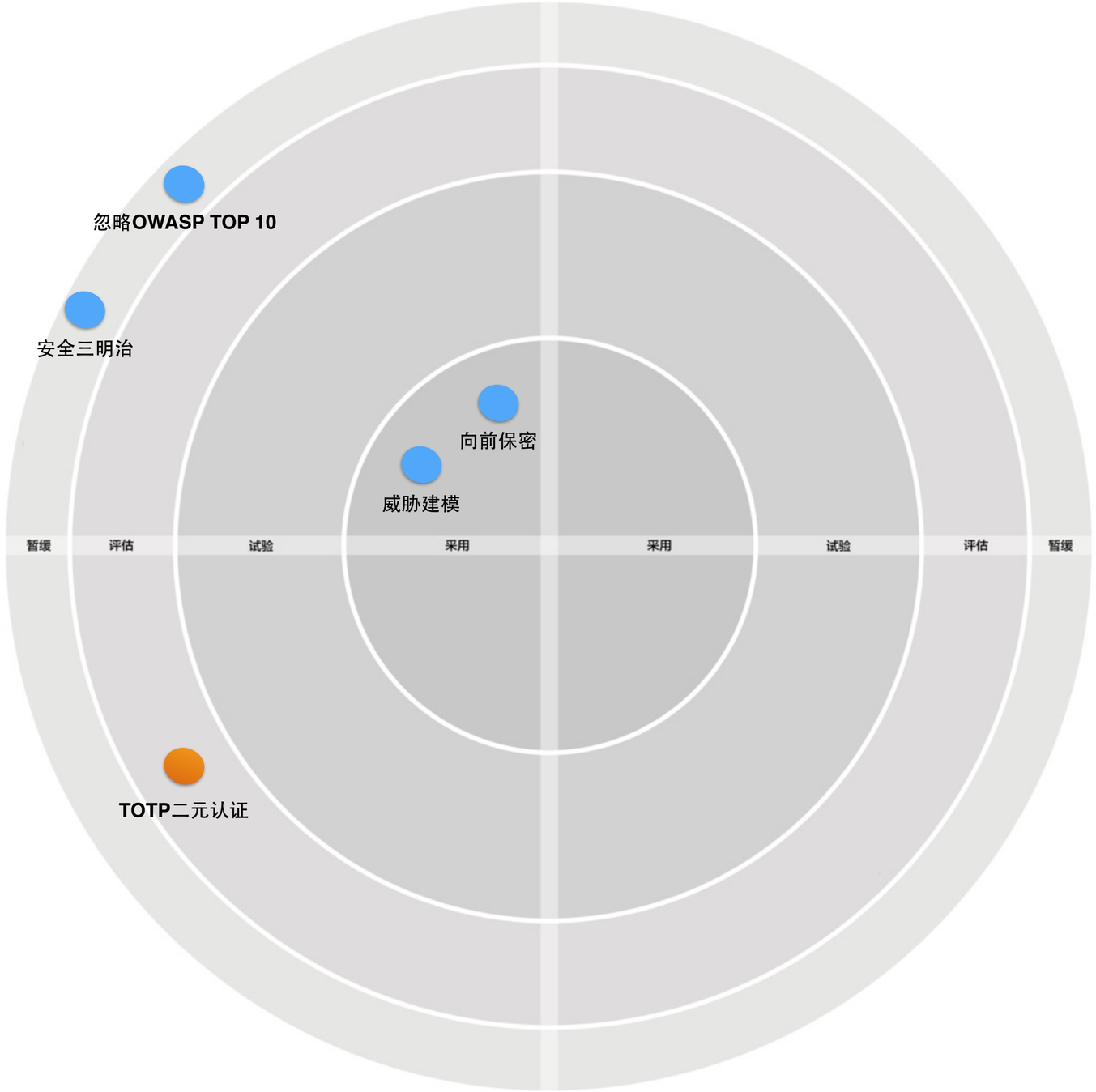


2014.01



2014.07

2014.01



2015.01

2014.07

2014.01

2015.05

2015.01

2014.07

2014.01

2015.11

2015.05

2015.01

2014.07

2014.01

2016.04

2015.11

2015.05

2015.01

2014.07

2014.01

2016.04

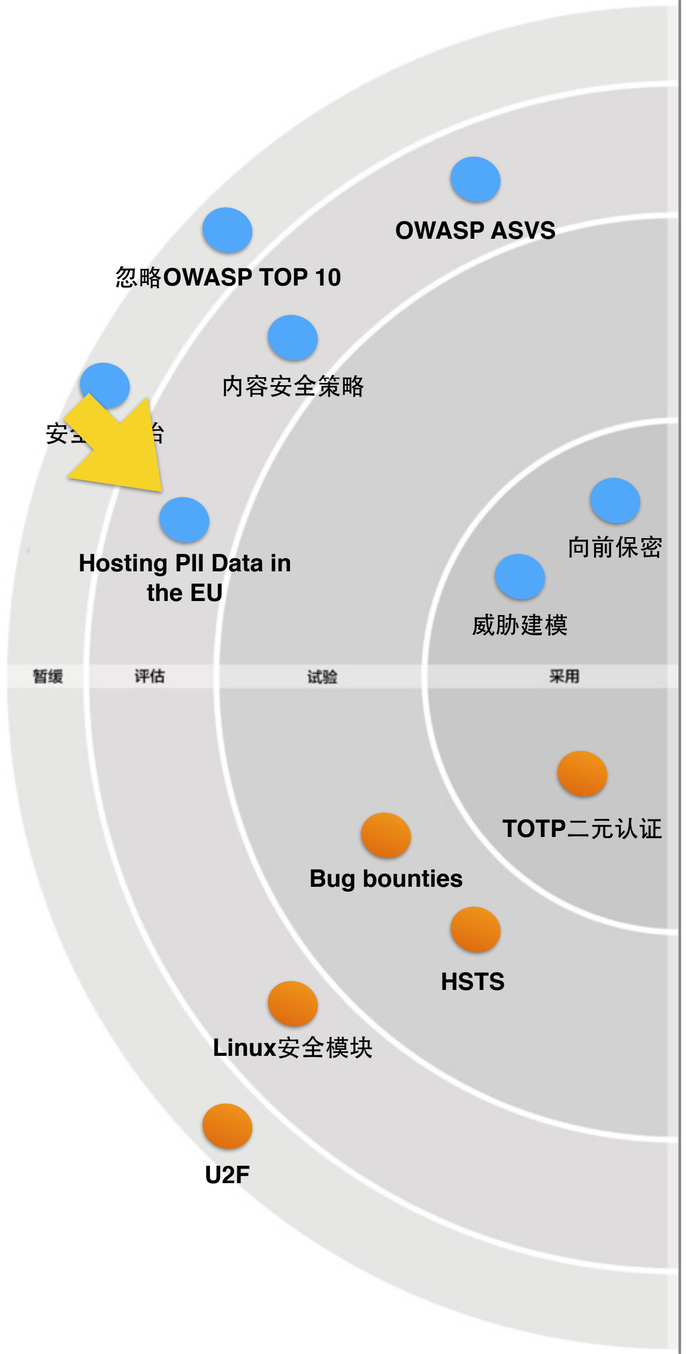
2015.11

2015.05

2015.01

2014.07

2014.01



将个人信息托管于欧洲境内（Hosting PII Data in the EU）

2016.04

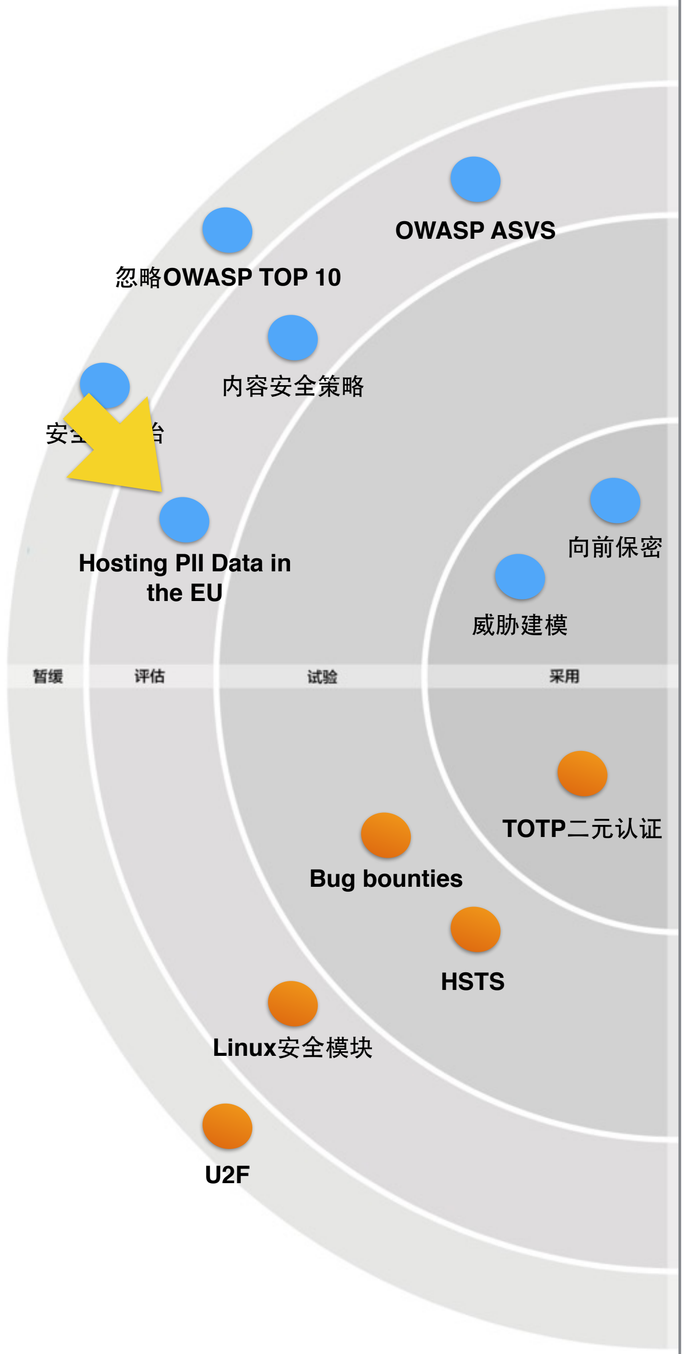
2015.11

2015.05

2015.01

2014.07

2014.01



将个人信息托管于欧洲境内（Hosting PII Data in the EU）

安全港协议

2000年12月

2016.04

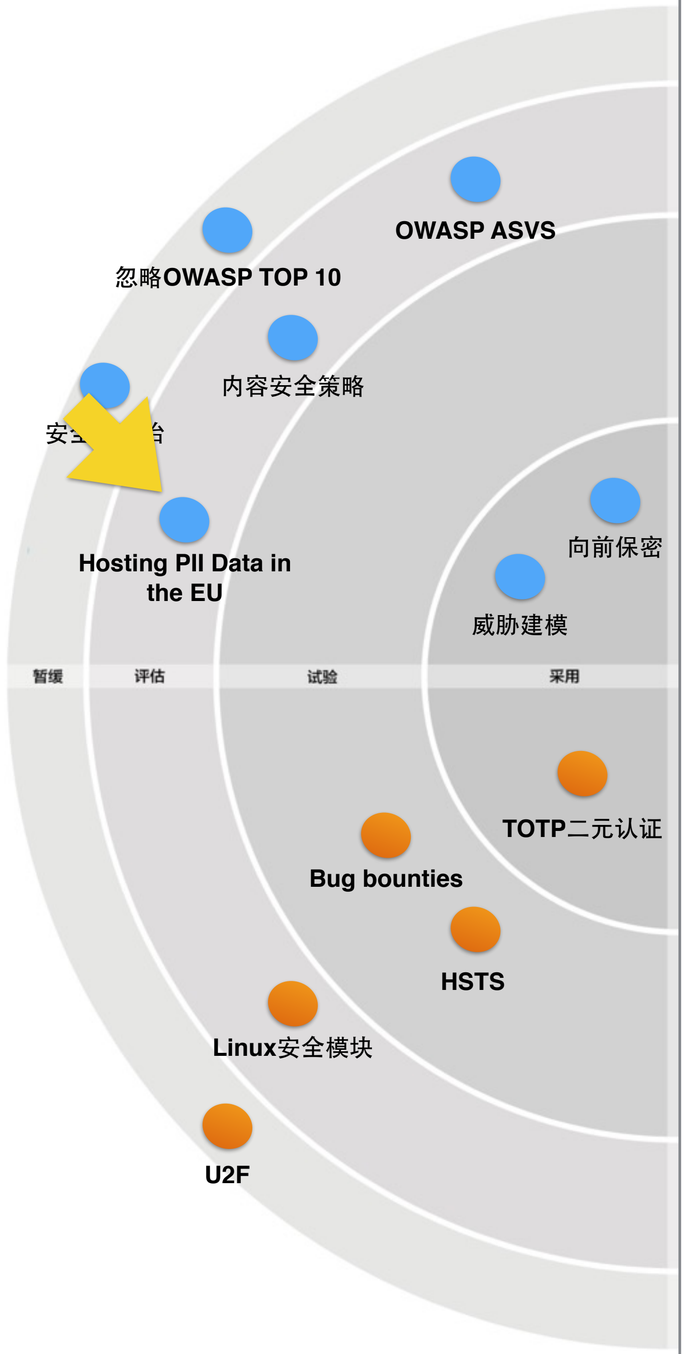
2015.11

2015.05

2015.01

2014.07

2014.01



将个人信息托管于欧洲境内（Hosting PII Data in the EU）

安全港协议

2000年12月

2016.04

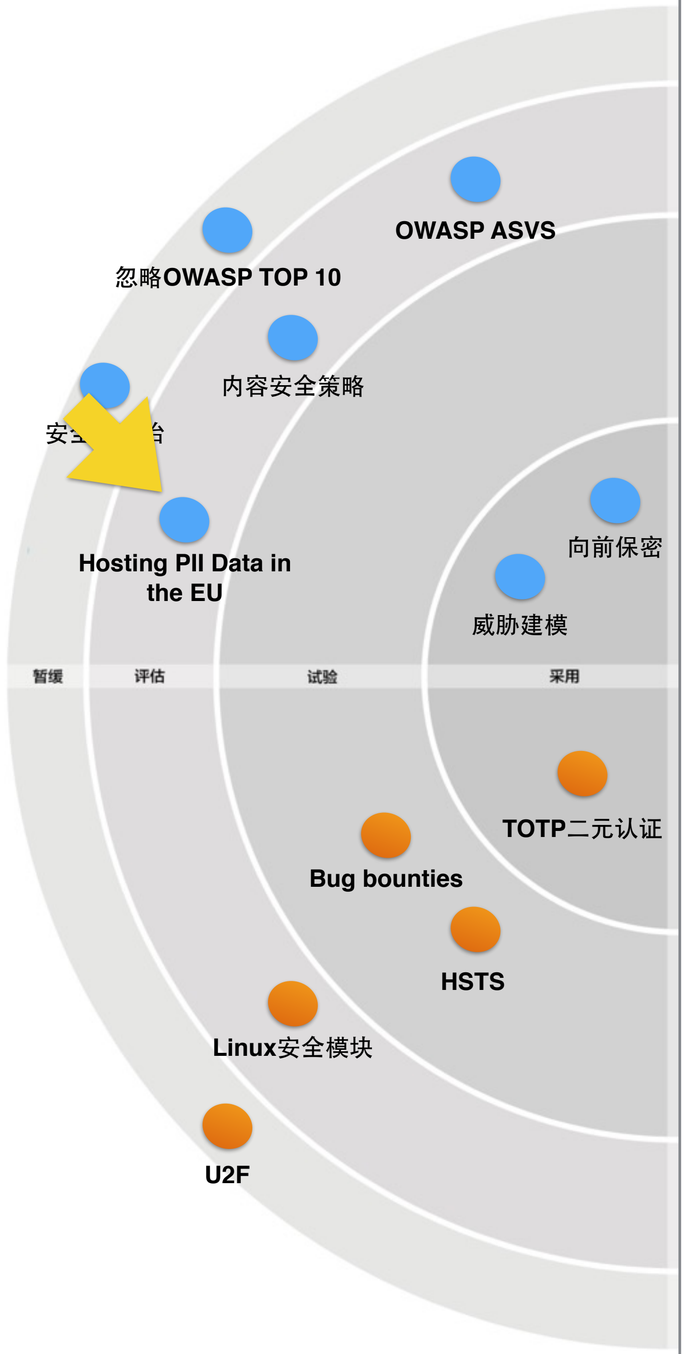
2015.11

2015.05

2015.01

2014.07

2014.01



将个人信息托管于欧洲境内（Hosting PII Data in the EU）

~~安全港协议~~

2000年12月 2015年10月6日

这样就安全了吗?

My biggest worry is about my colleagues can stole the customers' data then I will have huuuge trouble.

—— *From a conversation with a Director of IT Department*

我最大的担心是我的员工会偷走客户的数据，那样我会惹上大～～～～～～麻烦。

—— 和某*IT*部门总监的谈话

BSI, *Build Security In*

既有角色

项目/技术主管

BA

架构师

程序员

QA

既有流程

项目规划

需求分析

架构设计

编码实现

测试上线

- *OWASP TOP 10*

- 威胁建模

- 软件架构安全
- 拓扑结构安全

- 代码安全审查
- 自动代码安全扫描
- 自动依赖扫描
- 开发工具确认

- 渗透测试
- 安全功能测试
- 部署安全指导

谢谢

韩锴
khan@thoughtworks.com

ThoughtWorks®