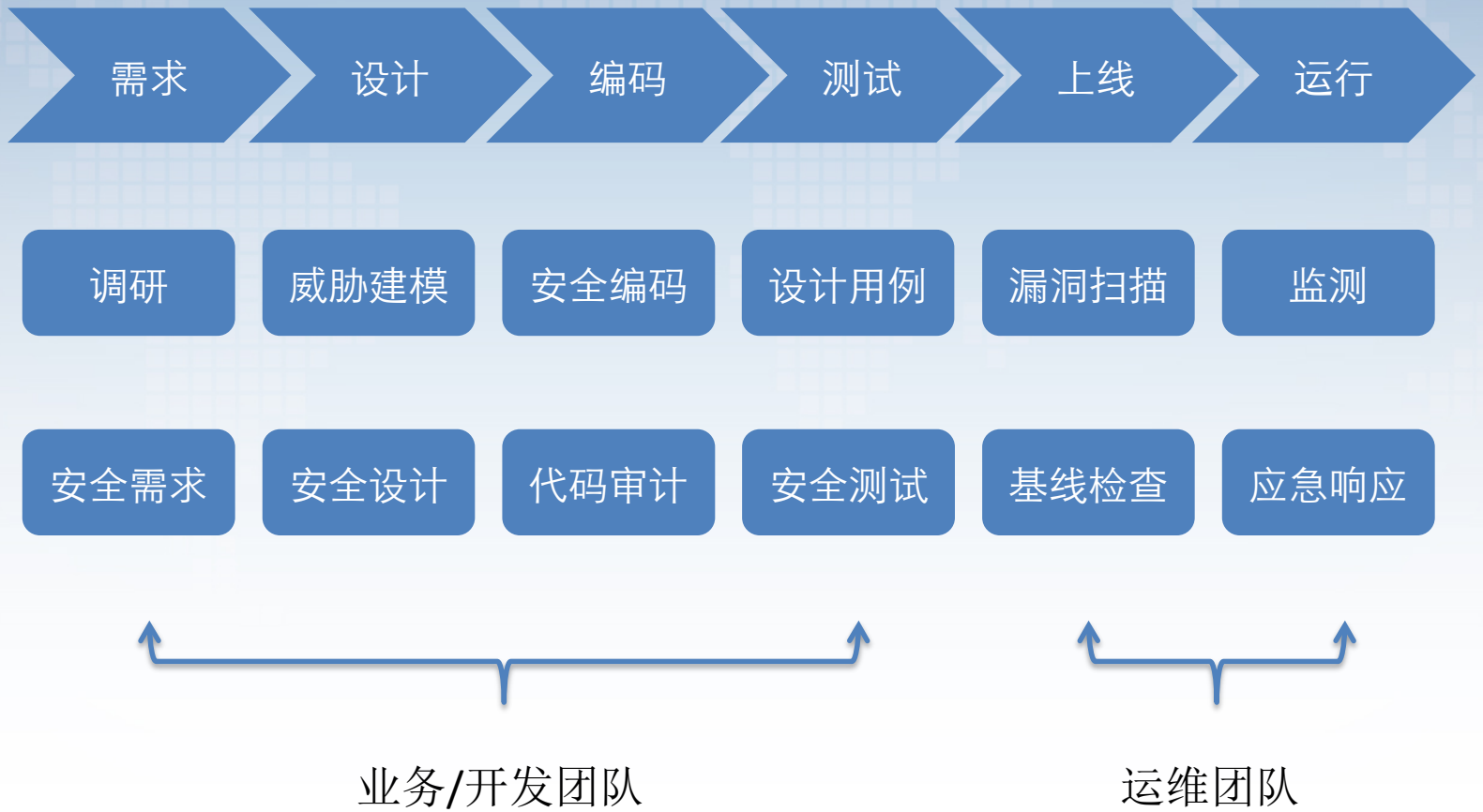
全生命周期开发安全的旧瓶与新酒

杨廷锋 @安恒信息

传统的S-SDLC

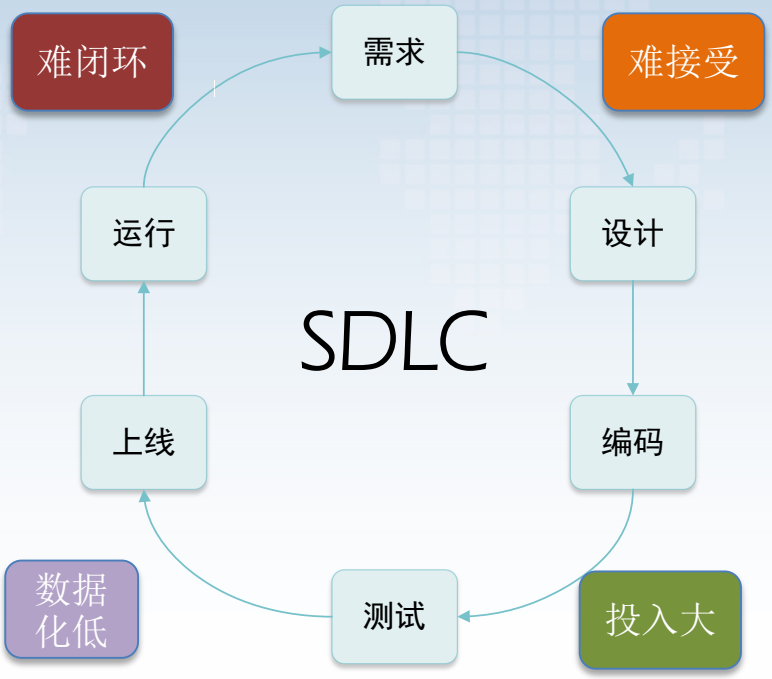


OWASP
Open Web Application Security Project

传统的S-SDLC

目前的S-SDLC服务以文档为主，难以闭环具体代码实现问题

部分设计可能过于专业，普通的需求经理和开发人员无法驾驭

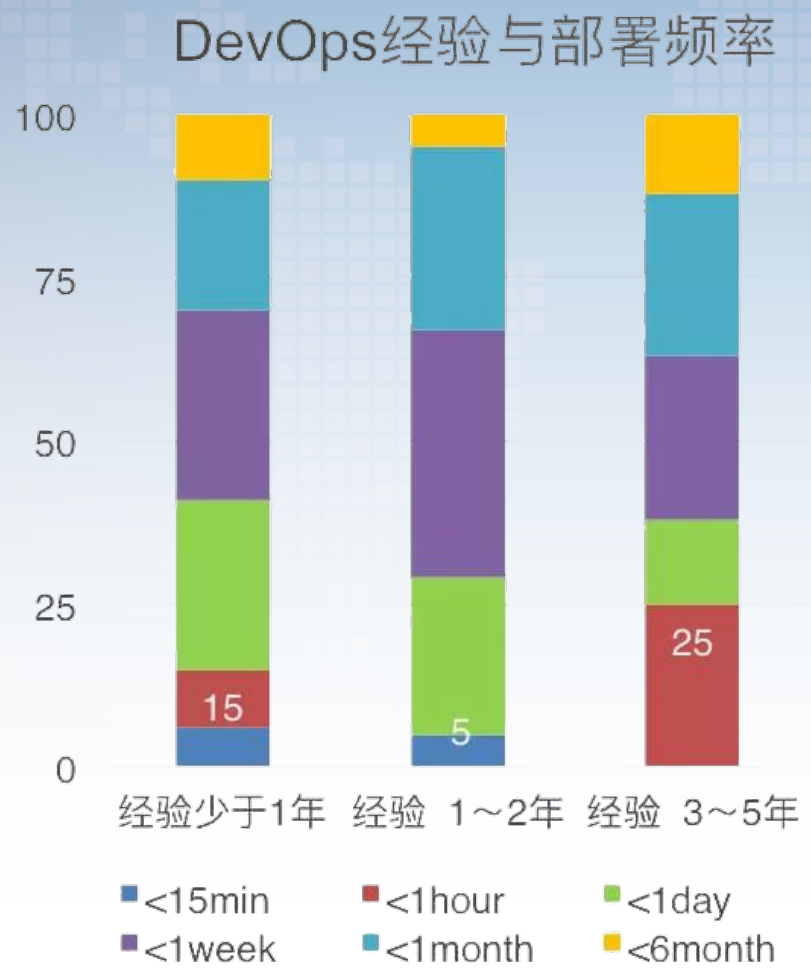


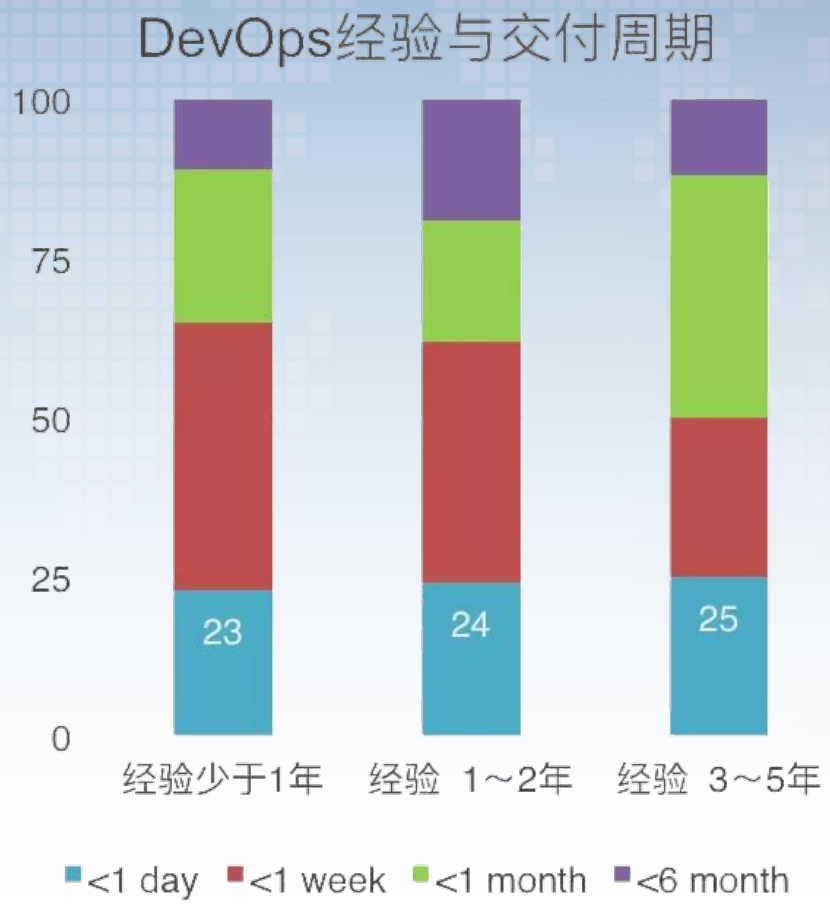
整个过程中产生大量文档，无法迅速转换成数据，进入到反馈环。难以适应快速变化的业务需求

从目前的服务来看在落地过程中需要大量的人力投入。但是内容都是重复性工作，没有时间深入挖掘漏洞。

OWASP
Open Web Application Security Project

DevSecOps





OWASP
Open Web Application Security Project

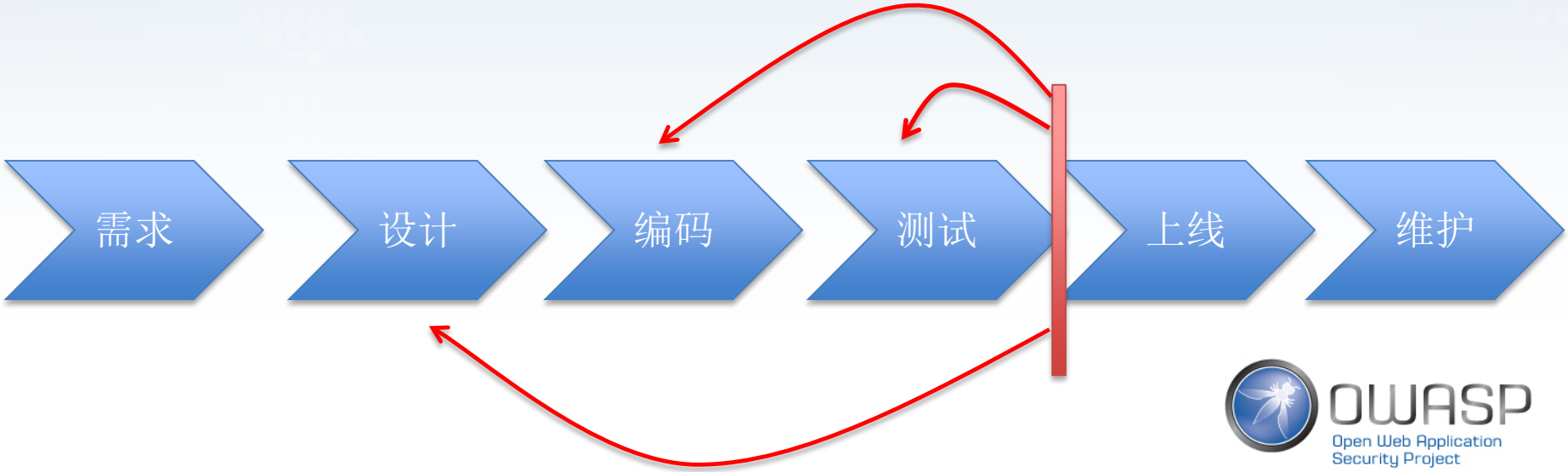
DevSecOps

- DevOps经典框架

OWASP
Open Web Application Security Project

DevSecOps

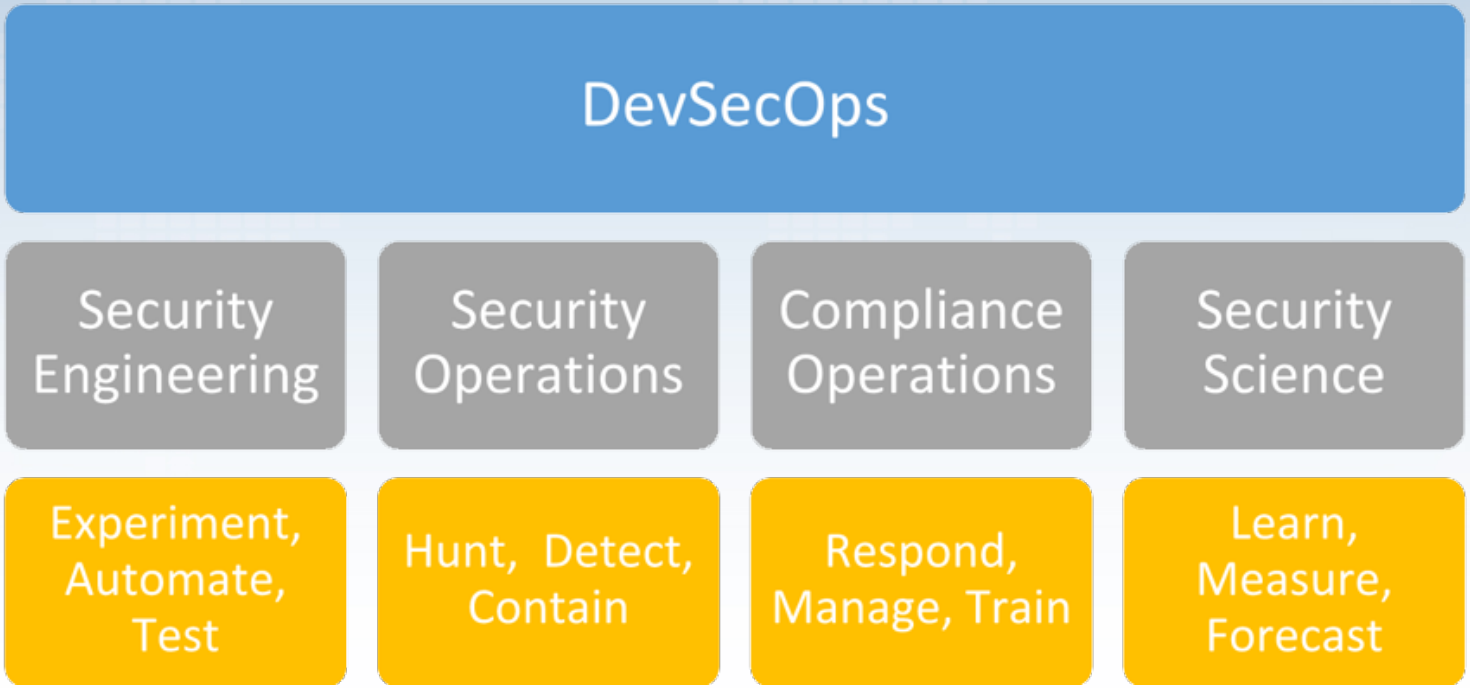
- 核心思想：
  每个人都对安全负责，将安全深入到整个软件生命周期。
- 优化沟通交流，注重反馈



OWASP
Open Web Application Security Project

DevSecOps

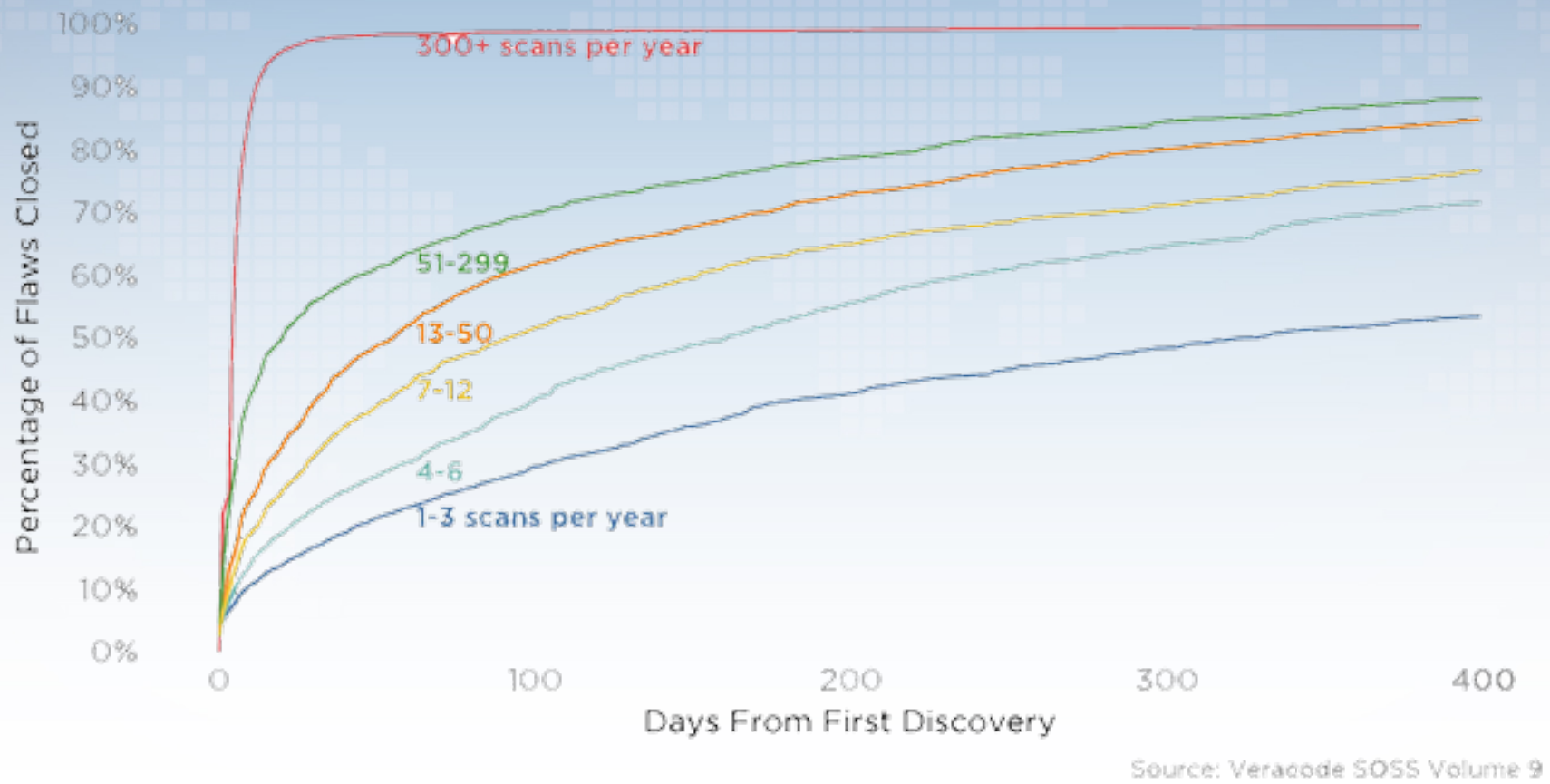
The Arts/Wushu of DevSecOps



OWASP
Open Web Application Security Project

DevSecOps

CA Veracode的调研结果



OWASP
Open Web Application Security Project

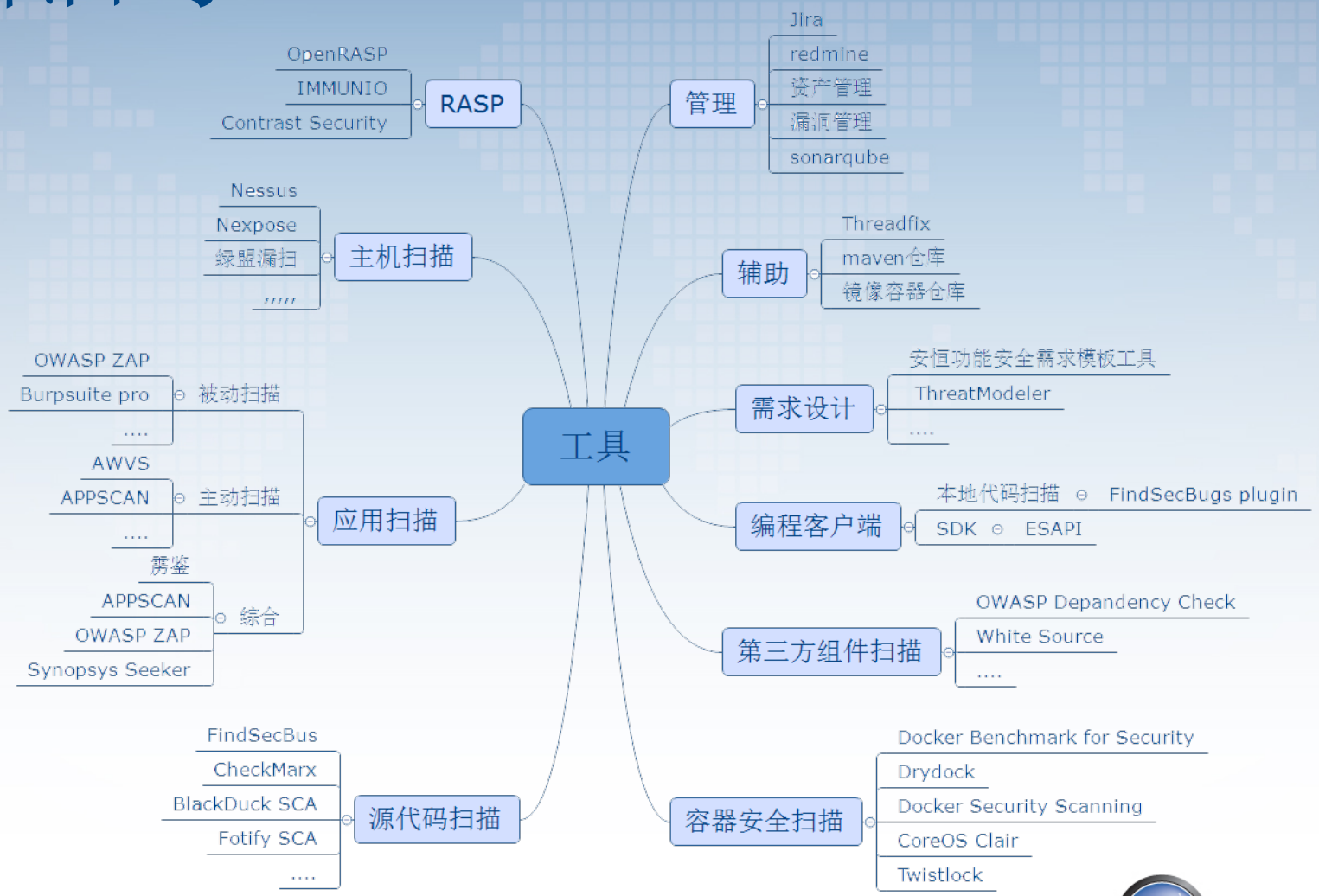
新酒与S-SDLC

思考方向

- 1. 能实现自动化的部分尽可能自动化
- 2. 将安全工作整合到开发过程
- 3. 尝试构建标准化基线
- 4. 文档数据化
- 5. 尽可能提高开发人员接受程度和易用性

OWASP
Open Web Application Security Project

新酒与S-SDLC

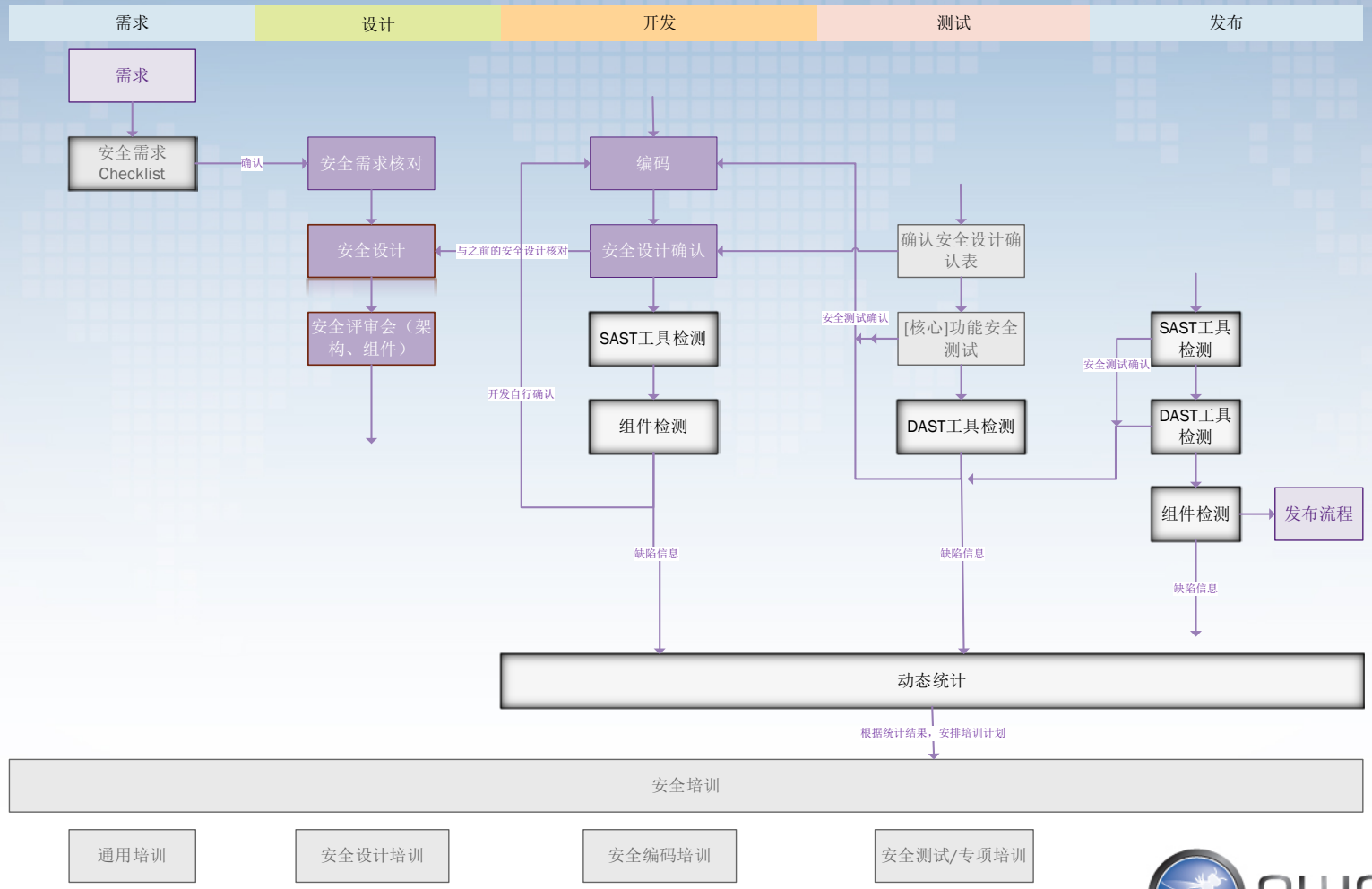


OWASP
Open Web Application Security Project

新酒与S-SDLC

OWASP
Open Web Application Security Project

新酒与S-SDLC



OWASP
Open Web Application Security Project

新酒与S-SDLC

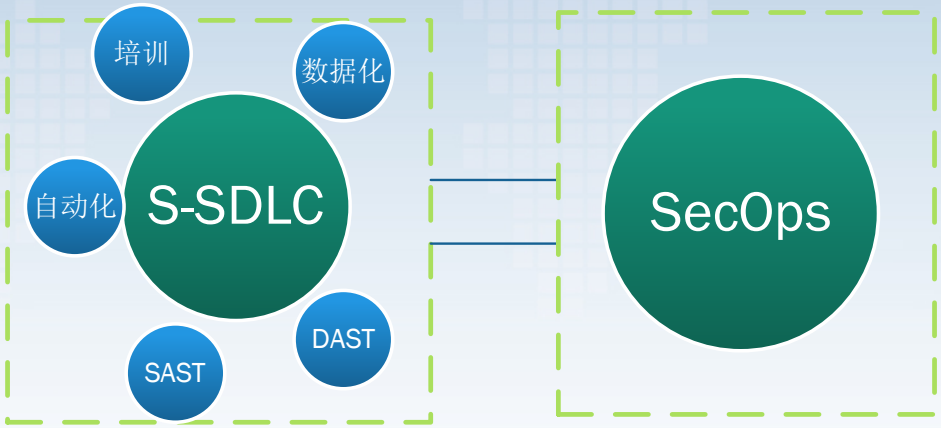
工具化自动化减少投入

数据化方便分析和共享

关注开发体验，易接受

数据+流程构成闭环

DeVSecOps



数据共享

对接安全运维平台，实现DevSecOps技术理念的完全落地。

通过不断调整，形成适合企业自身的S-SDLC落地方案

OWASP
Open Web Application Security Project

谢谢！

杨廷锋 @安恒信息