OWASP
Open Web Application Security Project

DevOps整合SDL落地的两难选择：效率 vs 安全

张克强

2020年9月26日

SimpleOpen

张克强 介绍

- Exin认证DevOps Master
- 系统分析师,高级程序员
- Certificated Scrum Master(2009)
- 规模化敏捷框架认证项目群咨询师(SAFe Program Consultant -SPC)
- 在中国大陆发布了首份在CMMI环境下导入敏捷报告
- 在中国大陆发布了首个Scrumban案例分析报告
- Scrumban SimpleOpen Edition 欣奔版出品人

微博：张克强-敏捷307
博客：从高效过程到卓越结果
微信公众号：大敏捷

微信:

SimpleOpen

OWASP
Open Web Application Security Project

内容大纲

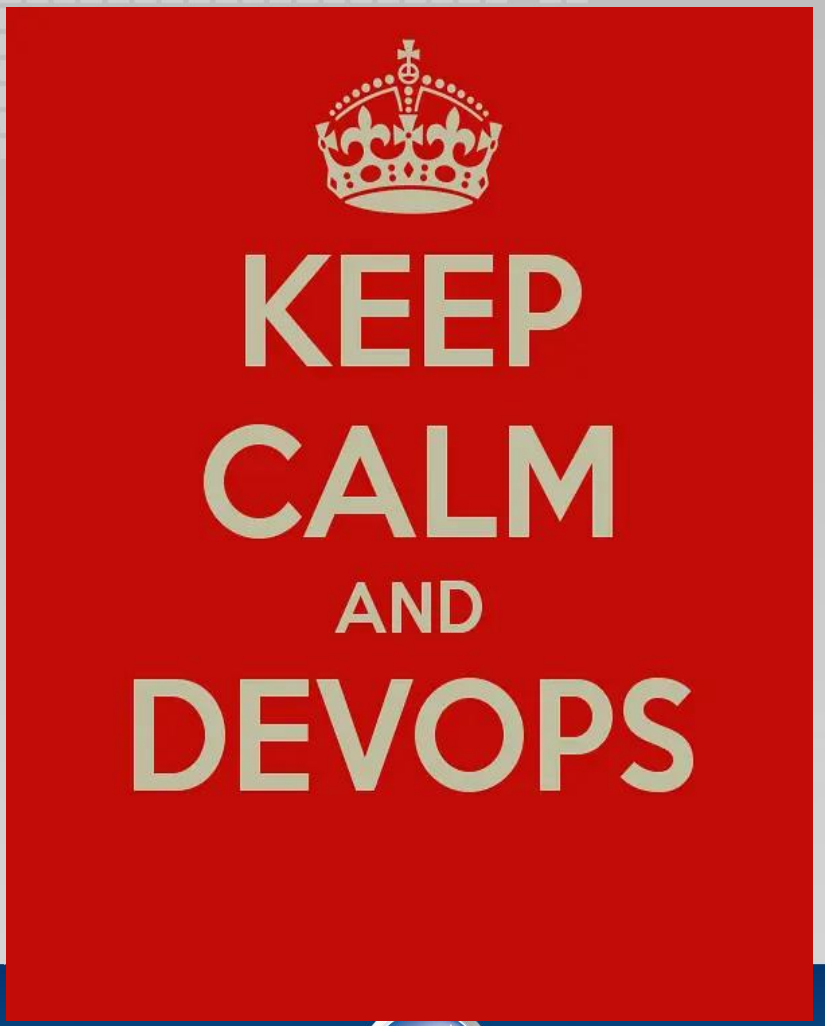
- 敏捷和DevOps给安全工作带来的冲击
- 安全工作在敏捷转型路上的障碍
- 更加安全和更高效率之间的矛盾
- 从结果导向来判断平衡安全和效率
- DevSecOps给SDL带来的高效实践
- 左移到需求的安全工作如何保证全程高效
- 安全工作的敏捷DevOps之旅

敏捷4大特征

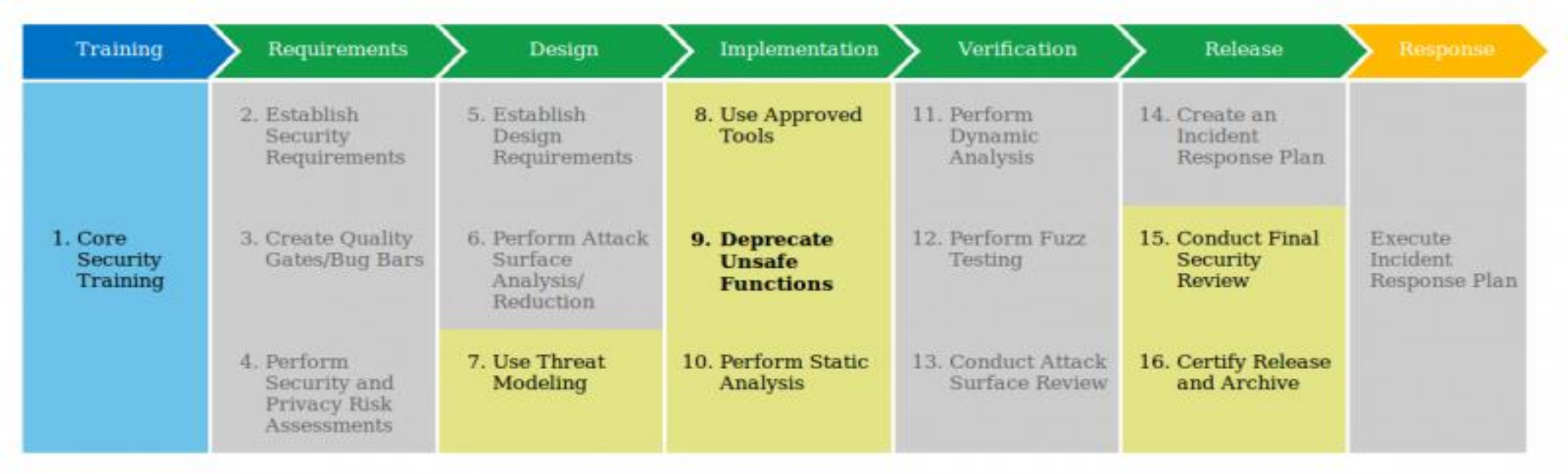
短迭代	• 最优先要做的是尽早、持续地交付有价值的软件 • 从数周到数月，交付周期越短越好
可运行	• 频繁地交付可工作的软件 • 可工作的软件是衡量进度的首要标准
快反馈	• 业务人员必须和开发人员每天都在一起工作 • 面对面交谈是最有效，也是最高效的沟通方式
拥变化	• 欣然面对需求变化，即使在开发后期 • 让客户满意

DevOps4大要点

文化Cultrue	• 责任共担，功过共享 • 无责备
自动化 Automation	• 利用机器替代人工 • 建设持续交付流水线
精益Lean	• 精益流加速交付 • 单件流
度量 Measurement	• 度量一切 • 首要度量前置时间

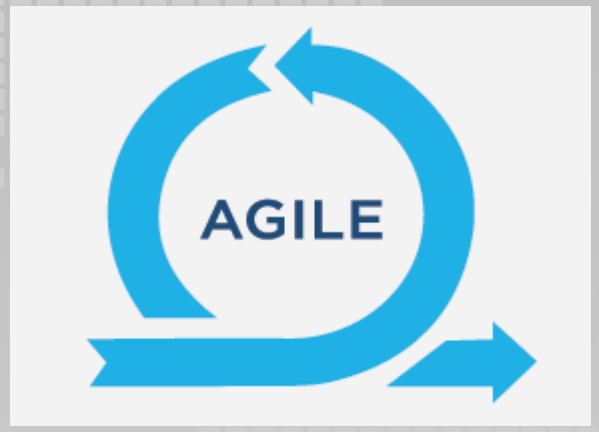


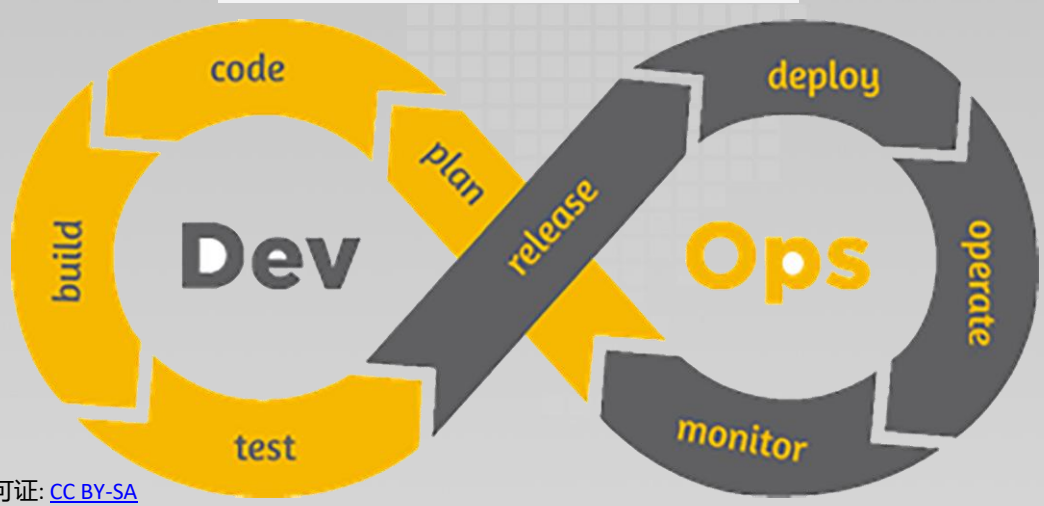
SDL-Security Development Lifecycle



- SDL的核心理念就是将安全考虑集成在软件开发的每一个阶段:需求分析、设计、编码、测试和维护。从需求、设计到发布产品的每一个阶段每都增加了相应的安全活动，以减少软件中漏洞的数量并将安全缺陷降低到最小程度。
- 2004年起，微软将SDL作为全公司的计划和强制政策

高频交付下的SDL



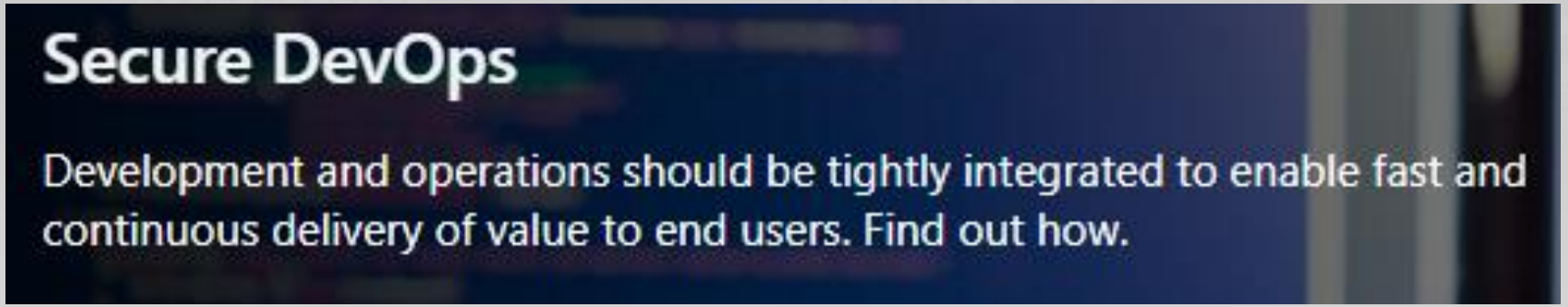


跟不上

靠边站

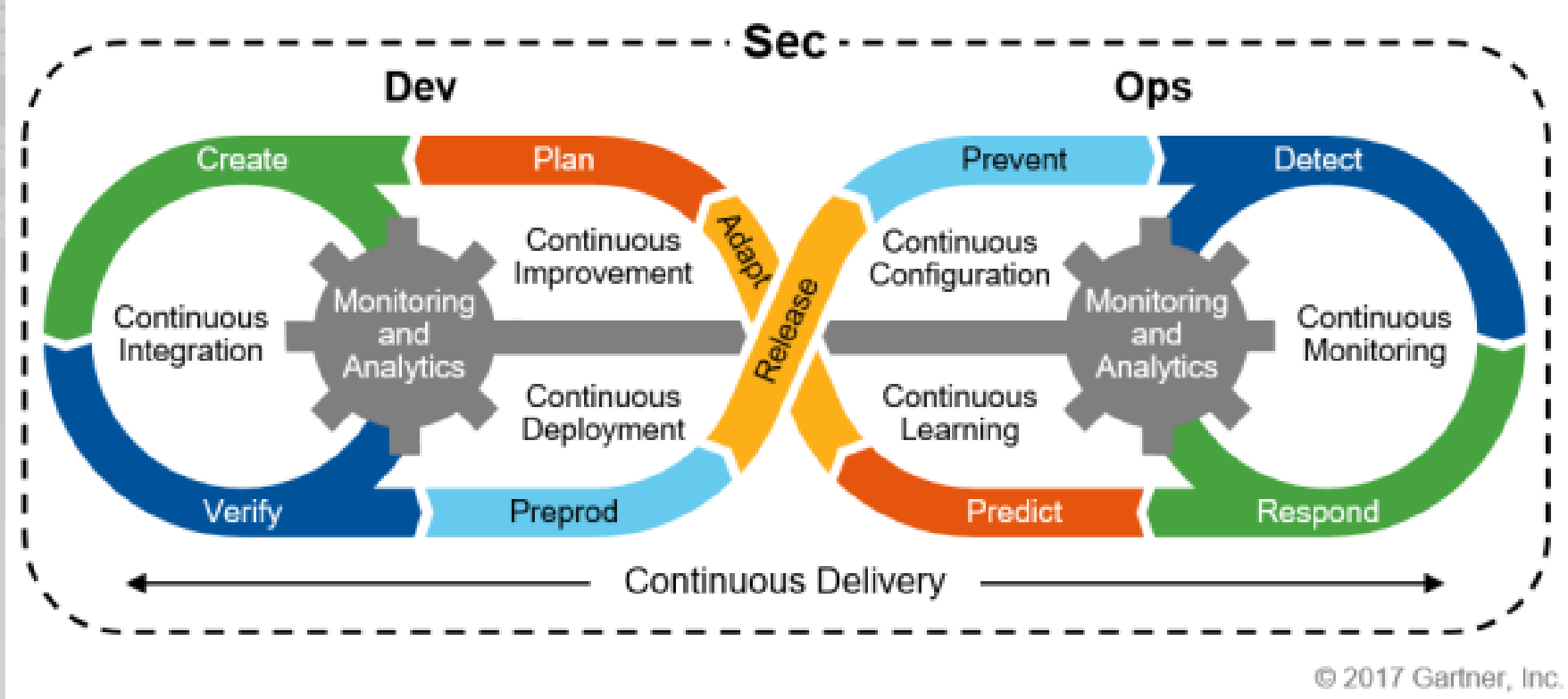
马后炮

Microsoft现在如何看待SDL

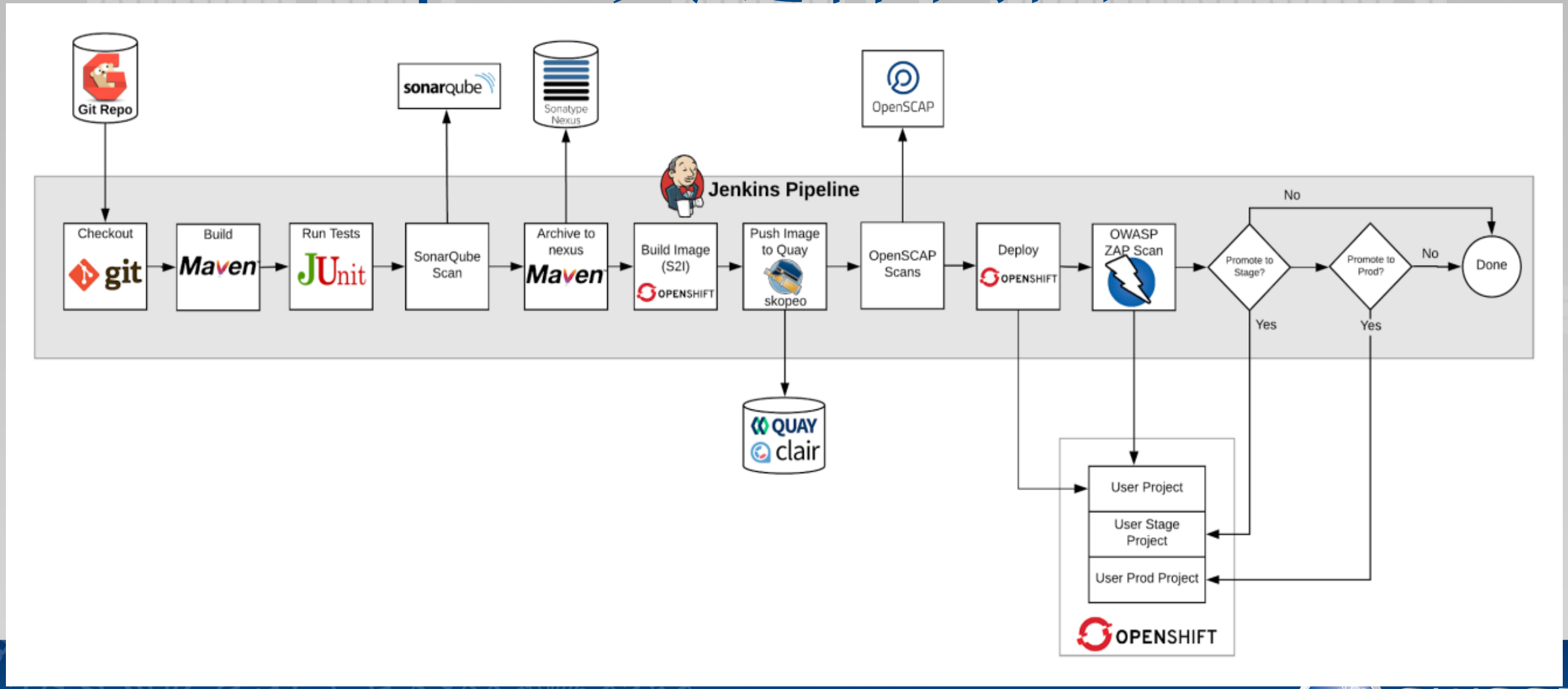


来自于微软SDL网站

DevSecOps


Sec
Dev
Ops
Create
Plan
Prevent
Detect
Continuous Integration
Monitoring and Analytics
Continuous Improvement
Continuous Deployment
Adapt
Release
Continuous Configuration
Continuous Learning
Monitoring and Analytics
Continuous Monitoring
Verify
Preprod
Predict
Respond
Continuous Delivery
© 2017 Gartner, Inc.

DevSecOps工具链样例图



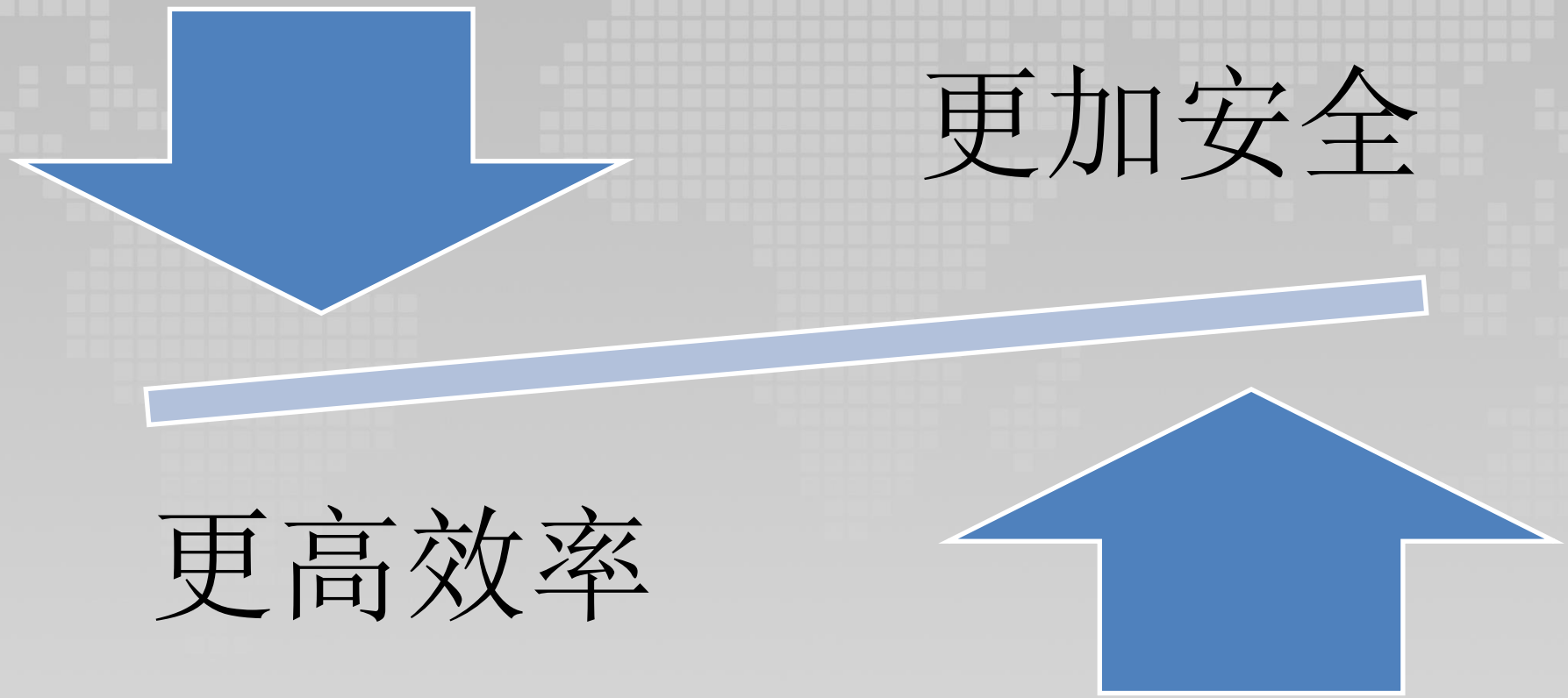
安全和开发的对话场景1

- 安工：Fortify扫描在CI当中执行的话，能够更加及时反馈
- 高工：Fortify扫描一次耗时10分钟，CI本身只要3分钟，加进来的话，太费时间了
- 安工：那放到Nightly Build里面如何？
- ……

安全和开发的对话场景2

- 安工：本版本的安全设计评审在哪里？
- 高工：安全设计评审记录已经上传
- 安工：20人2周的工作就这一份设计评审记录，你们这是应付吧
- 高工：弟兄们忙得很，要不是合规强制要求，才懒得弄，目前这份足够了

DevSecOps的两难问题？



安全和敏捷的矛盾？

因为Agile和DevOps转型，更快响应市场变化，安全合规要求可以放宽

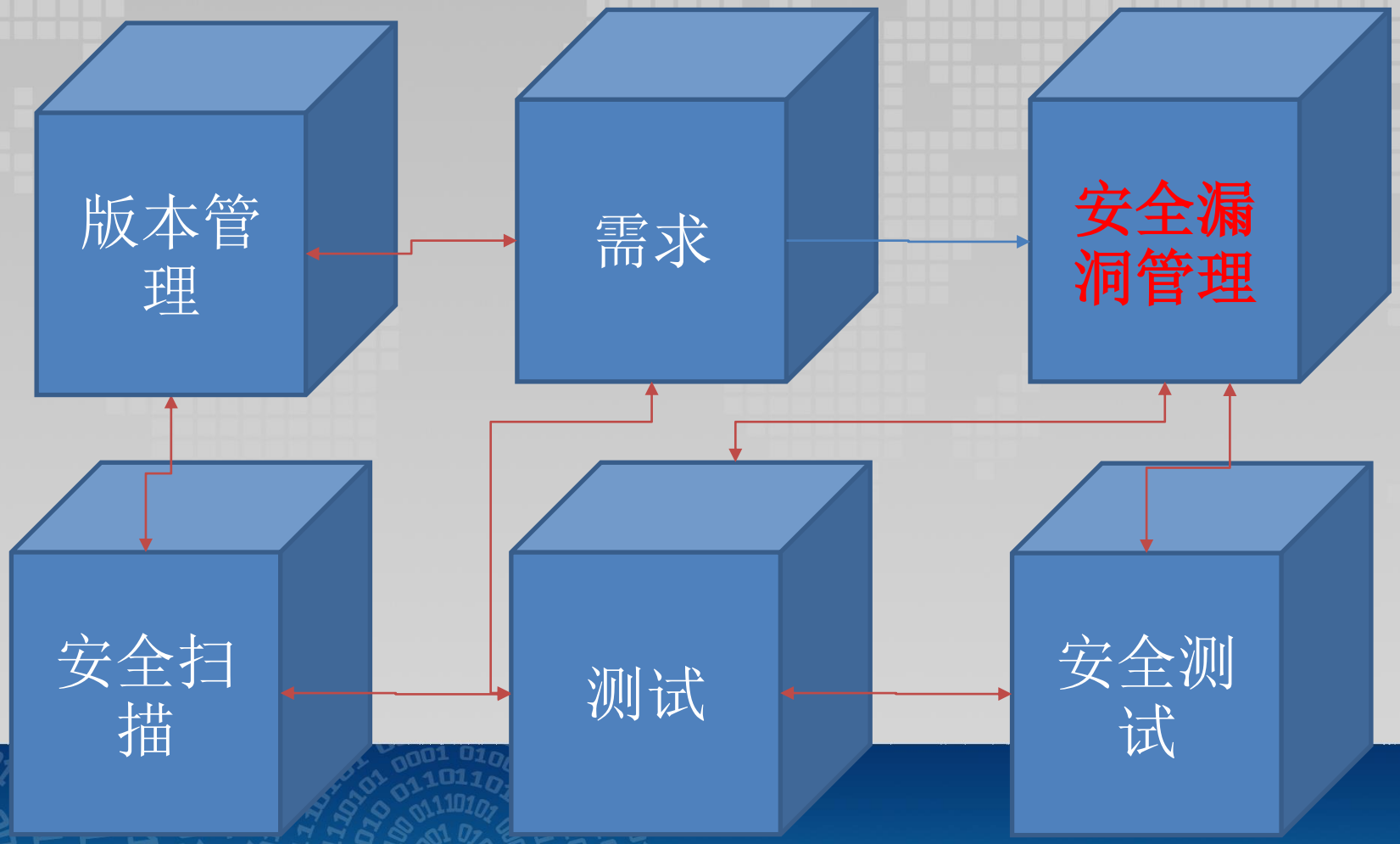
安全第一，无论搞Agile还是DevOps，相关安全合规的工作一个都不能少？

从结果导向来判断安全和效率的平衡

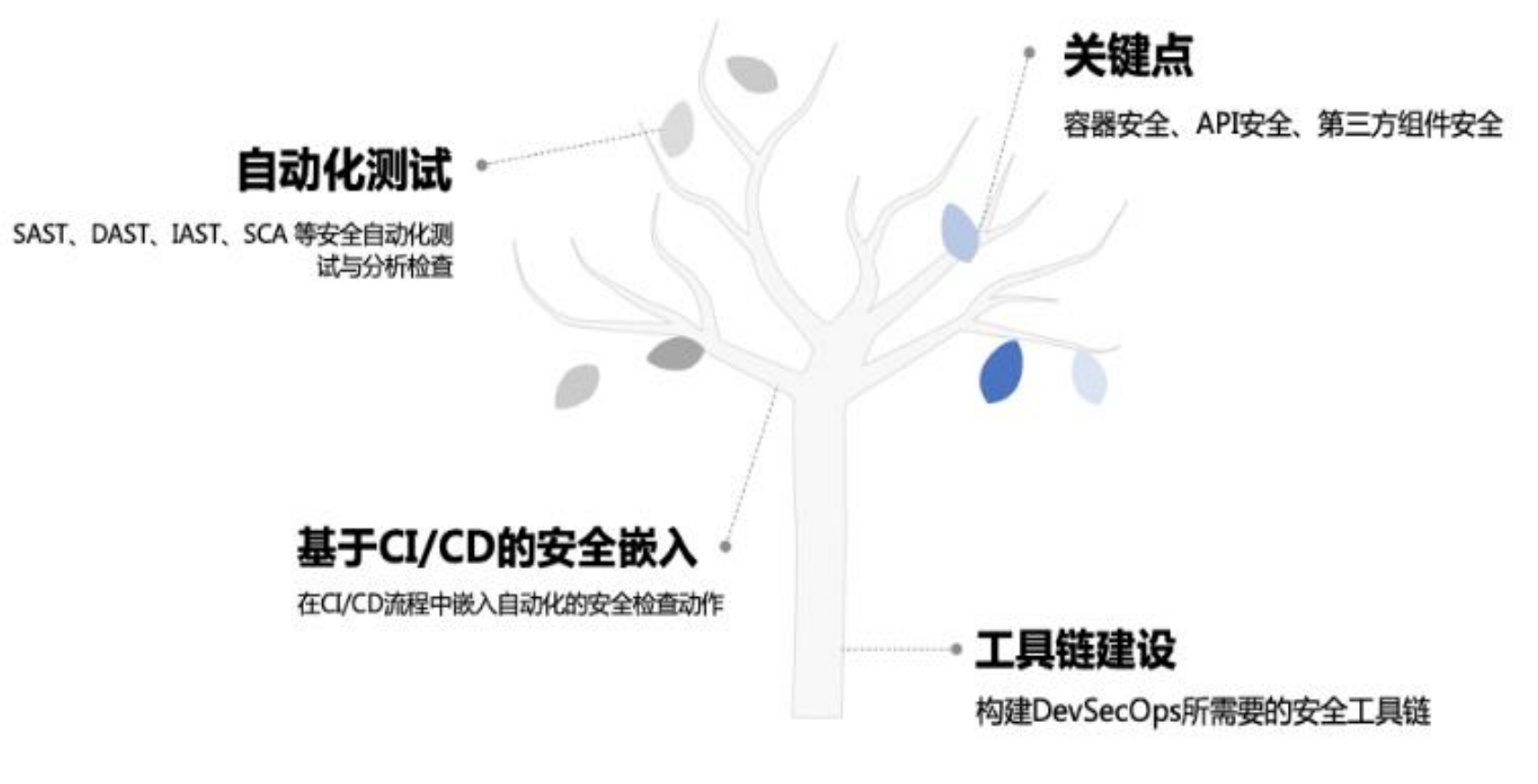
- 记录实际安全漏洞
  - 生产环境
  - 测试环境
- 多维度分析
  - 来源分类
  - 级别
  - ……
- 威胁建模

来自于微软SDL网站

DevOps需求-测试-安全工具链



DevSecOps给SDL带来的高效实践



- Be integrated into the CI/CD pipeline.
- Not require security expertise.
- Avoid a high false-positive rate of reporting issues.
- Prefer to Integrate SAST into IDE
- Prefer to Integrate DAST into CI

- 上图来自于腾讯张祖优

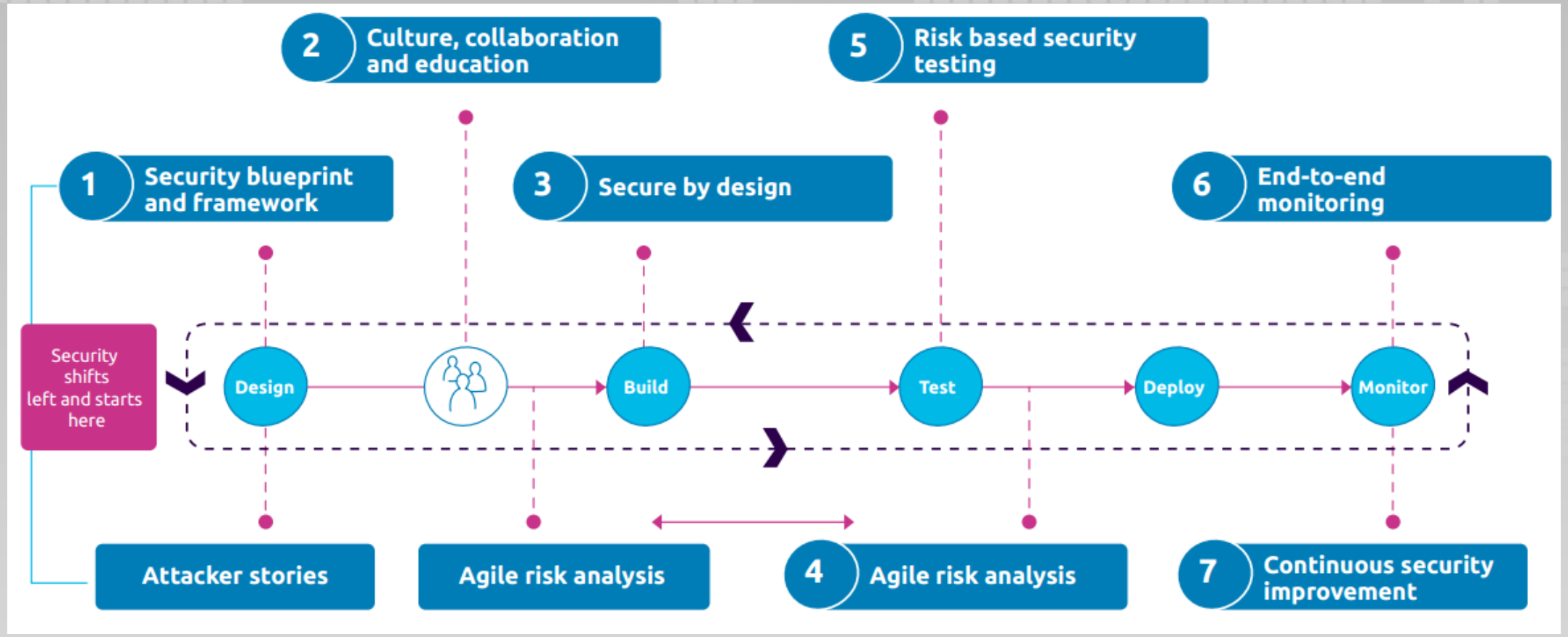
安全问题解决了吗？

- **DevSecOps**解决方案针对代码提供了各种自动化工具
- 人人参与安全，人人为安全负责
- 安全嵌入到全生命周期的每个环节。

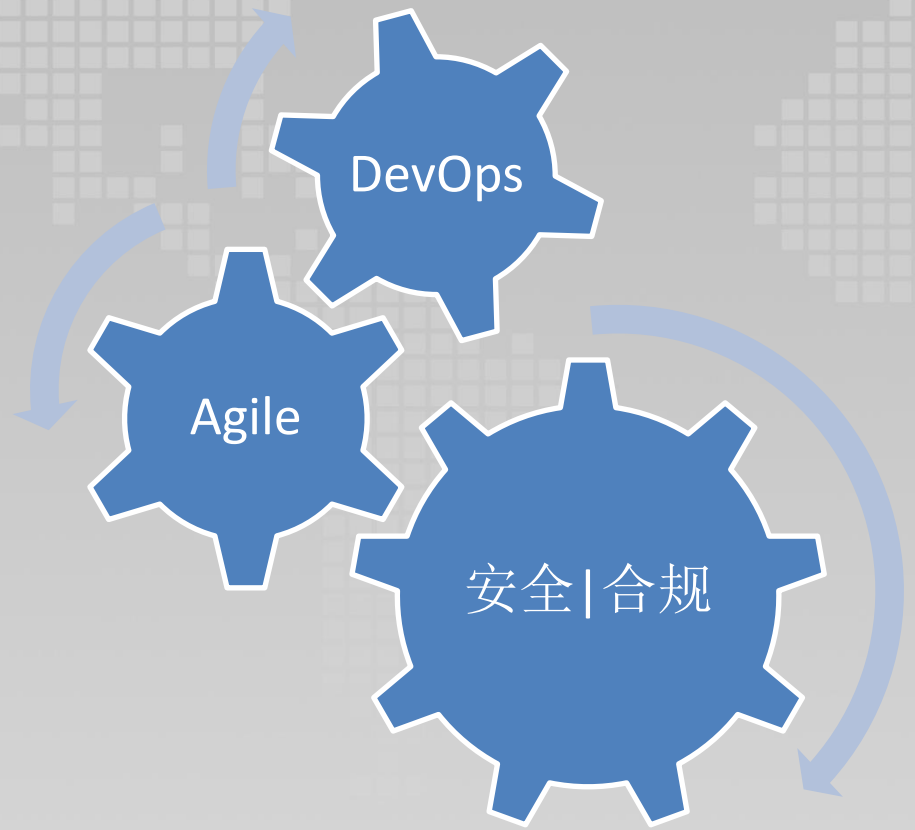
- 但不只有代码
  - 对于软件需求？
  - 对于软件设计？
  - 对于安全测试？
  - 各种合规贯标？

全生命周期中7个安全切入要点

来自于Capgemini Global DevSecOps Insights report 2020



安全团队与Agile|DevOps建设团队

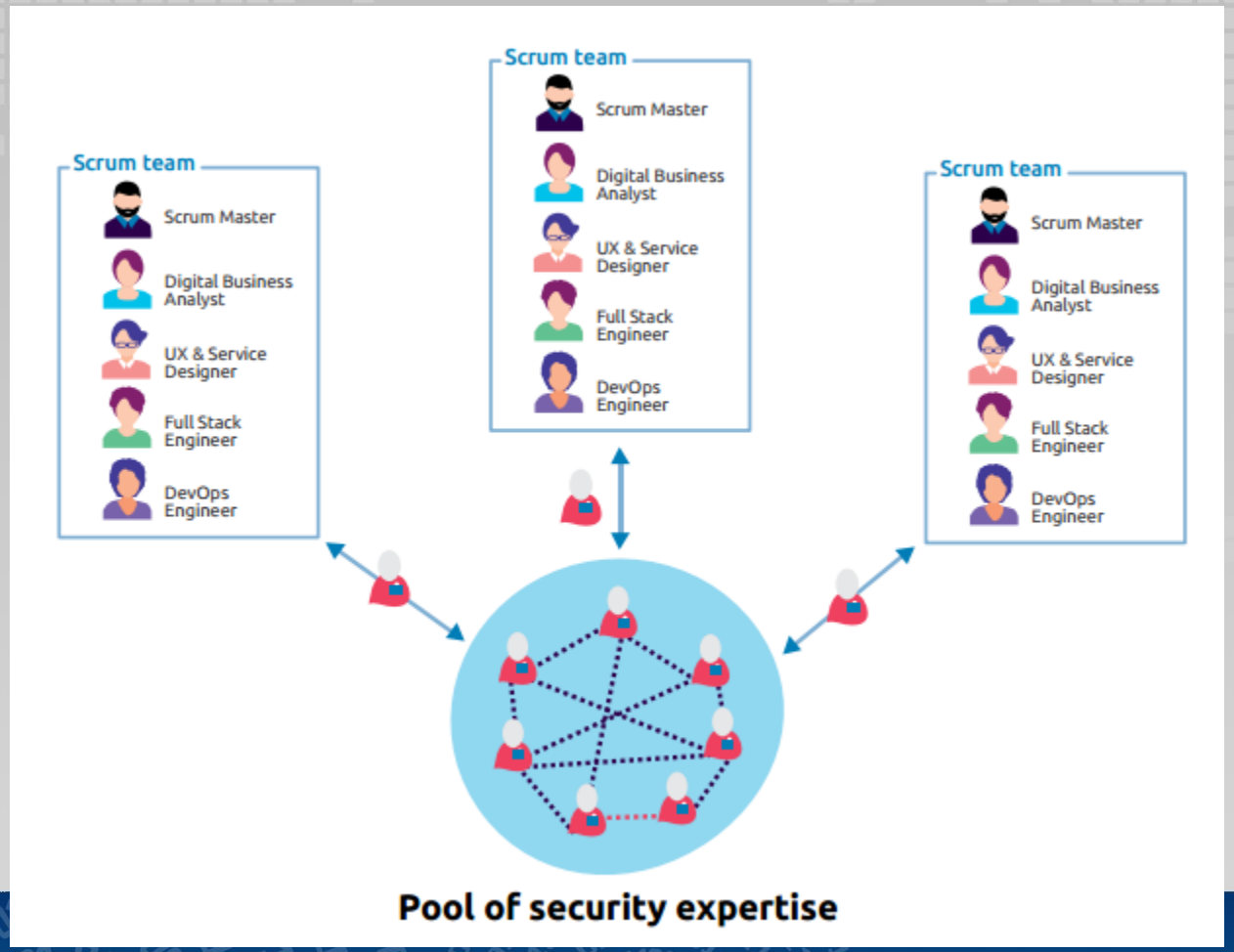


中心化DevSecOps工具链建设

- In the modern engineering world, it's easy to assume that automation is the solution and it's correct that automation is critical
- but it's important to be selective when choosing tools and be careful when deploying them. The goal is to fix issues and not to overload engineers with too many tools or alien processes outside of their everyday engineering experience.

enable organisations to achieve business objectives in an agile and secure manner

安全团队与开发团队

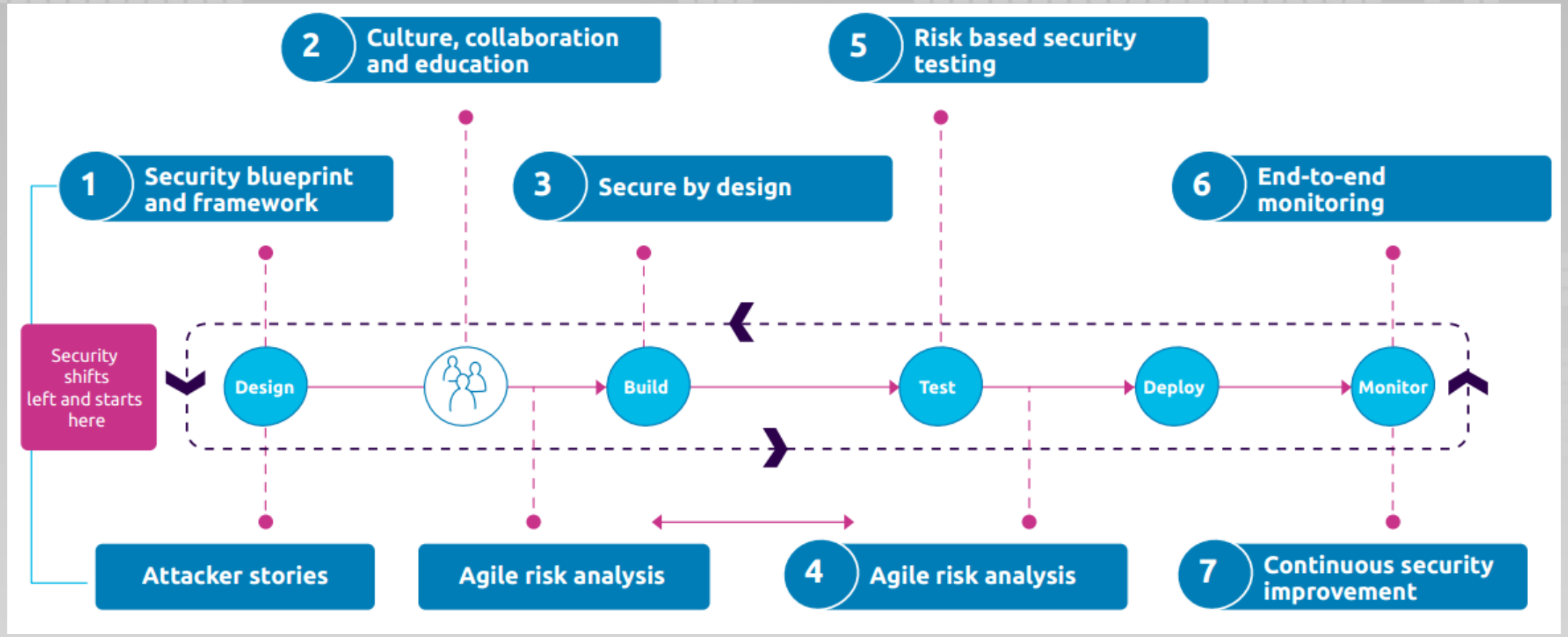


来自于Capgemini Global DevSecOps Insights report 2020

- Educate and empower others rather than policing compliance
- Automate security to help IT and the business achieve their agility goal
- Monitor exceptions rather than police non-compliance

全生命周期中7个安全切入要点

来自于Capgemini Global DevSecOps Insights report 2020



关于Attacker Stories攻击故事

- A set of go-to **‘attacker stories’** should be considered to support developers’ user stories by reflecting what malicious actors could do to compromise product or feature security.
- Code reviews, unit testing and dynamic testing should be targeted according to the attacker stories during design.

业务空间-研发空间组合

- 业务空间-对接业务领域

业务项目

意向

需求

需求关键字段

需求价值　业务产品

提出时间/期望投产时间　　计划/实际上线时间

需求流程

提出-分析-待评审-待排期-已排期----------待验收-验收通过----------投产验证-完成

拆分到1~N故事

创建-安全评审-设计-开发-安全审查-冒烟测试--------系统测试-测试通过-完成

故事流程

故事

开发任务

测试任务

测试缺陷/生产缺陷

关键字段

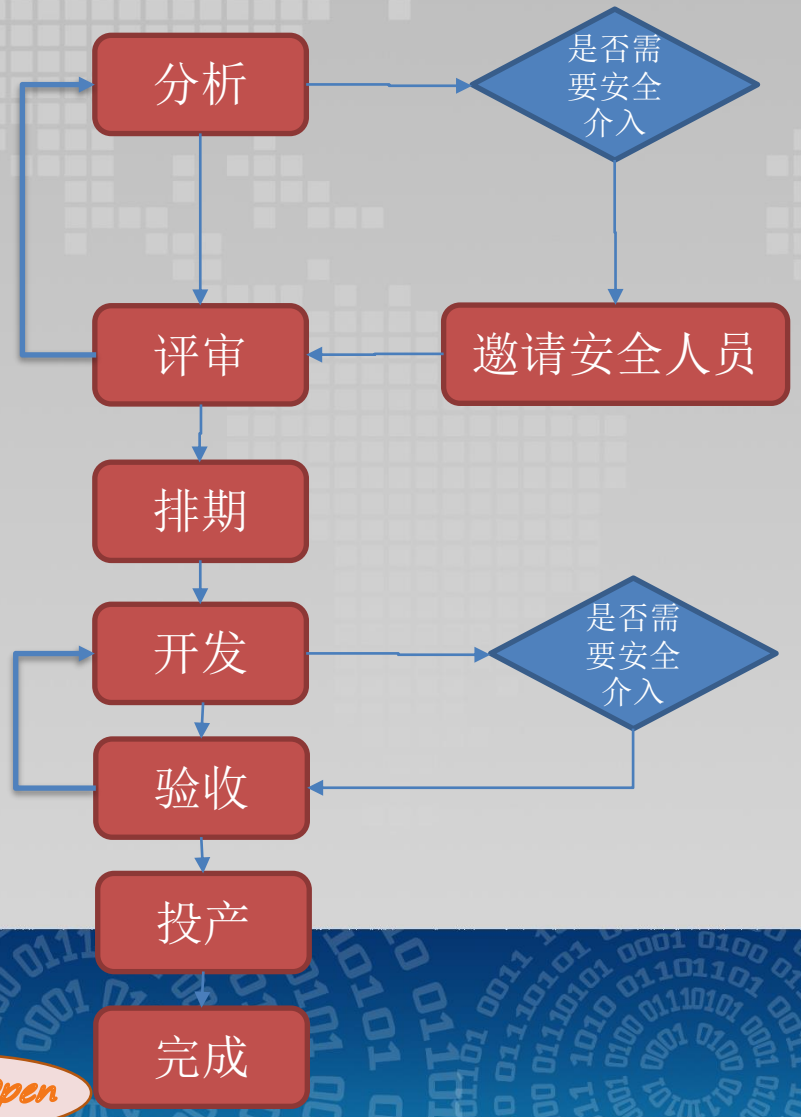
来源于1个需求，　同步业务产品

系统 版本 迭代

所属开发组

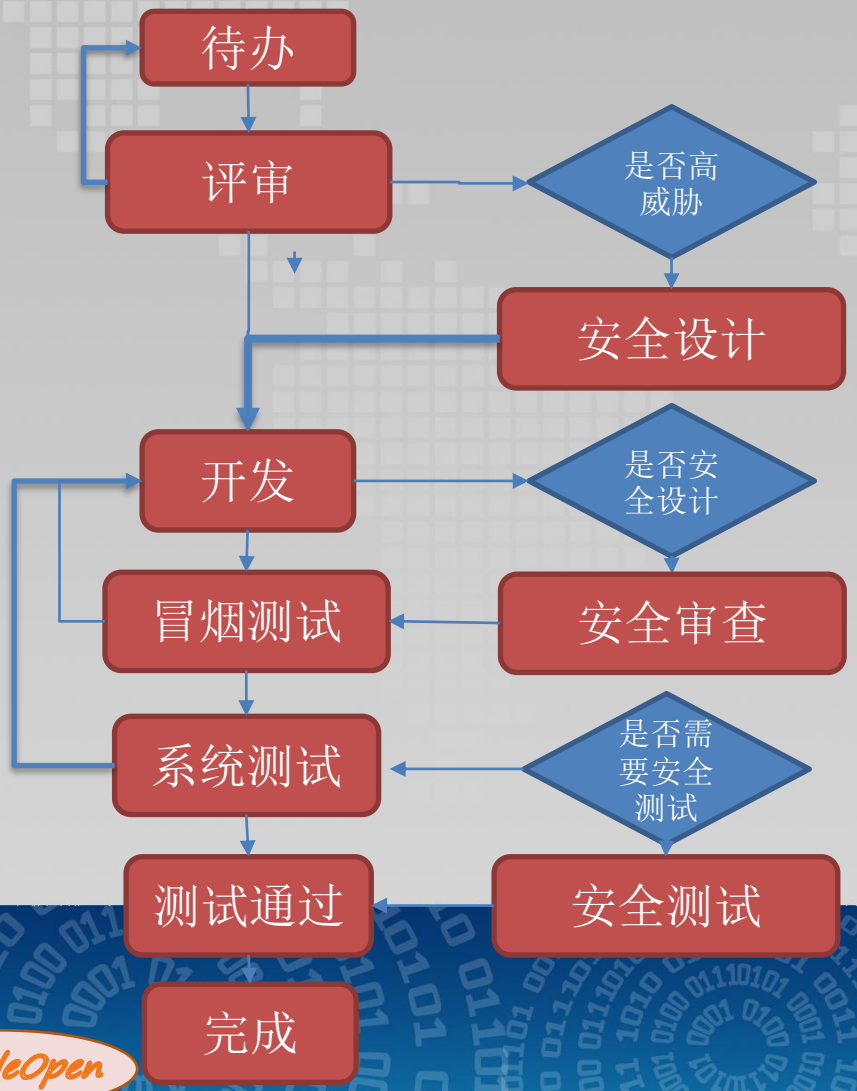
- 研发空间-A小队/B小队/C小队.....

需求按需进行安全活动



- 需求面向业务识别
- 评审焦点在于需求业务价值
- 安全方面评审按需识别后安排

故事按安全威胁等级进行安全活动



- 故事根据系统来识别
- 安全威胁等级判断来源于统一的系统管理工具，给出安全方面判定
- 识别故事面临的安全威胁，如有必要分拆识别专门的安全攻防故事

需求上平衡效率和安全的选择

故事

- 数量巨大
- 细致针对
- 工作量大

系统版本的故事集

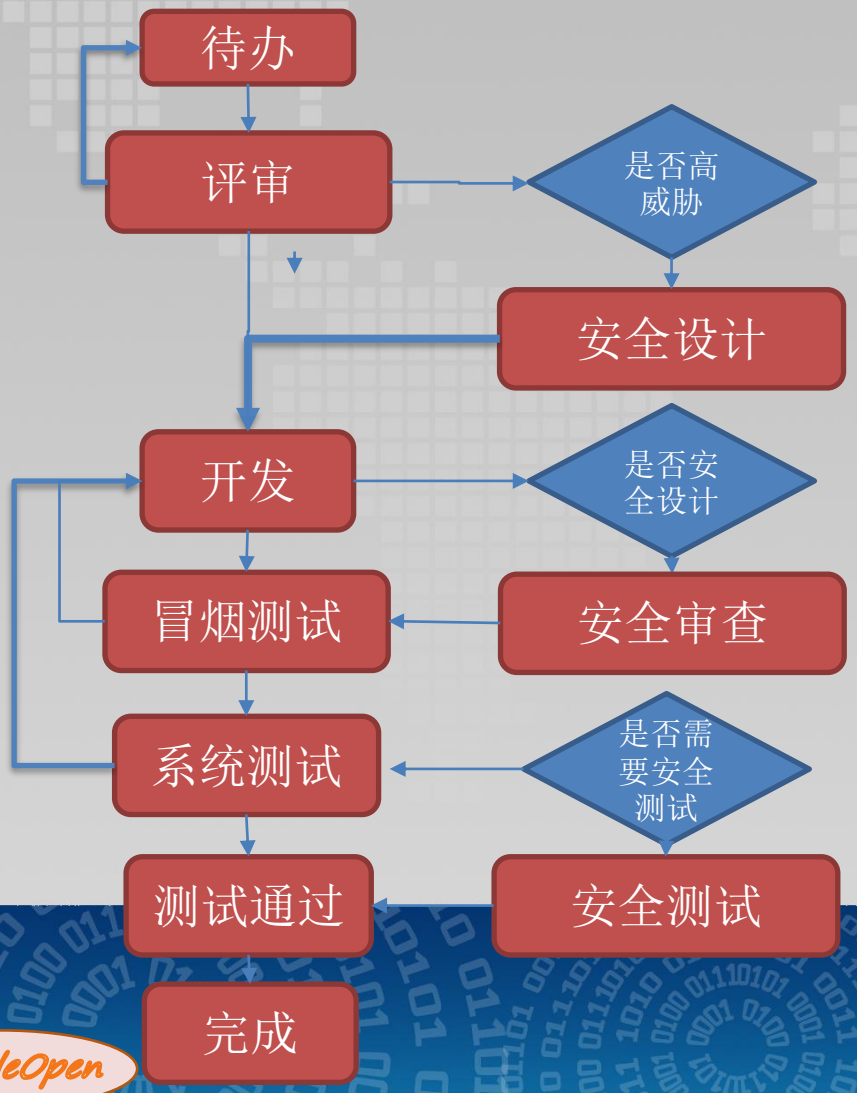
- 数量居中
- 批量操作，针对性差

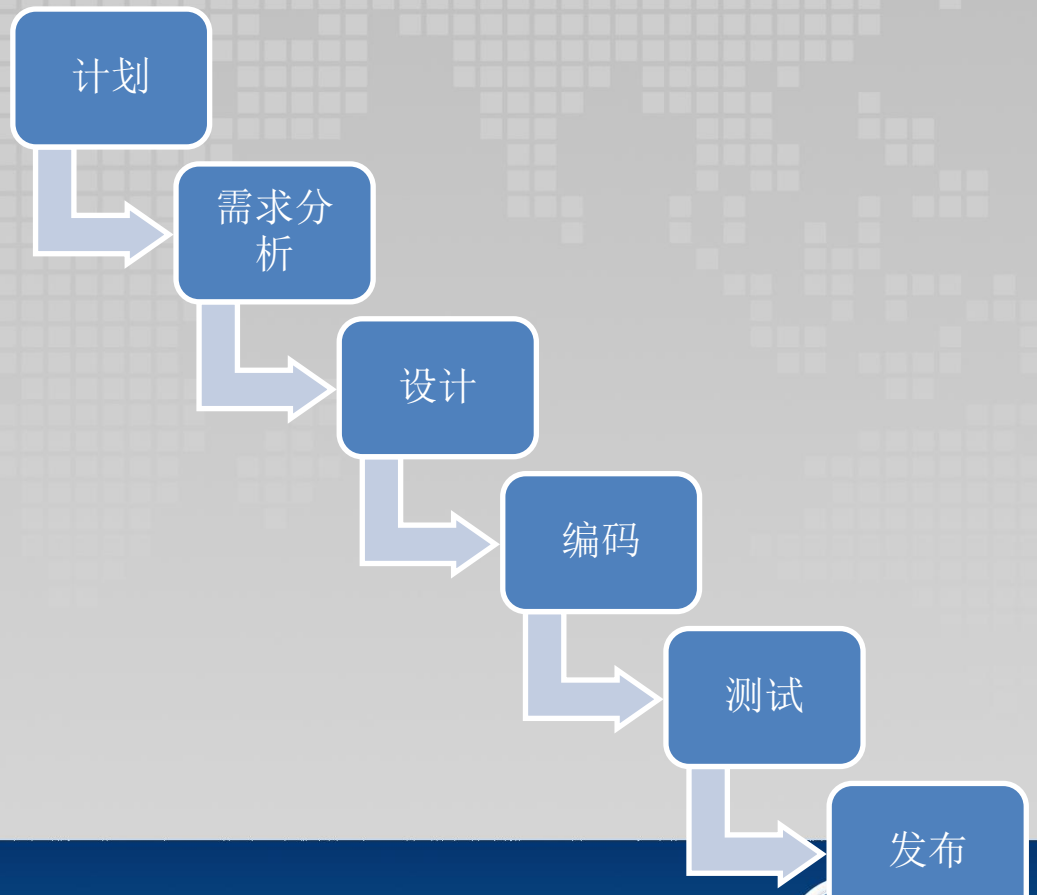
传统SRS

- 数量少-对应于系统
- 滞后

流模式 vs 小瀑布？

- 流程图相差无几？差别在哪里？





权限？

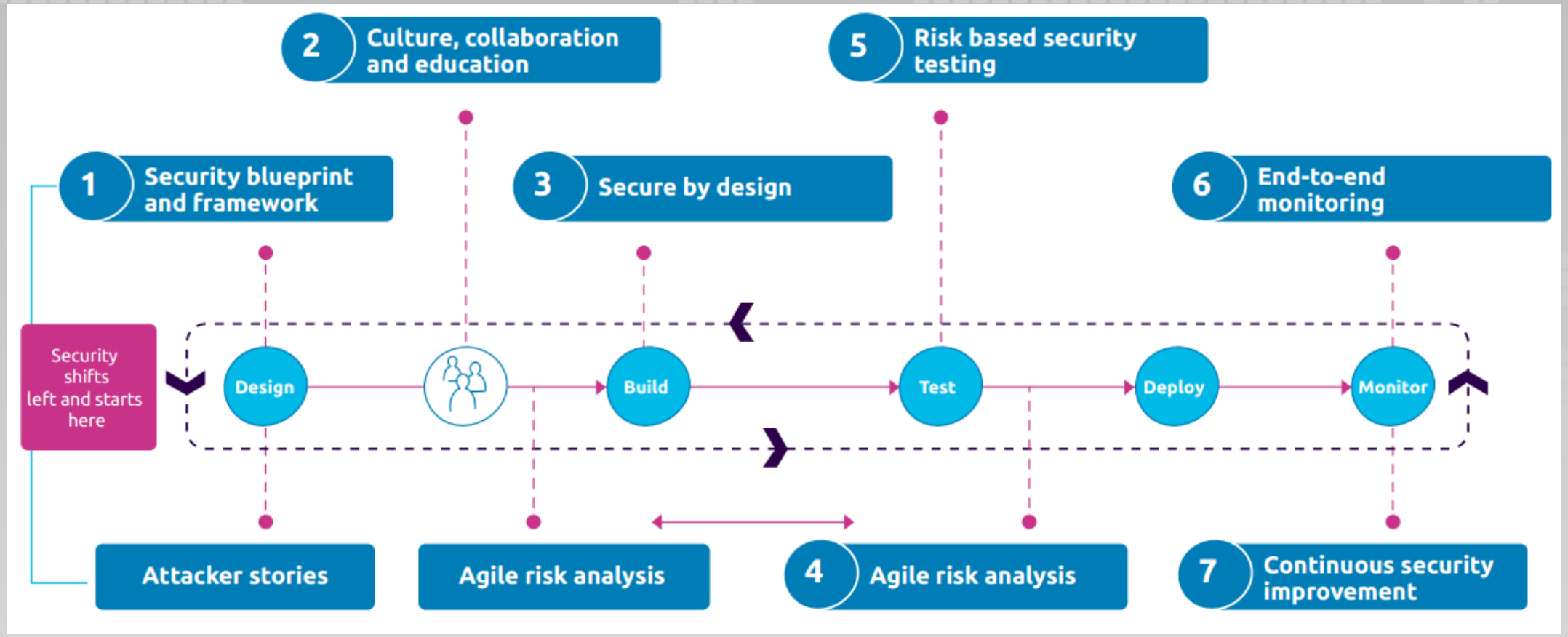
- 敏捷团队建设导向-互相补位
- 利用事后审计来替代前控权限

评审留痕?

- 上传Email或者会议纪要?

全生命周期中7个安全切入要点

来自于Capgemini Global DevSecOps Insights report 2020



软件设计上平衡效率和安全的选择

类

- 数量巨大
- 细致针对
- 工作量大

组件-单个代码工程

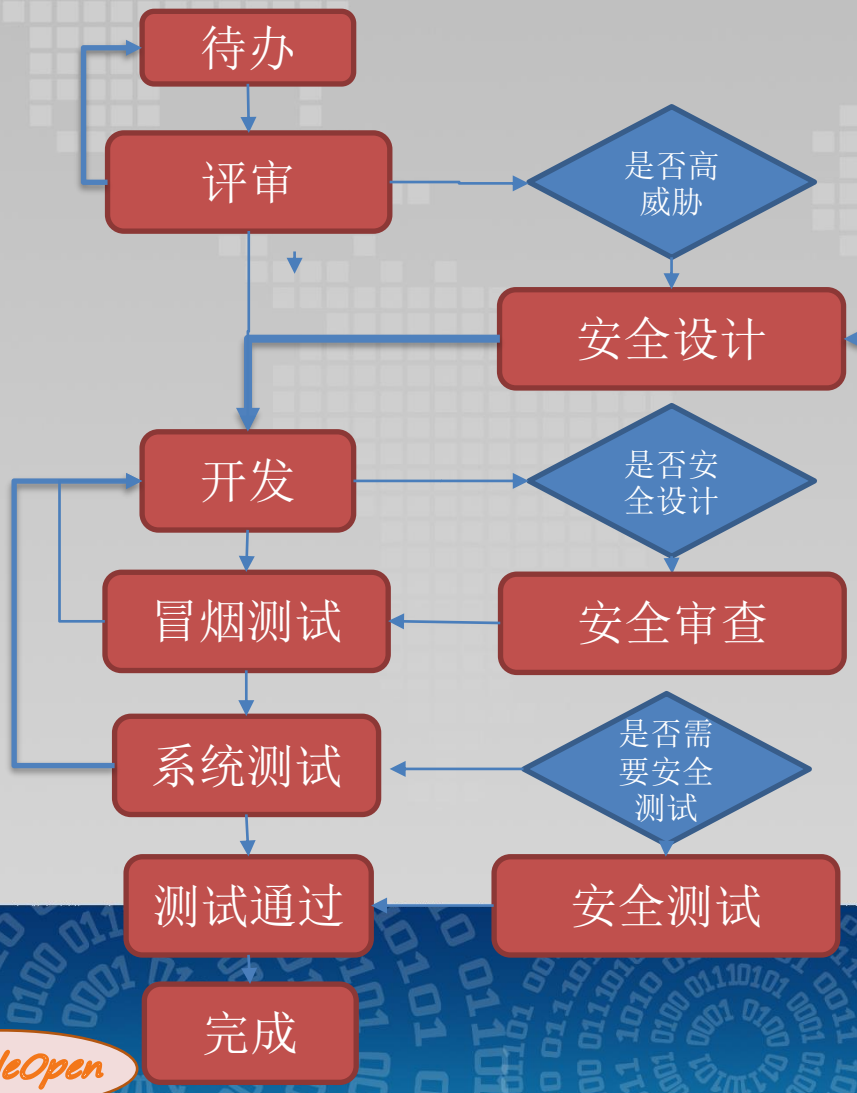
- 数量居中
- **接口API**

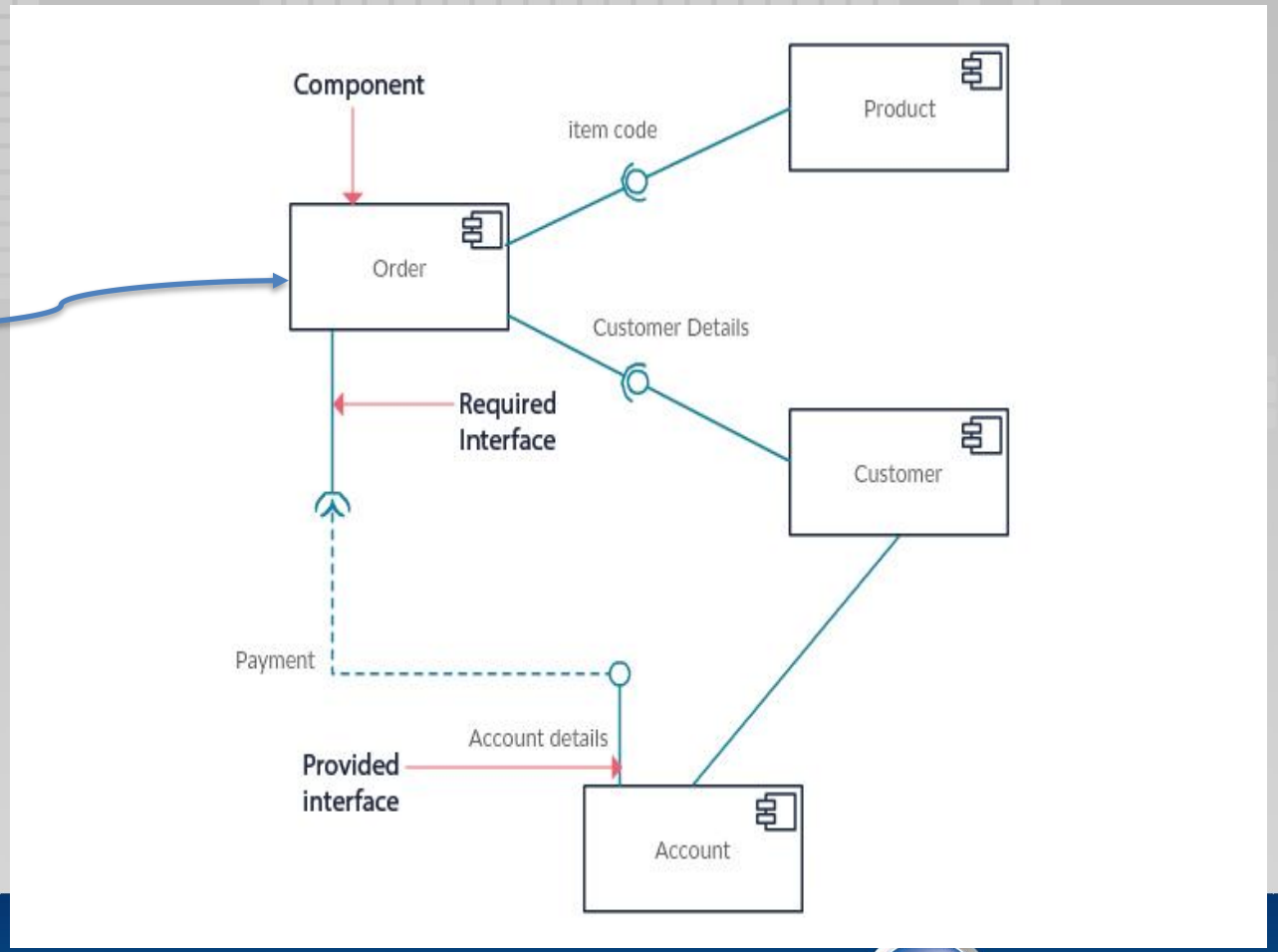
系统

- 数量少
- 接口API

从需求到设计

值得保持追溯性





SimpleOpen

OWASP Open Web Application Security Project

接口API安全设计考察要素实例

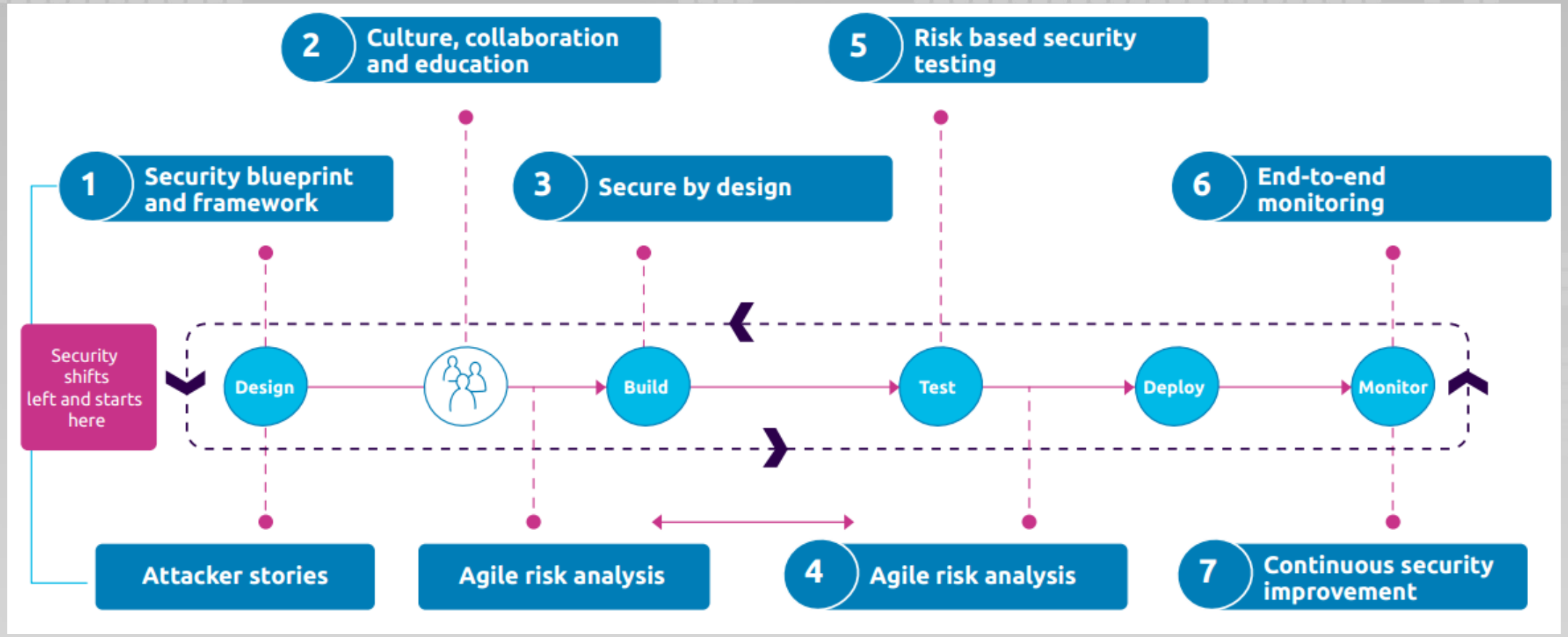
- 输入校验
- 访问控制
- 敏感信息
- 参数化SQL
- 输出编码
- 防短信炸弹
- 资源竞争

设计

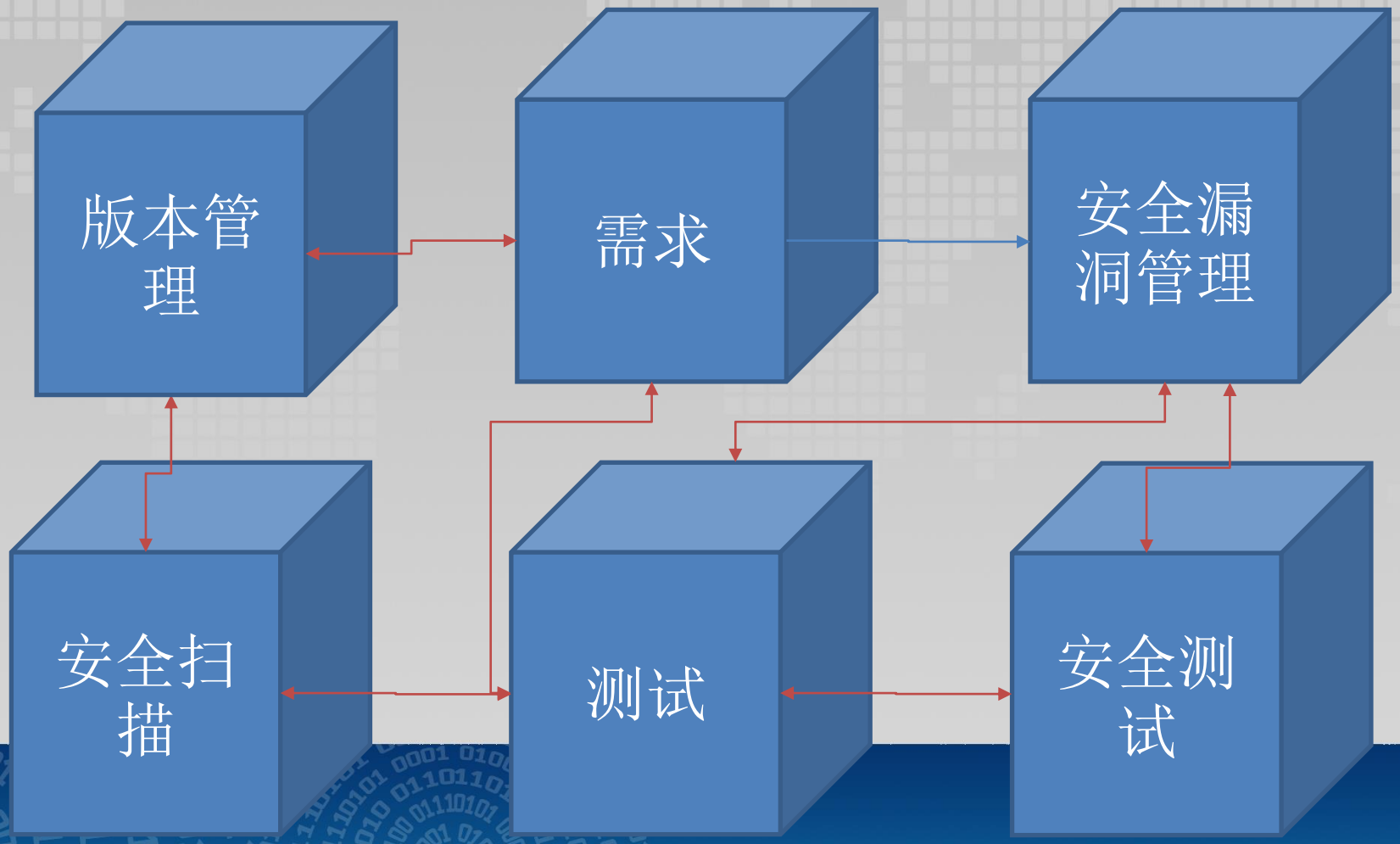
- 不同类型的设计能否整合？
- 组件和接口？
  - 接口管理
  - 非接口管理

全生命周期中7个安全切入要点

来自于Capgemini Global DevSecOps Insights report 2020



DevOps需求-测试-安全工具链



DevSecOps建设策略-保持各层级快速流动

全线上化

- 去掉word
- 去掉附件
- 去掉会议纪要

自动化

- 任何地方都寻求减少手工操作，警惕每个合规要求带来的手工
- 链接工具
- 用机器替代人

自动合规

- 执行中自动留痕
- 不再补文档
- 满足CMMI,SDL,各种合规等保……

网安加学院