DevOpsDays

Shanghai

— 2017.8.18-8.19 —

上海龙之梦酒店（长宁区延安西路1116号）

主办单位：

DevSecOps 三问：Why? What? How?

宗良
文思海辉 信息安全助理副总裁

宋良

文思海辉
信息安全助理副总裁

个人介绍：

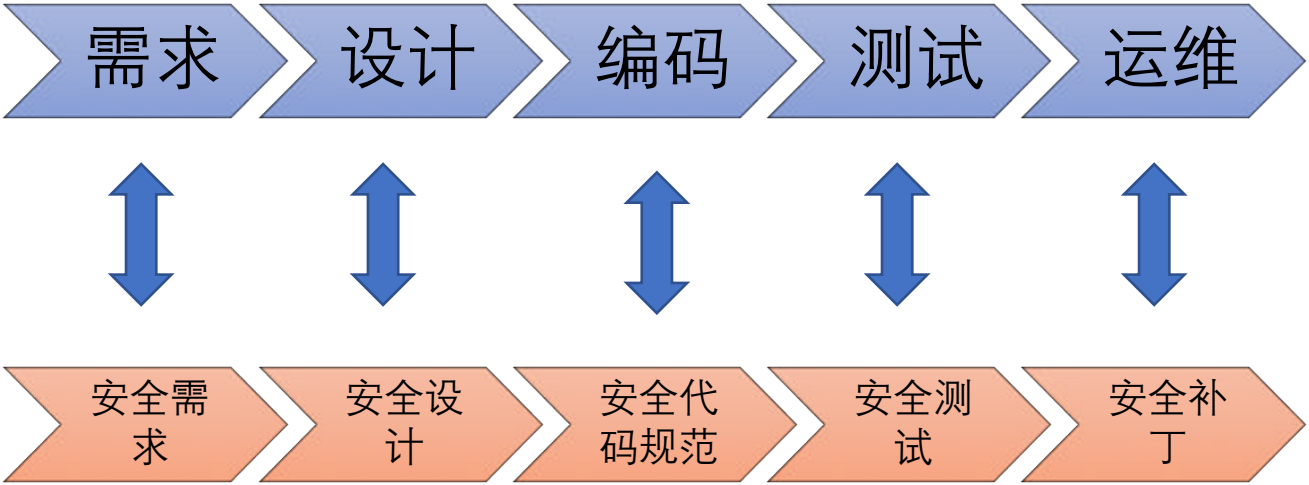
现任文思海辉信息技术有限公司全球信息安全与风险办公室信息安全助理副总裁，负责文思海辉全球信息安全内控，以及对外的集成安全服务。

15年以上从业经验，对软件开发/测试，服务与项目管理，信息安全与风险管控，质量与流程体系，培训体系与培训实施等多个方面都有深入理解与实际操作。

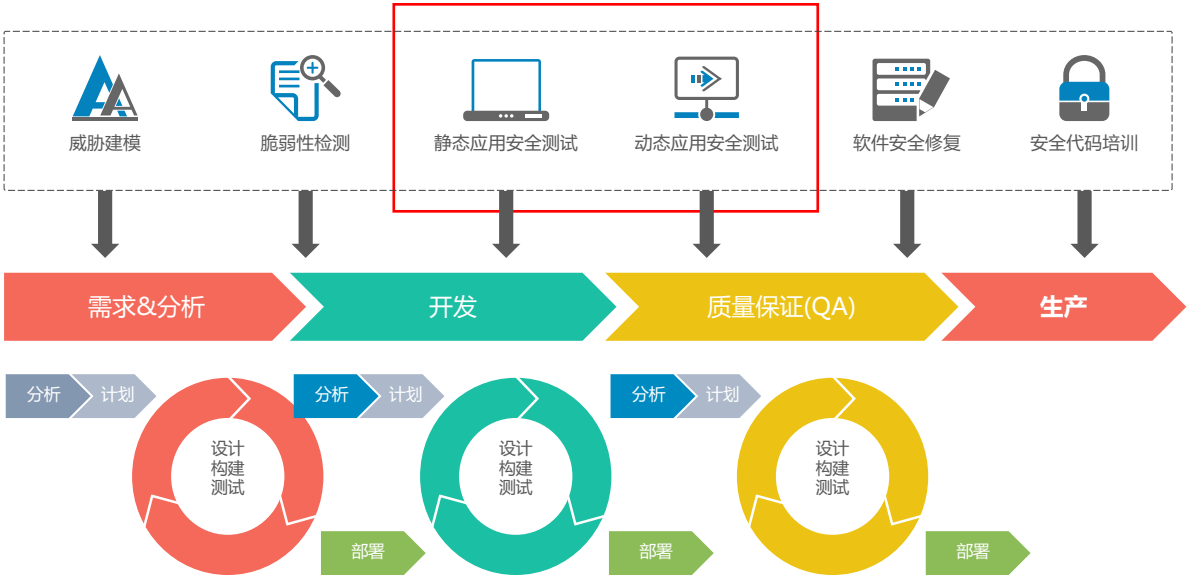
目录

传统的SDLC 与传统的应用安全

瀑布模型为例

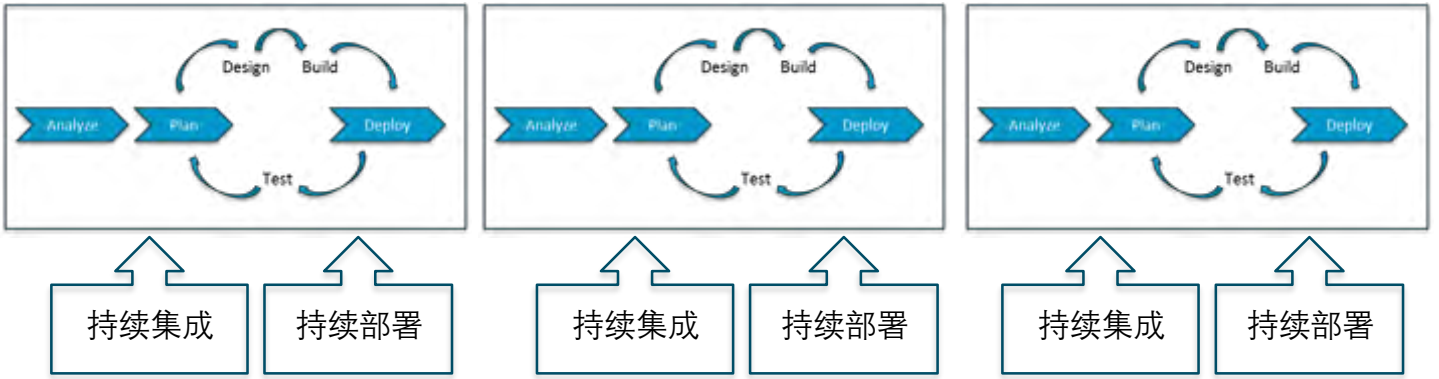


敏捷模型对应的应用安全



标准的 DevOps 与 应用安全

DevOps ---- Faster & Faster



CI & CD 之下，安全如何立足？

SecOps

- BMC 公司，2016年推出
- 作为一种 Service Offering
- 核心理念：
  自动化（Automation）是解决安全（Security）与运营（Operation）之间鸿沟的主要手段。

SecDevOps

- Stevan Arychuk
- 2015-08-17
- 核心理念：
  Inject/Embed Security Into DevOps
  在早期引入必需的风险建模（Risk Modeling）、威胁评估（Threat Assessment）与渗透测试（Penetration Test）。

DevSecOps

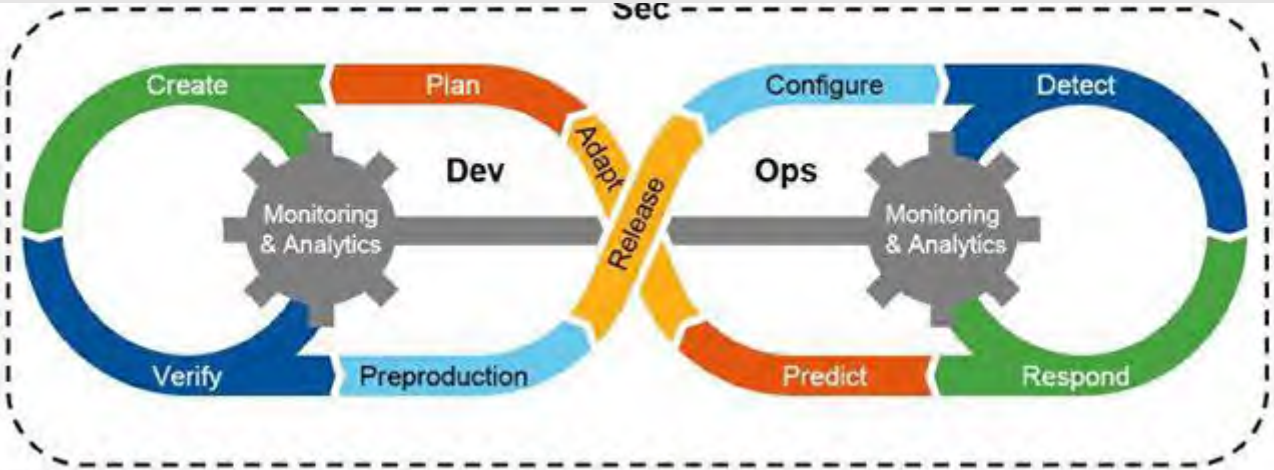
- SANS, 2016 年3月
- Whitepaper
- 核心理念：
  Co-exist of DevOps & Information Security

目录

DevSecOps 的概念

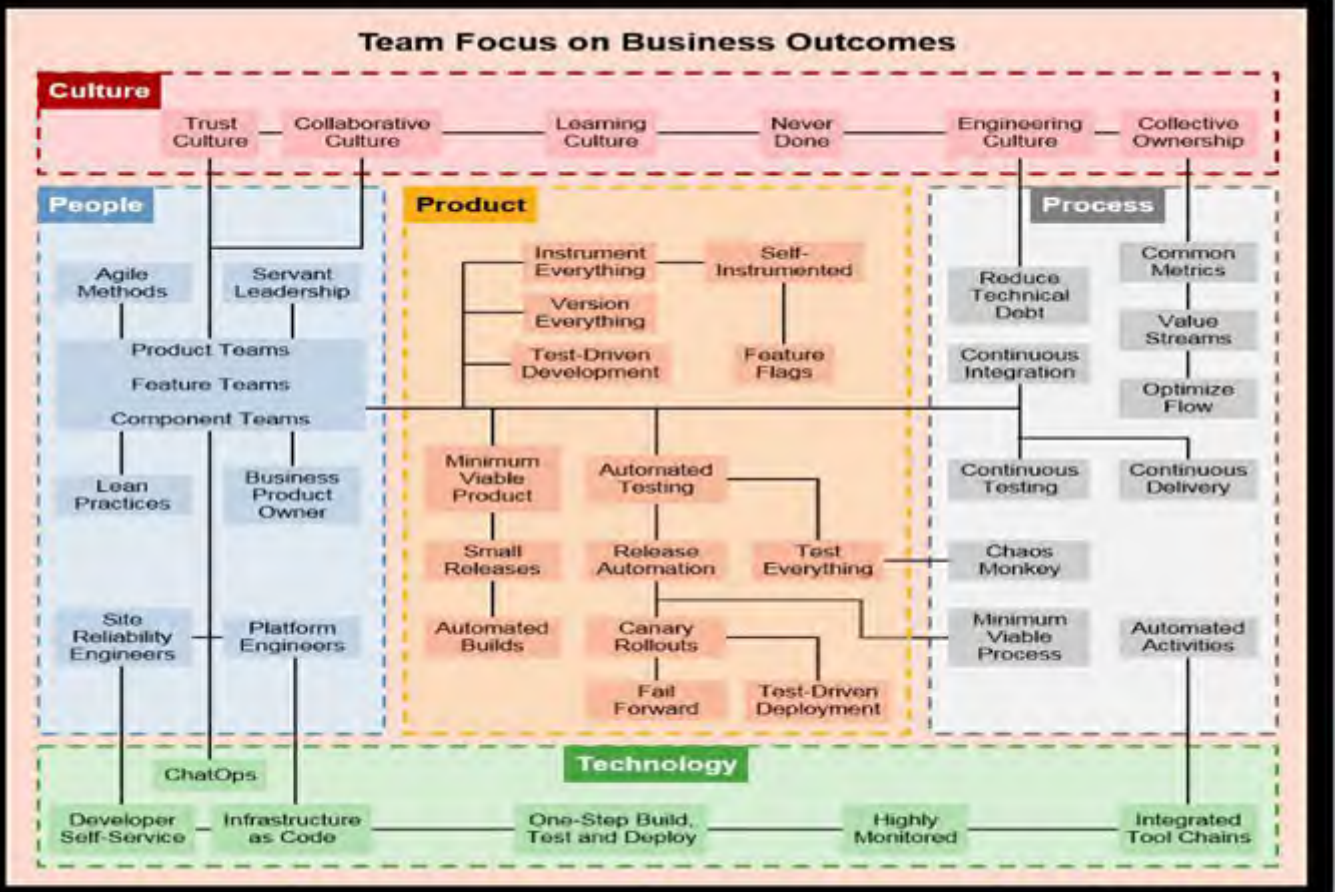
DevSecOps strives to **automate core security tasks** by **embedding** security controls and processes into the DevOps workflow.
DevSecOps originally focused primarily on automating code security and testing, but now it also encompasses more operations-centric controls. Security can benefit from automation by incorporating logging and event monitoring, configuration and patch management, user and privilege management, and vulnerability assessment into DevOps processes.

------ *Sourced from SANS*

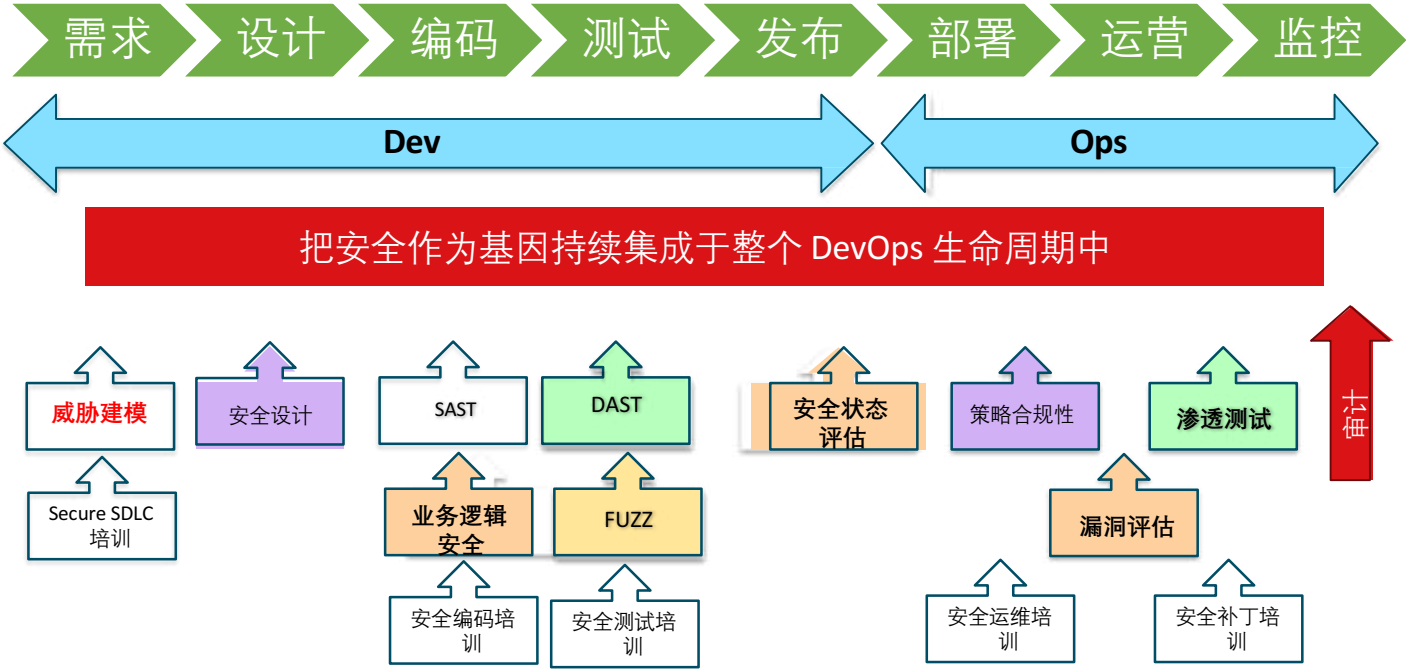


Source: Gartner (September 2016)

DevSecOps 聚焦



DevSecOps = DevOps + Security Embedded



目录

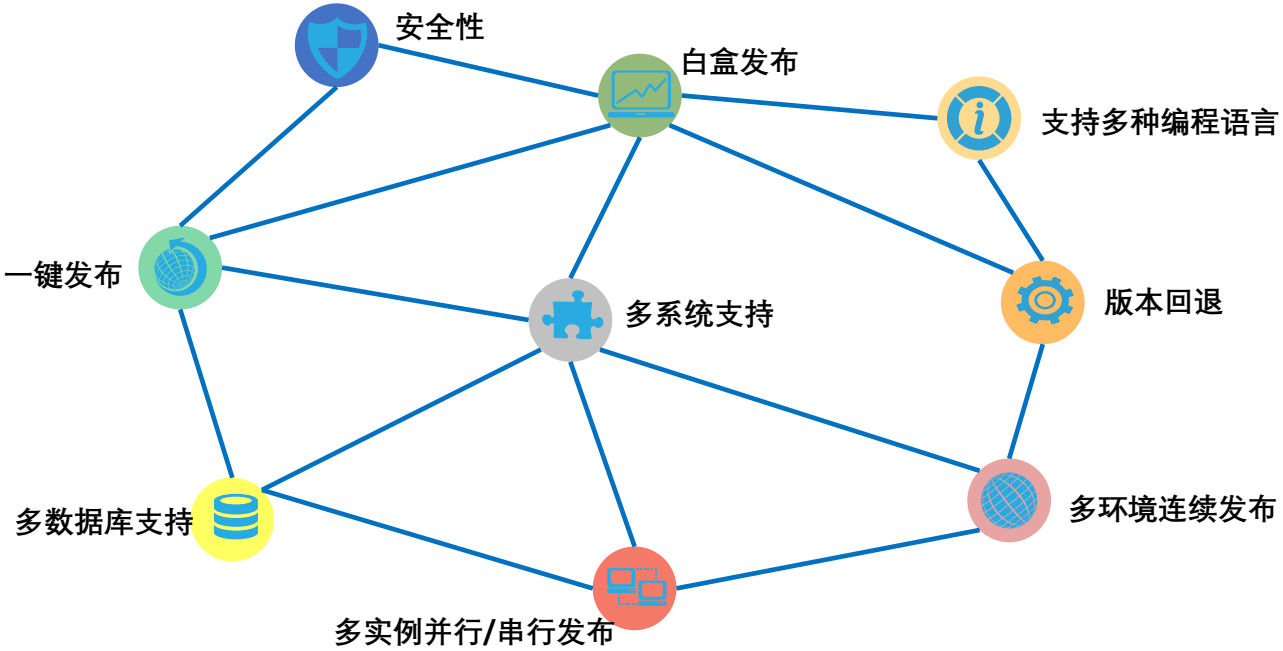
How to Design DevOps

How to Integrate Security

How to Automate & Self-Driven

How to V & V

安全的自动发布特性


安全性
白盒发布
支持多种编程语言
一键发布
多系统支持
版本回退
多数据库支持
多环境连续发布
多实例并行/串行发布

安全控制特性

安全性

- 全新防护机制，实时自动化代码安全扫描
- 主机、数据库等账号密码统一加密存储
- 发布用户仅有发布、启停应用等权限，无其他直接控制权限
  - Linux/Unix采用ssh传输应用软件包，Windows采用winrm+https验证传输

白盒发布

- 发布状态实时显示，真正可视化发布
- 发布过程可交互，用户可随时根据发布状态选择中止或取消发布

版本回退

- 应用发布过程中可随时中止，自动回退到任何指定的稳定版本
  - 数据库脚本回退

实例问题感悟

版本管理和发布存在的问题:

- 自动发布的代码未经安全检测，安全隐患漏出率过高，多次收到上级主管部门警告
- 以时间作为版本号，缺少版本号规则和规范，容易导致发布错乱
- 配置文件存放目录没有相应规范目录，环境相关配置存在多个文件中，导致应用发布复杂度增加
- 缺乏统一的编译工具，容易导致发布的应用不一致
- 没有建立开发分支，不支持并行项目，当存在并行项目时，很容易出现代码混乱
- 手工发布应用，交付时间长，效率低

教训:

由于存在左边所述的问题，某客户在以往的应用发布过程中频繁发生故障，例如:未测试的错误代码被发布到生产环境，甚至发生了已修复的Bug在生产环境中重复出现的重大生产故障，给客户的业务开展造成重大损失，曾经被上级主管部门直接书面警告

DevSecOps 未来可以整合的元素

延伸推荐内容

组织或作者	标题
BMC	SecOps Solutions Help Teams Address Critical Security Vulnerabilities
Stevan Arychuk	SecDevOps: Injecting Security Into DevOps Processes
SANS	A DevSecOps Playbook
Chris Carlson	DevSecOps – Building Continuous Security into IT and App Infrastructures
GitHub	Awesome DevSecOps
Pactera	Pactera DevSecOps Security Product Service Guide - 2017

高效运维社区
GreatOPS Community

会议

- 8月18日 DevOpsDays 上海
- 全年 DevOps China 巡回沙龙
- 11月17日 DevOps金融上海

培训

- EXIN DevOps Master 认证培训
- DevOps 企业内训
- DevOps 公开课
- 互联网运维培训

咨询

- 企业DevOps 实践咨询
- 企业运维咨询

商务经理：刘静女士
电话 / 微信：13021082989
邮箱：liujing@greatops.com

Thanks

荣誉出品

高效运维社区

国际最佳实践管理联盟

想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好