GOPS2017 Shanghai

GOPS

GOPS 全球运维大会 2017 上海站

指导单位：数据中心联盟 Data Center Alliance

主办单位：高效运维社区 GreatOPS Community　开放运维联盟 OOPSA Open OPS Alliance

大会时间：2017年11月17日-18日

大会地点：上海光大会展中心国际大酒店（上海徐汇区漕宝路67号）

GOPS2017
Shanghai

业务安全-DevSecOps的催化剂

赵锐 IT风控高级经理

讲师介绍

上海首席安全官联盟成员、银联认证讲师，曾在国有金融机构担任安全主管、移动产品经理、信息安全专家等职务。
专业领域：**互联网金融业务风险管理**、**信息安全管理**、**账户安全管理**、**开发安全管理**
赵锐拥有10余年资深金融科技工作经验，10余年金融科技风险管理工作经验，深入了解国内外金融行业信息安全标准与要求。工作期间多次代表单位参加信息安全技能竞赛并获二、三等奖；负责的信息安全等级保护工作多次获得上海市优秀奖；工作期间多次被评为优秀员工。
拥有PMP、CISM、CISP、CISAW（二级）、中级经济师、ISO27001审核员、ISO20000审核员、ISO9001审核员等多项资质认证。
曾在银监会《金融科技治理与研究》杂志发表论文《“互联网+”环境下银行信息安全风险之应对》。

DevSecOps的困境

鄙视链-安全是麻烦制造者？

- 整天提安全需求
- 增加开发工作
- 增加运维要求
- 增加不确定性
- 延后业务上线

DevSecOps的困境

安全是为了满足合规要求？

- 法律要求
- 法规要求
- 监管要求
- 合同约束

中华人民共和国
网络安全法
含草案说明

DevSecOps的困境

安全是因为出事了？

- 安全事件
- 业务倒逼
- 外部诉讼

信用服务公司Equifax数据泄露 涉及1.43亿用户

互联网　腾讯科技　2017-09-08 10:48　收藏　1 评论　分享

腾讯科技讯 数据泄露事件现在已经变得越来越常见，以至于当我们再次看到有公司的用户数据被泄露的新闻时，都已经变得习以为常。美国信用服务公司Equifax今天宣布公司数据遭到黑客攻击并泄露，并且可能会涉及1.43亿用户。

DevSecOps的困境

安全是风险管理

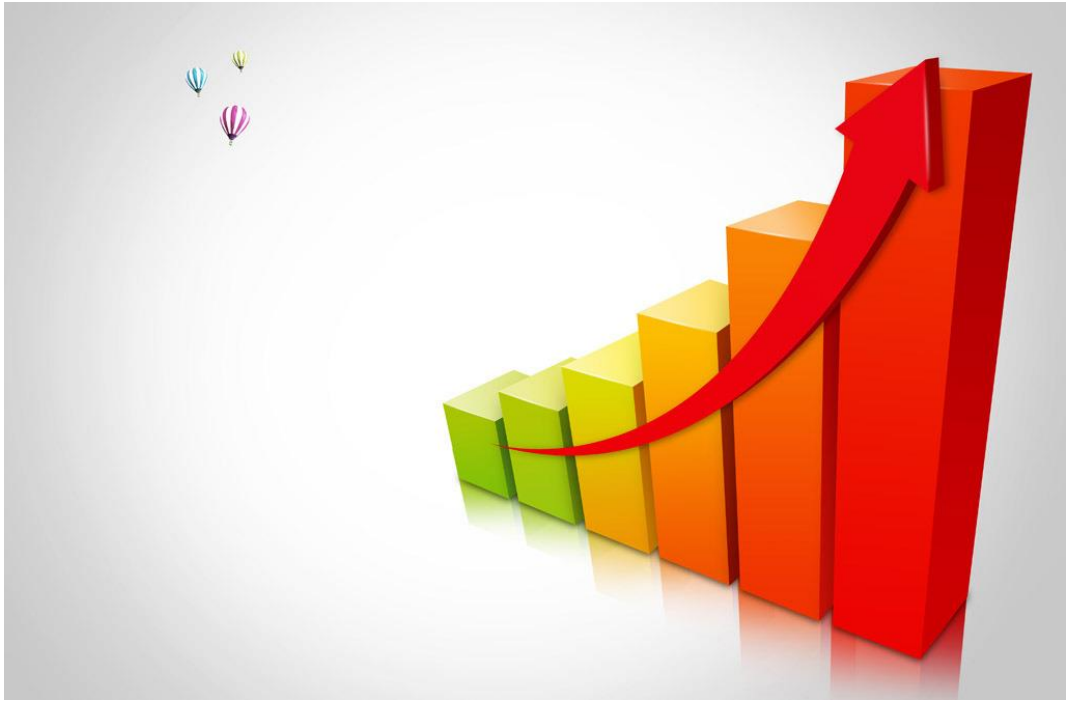
- 业务风险
- 感知风险
- 业务价值

目录

公司的关注点-高层

GOPS2017
Shanghai

1. 公司的发展
   - 使命愿景
   - 战略发展
   - 商业目标
2. 业务安全
   - 风险
   - 成本
   - 影响



公司的关注点-业务部门

1. 换位思考
   - 影响-短期增加工作量、中长期减少业务事件处理工作
   - 收益-降低业务风险、提升正常用户的体验、增加业务收入
2. 双赢思维

公司的关注点-科技部门

1. 换位思考
   - 影响-增加培训工作、增加开发和运维工作量、提升开发运维人员工作价值
   - 收益-提升代码质量、降低安全事件发生率、减少修改BUG的次数、保障稳定

2. 双赢思维

目录

什么是DevSecOps

2012年，Gartner介绍了DevSecOps的概念（最初使用“DevOpsSec”）

2017年RSA年度会议上DevSecOps成为热门词汇。

来源：gartner.com, rsaconference.com

DevSecOps的特点

1. 每个人都对安全负责
2. 高层决策
3. 科技团队之间相互协作
4. 专注于风险，而非安全

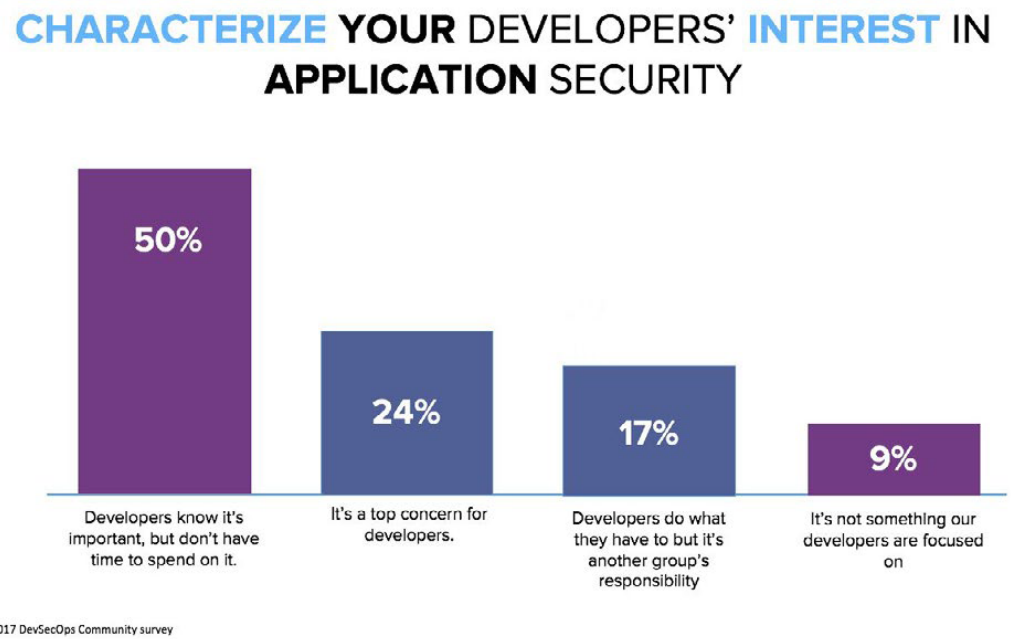
来源：gartner.com,

devsecops.com, sonatype.com

DevSecOps的现状

开发人员对应用安全的兴趣情况

2017年2月，Sonatype进行了DevSecOps社区调查，有超过2200名IT专业人员参与。 调查显示，成熟的开发组织确保自动化安全性在早期，到处，大规模中融入DevOps实践中。

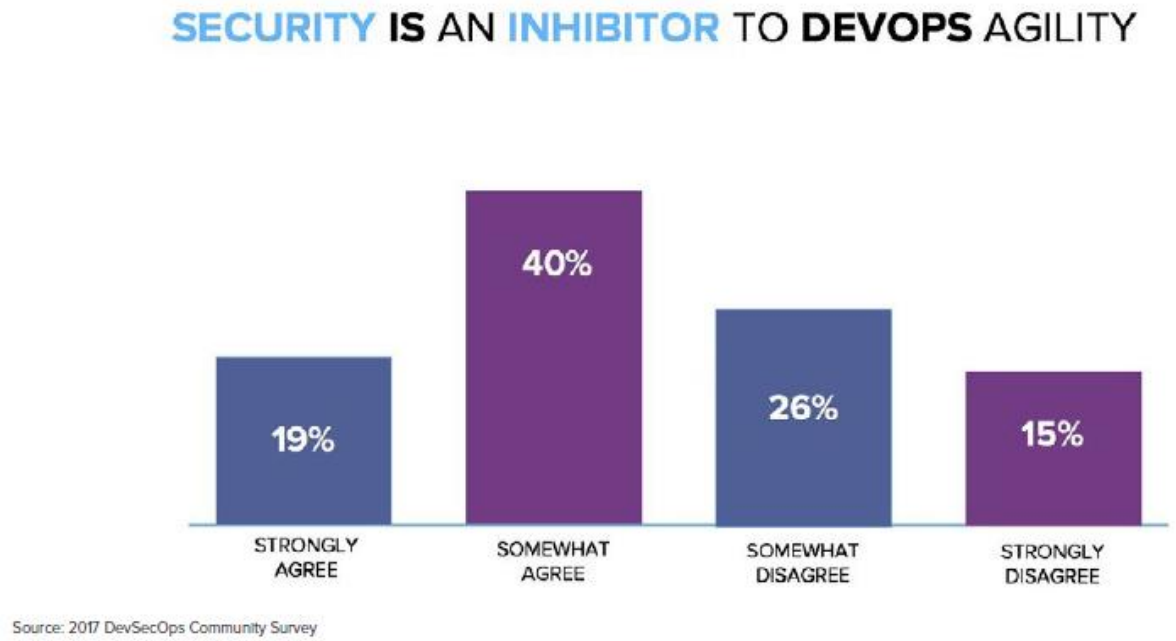


来源：sonatype.com

DevSecOps的现状

安全性是抑制灵活性的一个因素。

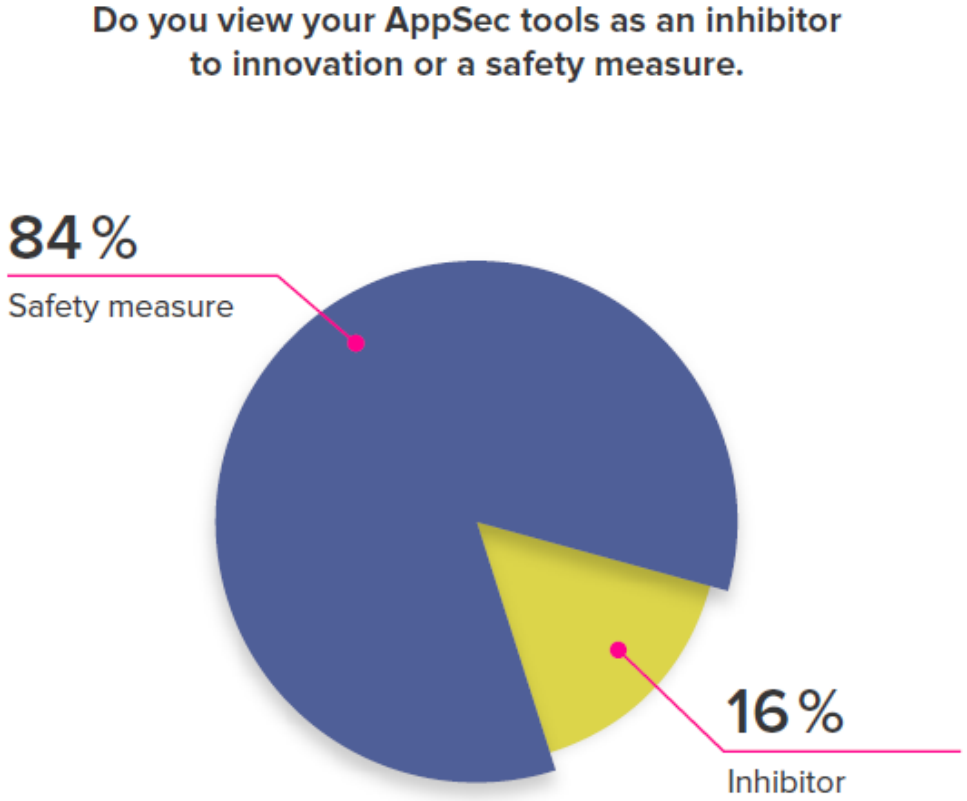
来源：sonatype.com



DevSecOps的现状

应用安全工具是抑制创新

还是安全措施。



来源：sonatype.com

DevSecOps -把握底线

1. 什么可以做
2. 什么不可以做

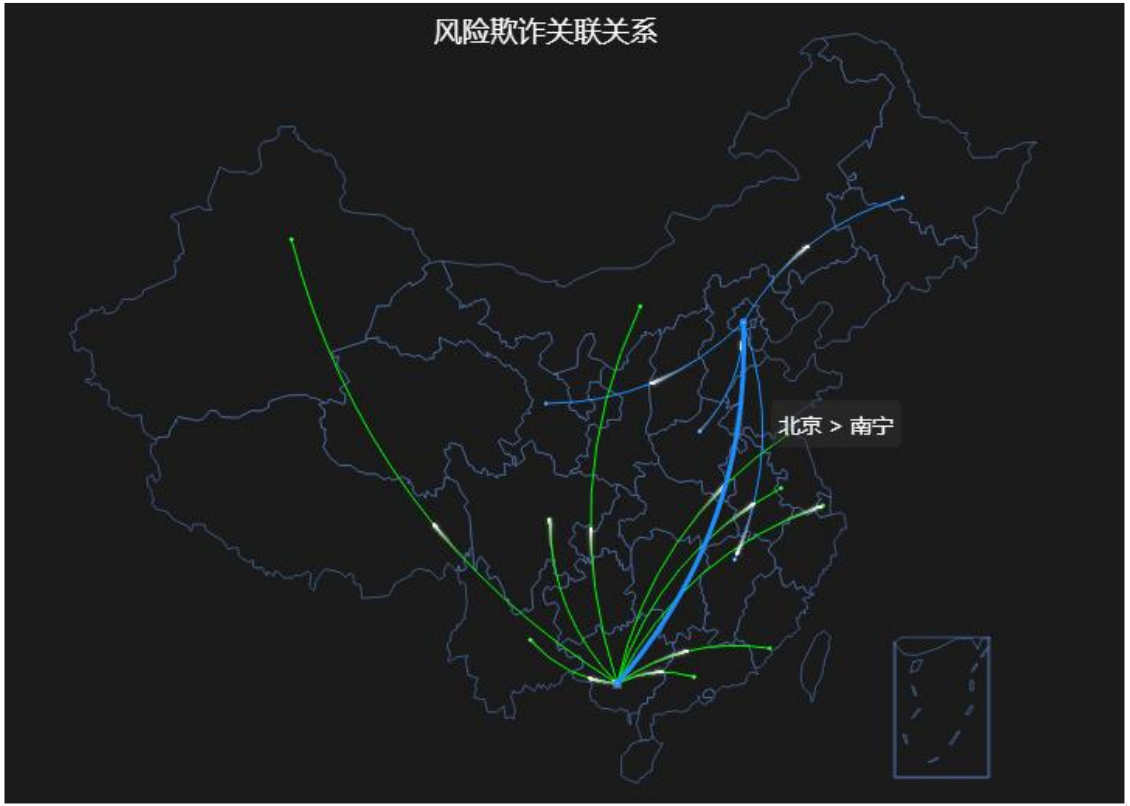
DevSecOps -基线管理

1. 基线（业务、系统）
2. 按业务的增强要求

DevSecOps –可视化

GOPS2017
Shanghai

1. 直观易懂
2. 帮助管理层
3. 帮助业务团队
4. 帮助各科技团队
5. 体现大家的成果



DevSecOps –团队

GOPS2017
Shanghai

1. 21世纪人才最贵
2. 团队成长
3. 职业发展

目录

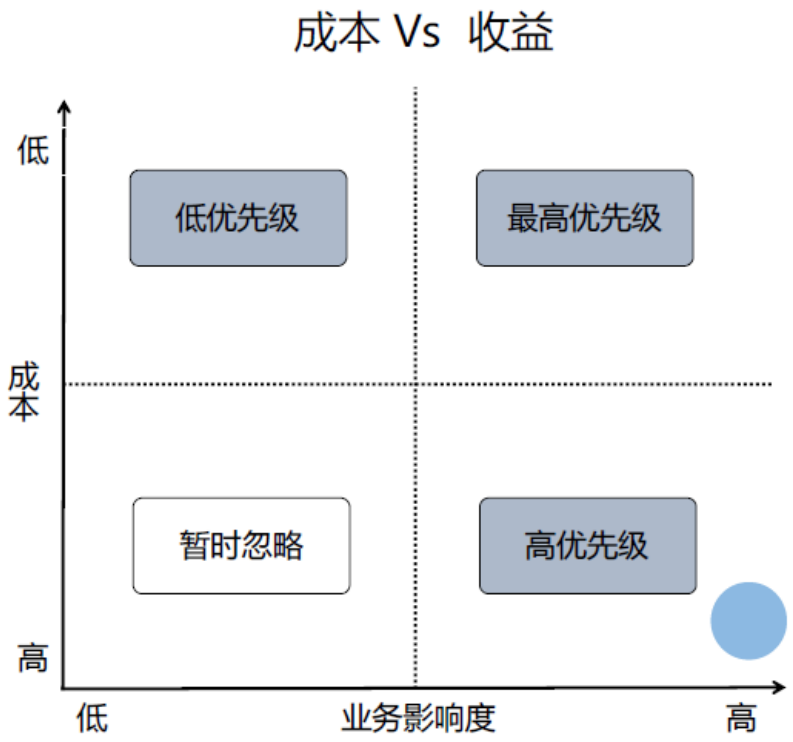
什么是业务安全

业务安全是指保护业务系统免受安全威胁的措施或手段。广义的业务安全应包括业务运行的软硬件平台(操作系统、数据库等)、业务系统自身(软件或设备)、业务所提供的服务的安全;狭义的业务安全指业务系统自有的软件与服务的安全。

业务安全

业务安全目标

- 支持公司战略
- 保障业务发展
- 减少资金损失



原来的软件安全

1. 满足业务功能需求
   - 功能第一
   - 只符合部分安全配置基线
   - 有基础的代码安全要求
   - “安全”是敏捷的拦路石
   - 缺少业务安全管理

业务安全的催化作用

GOPS2017
Shanghai

1.安全地满足业务功能需求

- 联合提出安全需求
- COO、CRO、CTO、CSO的合作
- 业务风控与信息安全结合
- 业务场景安全
- 安全更好融入DevOps

业务安全的催化作用

2.从被动到主动

- 减少攻击面
- 减少资金损失
- 完善SDLC
- 主动提出安全要求

业务安全的催化作用

3.我们的成果

- 业务、开发都有业务绩效
- 开发激励安全、风险和业务提出更好的安全需求
- 完善SDLC

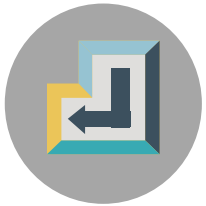
业务安全的催化作用

一、设计产品雏形

- **交付**：产品描述、产品设计、业务模块、财务模块、业务安全模块、基础安全模块等八大内容分析、整体环境与目标市场分析

二、验证产品价值

- **交付**：产品价值主张验证计划、业务测试以及风险验证



三、威胁分析综合评估与结论

- **交付**：综合评估后的结论与建议

业务安全的催化作用

01 产品描述

02 产品设计

03 业务模块

04 财务模块

05 业务安全控制模块

06 基础安全控制模块

07 清结算模块

08 产品运营模块

业务安全的催化作用-后续

- 结合业务场景不段梳理业务安全需求
- 结合业务完善基础安全要求
- 结合业务调整系统架构
- 自动输出开发安全要求、业务安全要求、运维安全要求
- 提升自动化测试的覆盖率，基础：代码安全扫描、安全基线扫描（操作系统、中间件、数据库、网络设备）、WEB应用扫描、移动APP安全扫描

GOPS2017
Shanghai

Thanks

高效运维社区

开放运维联盟

荣誉出品

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