



GOPS2018
Shenzhen

GOPS

全球运维大会 2018

2018.4.13-4.14

中国·广东·深圳·南山区 圣淘沙大酒店（翡翠店）





GOPS2018
Shenzhen

业务安全与DevSecOps的最佳实践

赵锐（锐少） 高级经理

讲师介绍



GOPS金牌讲师、国家网络安全宣传周校园安全讲师、中国信息安全竞赛组委会专家、首席安全官联盟网络安全公益达人。

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**

拥有CISM、CEH、CISP、CISAW（二级）、PMP、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》，参与(ISC)²安全书籍翻译、校审。



GOPS2018
Shenzhen

目录



1

困境

2

业务安全与DevSecOps

3

最佳实践的要素

4

实施最佳实践项目



GOPS2018
Shenzhen

困境？

时间紧任务重

- 业务要求快速上线
 - 保障基本功能测试
 - 减少安全测试
 - 功能快速迭代
 - 上线再改
 - 开发新功能





GOPS2018
Shenzhen

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





GOPS2018
Shenzhen

目录

1 困境

➔ **2** 业务安全与DevSecOps

3 最佳实践的要素

4 实施最佳实践项目



GOPS2018
Shenzhen

我们为什么工作？

1. 生存需求

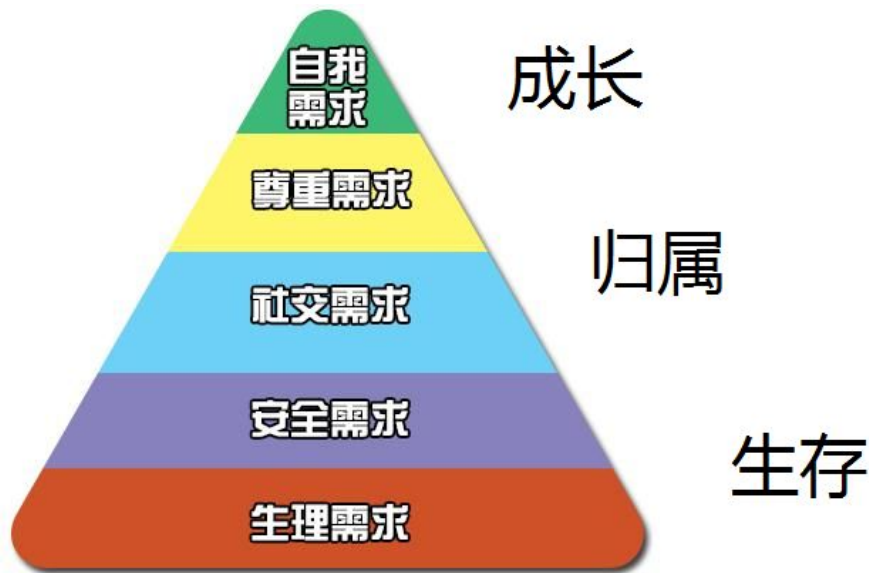
- 穷！困难群众

2. 归属

- 男票、女票

3. 成长、理想

- 闯出天地
- 改变世界





GOPS2018
Shenzhen

我们如何工作？

1. 想老板所想，急老板所急

- 业务老板
 - 业务安全
- 技术老板
 - DevSecOps





GOPS2018
Shenzhen

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。





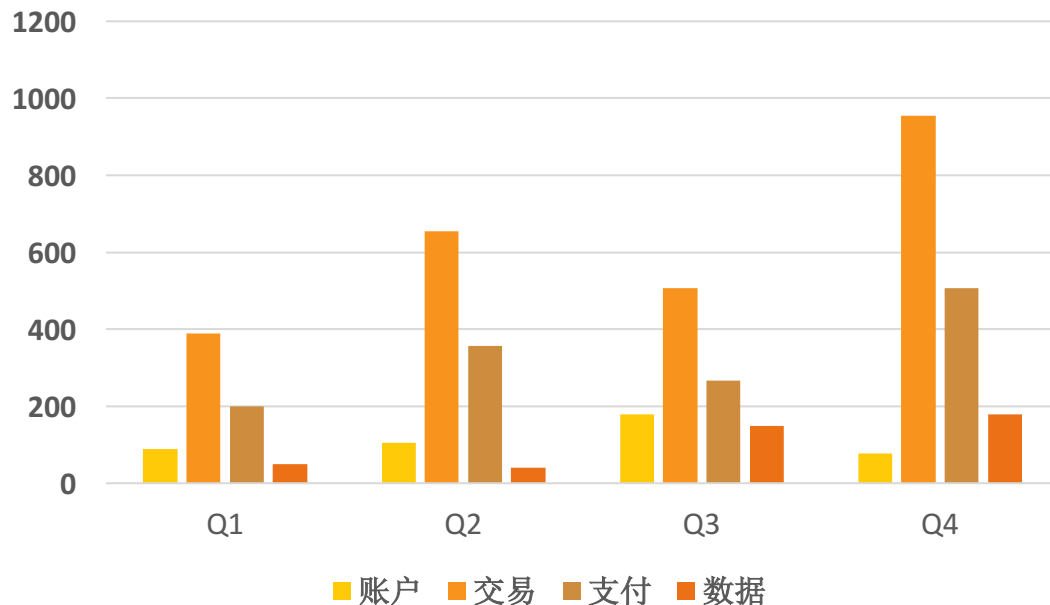
GOPS2018
Shenzhen

通过业务安全充分体现工作-降风险、减损失

1. 转换成具体的金额

- 账户安全
- 交易安全
- 支付安全
- 数据安全

减少的损失金额（千元）



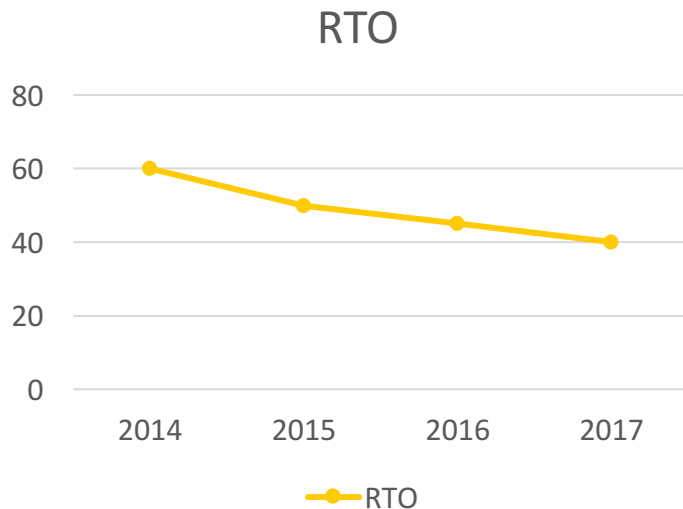


GOPS2018
Shenzhen

通过业务安全充分体现工作-省成本、增效益

1. 转换成时间和金额

- RTO、RPO
- DevSecOps
- 效率、速度





GOPS2018
Shenzhen

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。

RSA® Conference 2017

Moscone Center | San Francisco

February 13 - 17, 2017

来源：gartner.com,
rsaconference.com



GOPS2018
Shenzhen

如何做好DevSecOps

- Making security a part of everyone's job
- 使安全成为每个人工作的一部分
- Integrating preventative controls into our shared source code repository
- 将预防性控制集成到我们的共享源代码库中
- Integrating security with our deployment pipeline
- 将安全与部署管道集成

来源：DevOps HandBook



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

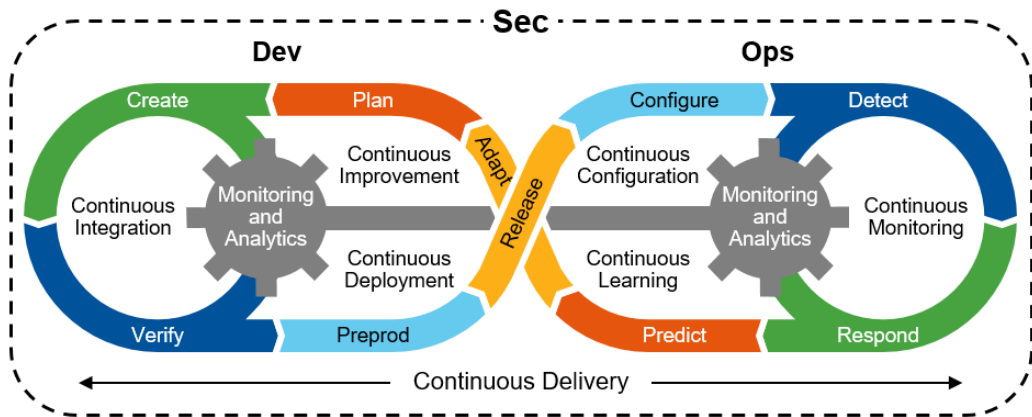
- 交付：综合评估后的结论与建议



GOPS2018
Shenzhen

如何做好DevSecOps

- Protecting our deployment pipeline
- 保护我们的部署管道
- Integrating our deployment activities with our change approval processes
- 将我们的部署活动与我们的变更审批流程相集成
- Reducing reliance on separation of duty
- 减少对分离职责的依赖



© 2017 Gartner, Inc.

来源：DevOps HandBook



GOPS2018
Shenzhen

目录

1 困境

2 业务安全与DevSecOps

➔ **3** 最佳实践的要素

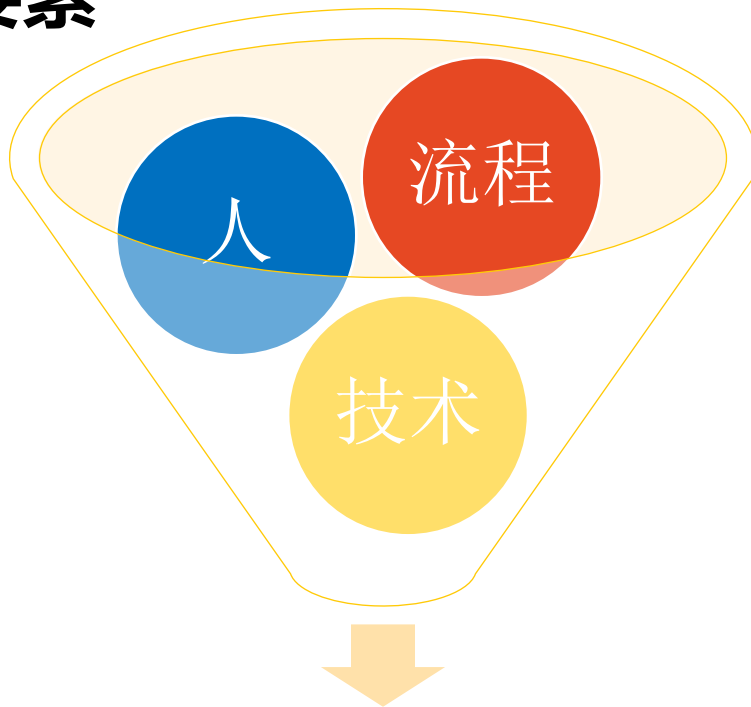
4 实施最佳实践项目



GOPS2018
Shenzhen

成功的三个要素

1. 人
2. 流程
3. 技术



成功的DevSecOps



GOPS2018
Shenzhen

1. 人是一切的基础

2. 打破孤岛

3. 培训

+ **Ensure that security is not a blocker** on active development or reviews

+ **Be empowered** to make decisions

+ **Work with AppSec team** on mitigations strategies

+ **Help with QA and Testing**

+ **Write Tests** (from Unit Tests to Integration tests)

+ **Help with development of CI** (Continuous Integration) environments

+ **Keep track of and stay up to date** on modern security attacks and defences

+ **Introduce body of knowledge** from organisations such as OWASP (Top 10, Application Security Verification Standard, Testing Guide etc.)

流程



GOPS2018
Shenzhen

版本控制，元数据和编码

整合流程

CI / CD中的安全工具

合规

安全架构

事件管理

红蓝对抗和SRC

威胁情报

技术



GOPS2018
Shenzhen

自动化和配置管理

安全编码

基线加固

持续集成连续交付的修补

应用程序的审核和扫描

自动漏洞管理扫描

自动合规性扫描

敏感信息管理



GOPS2018
Shenzhen

目录

1 困境

2 业务安全与DevSecOps

3 最佳实践的要素

➔ 4 实施最佳实践项目



GOPS2018
Shenzhen

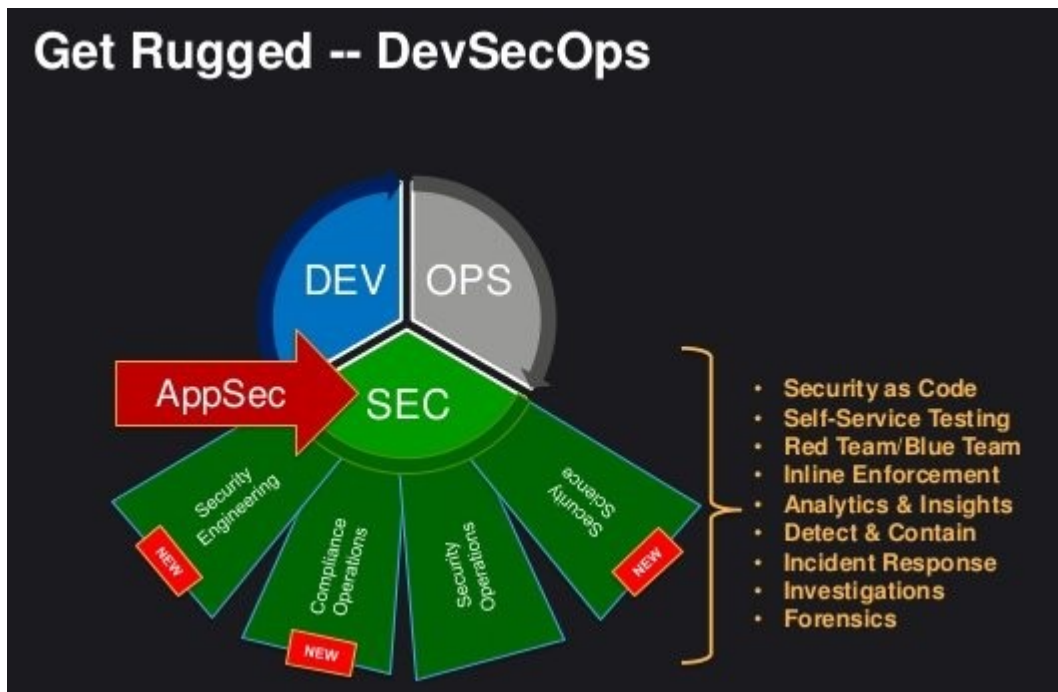
选择适合DevSecOps的项目

1. 自动化

- 工具
- API

2. 非强制监管

- 金融
- 等保三级或以上





GOPS2018
Shenzhen

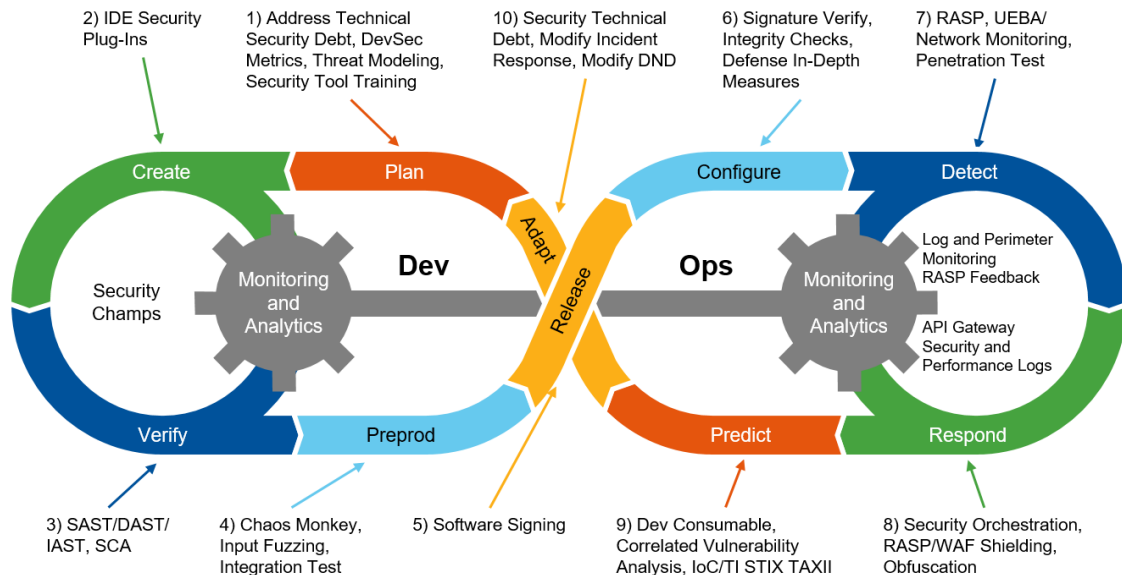
选择适合DevSecOps的项目

1. 快速迭代

- APP
- WEB Site

2. 可接受业务风险

- 利益相关方
- 安全风险
- 开发



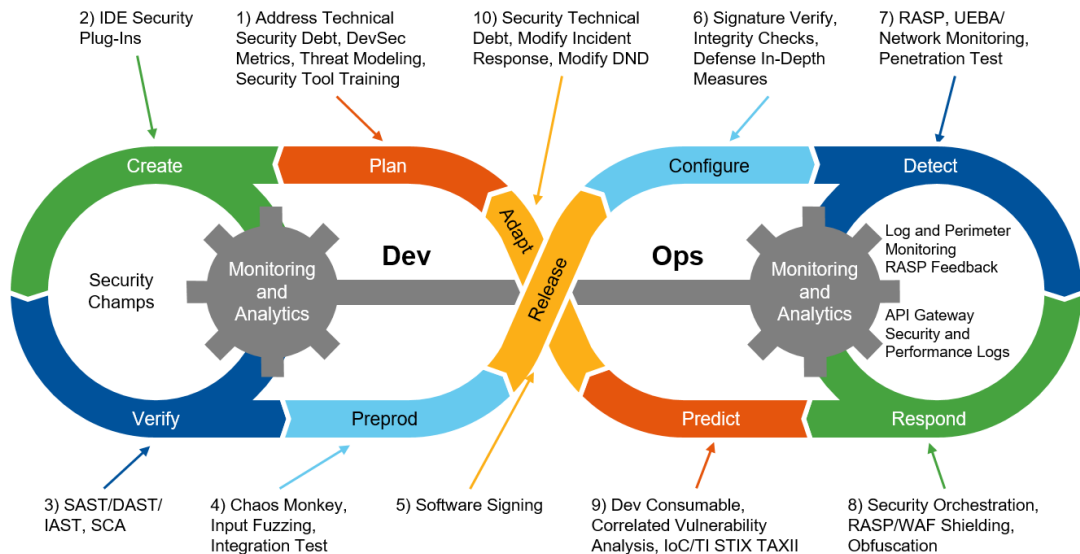
© 2017 Gartner, Inc.

选择适合DevSecOps的项目



GOPS2018
Shenzhen

1. DevSecOps适用性
2. 开发方法项目约束
3. 合适的项目



© 2017 Gartner, Inc.

实施DevSecOps项目



GOPS2018
Shenzhen

1. 使用原有的Secure SDLC工具
2. 左移



实施DevSecOps项目



GOPS2018
Shenzhen

1、计划

- Scrum安全问题
- 基线
- 代码规范
- 安全培训
- 威胁建模
- 收集安全需求



实施DevSecOps项目



GOPS2018
Shenzhen

2、创建

- 安全IDE插件
- 安全拼写检查器
- 威胁建模
- 安全架构评估
- 开源产品评估



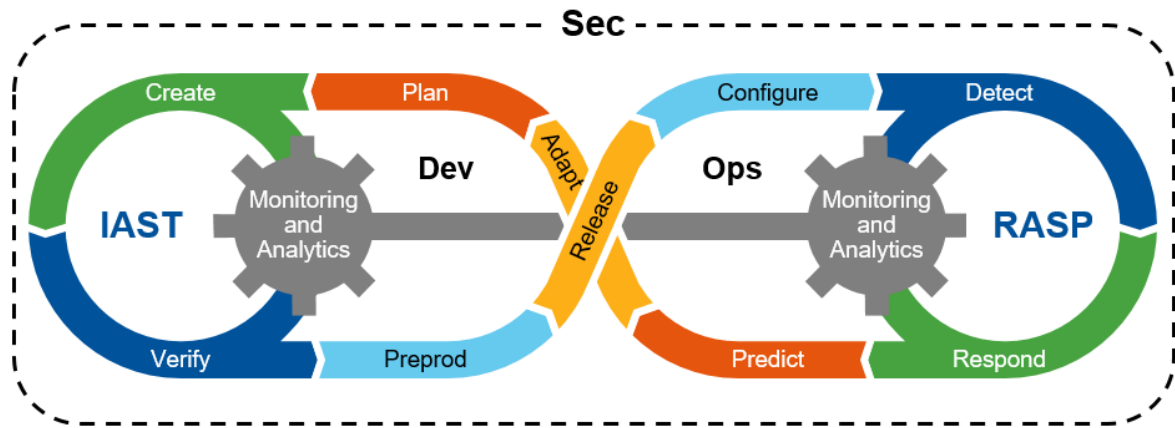
实施DevSecOps项目



GOPS2018
Shenzhen

3、验证

- 扫描已知漏洞
- 扫描基线、配置
- 扫描未知漏洞
- SCA执行OSS策略
- SAST、DAST
- IAST、RASP



© 2017 Gartner, Inc.

实施DevSecOps项目



GOPS2018
Shenzhen

4、安全测试

- 已知攻击测试
- Fuzz测试
- Chaos Monkey
- 代码签名

```
C:\WINDOWS\system32\cmd.exe

Syntax:

peach -a channel
peach -c peach_xml_file [test_name]
peach -g
peach [--skipto #] peach_xml_file [test_name]
peach -p 10,2 [--skipto #] peach_xml_file [test_name]
peach --range 100,200 peach_xml_file [test_name]
peach -t peach_xml_file

-1                Perform a single iteration
-a,--agent        Launch Peach Agent
-c,--count        Count test cases
-t,--test_xml_file Test parse a Peach XML file
-p,--parallel M,N Parallel fuzzing. Total of M machines, this
                  is machine N.
--debug           Enable debug messages. Usefull when debugging
                  your Peach XML file. Warning: Messages are very
                  cryptic sometimes.
--skipto N        Skip to a specific test #. This replaced -r
                  for restarting a Peach run.
--range N,M       Provide a range of test #'s to be run.
```

实施DevSecOps项目

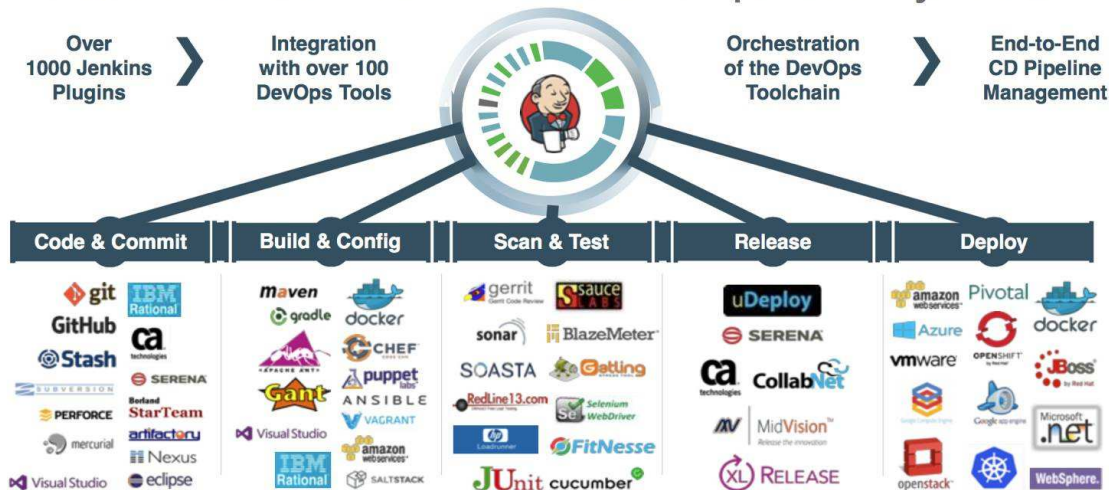


GOPS2018
Shenzhen

5、安全发布

- 正确部署
- 一致性：签名验证、完整性检查
- 右移

Jenkins is the Hub of CD/DevOps Ecosystem



cloudbees

© 2016 CloudBees, Inc. All Rights Reserved.

57

实施DevSecOps项目

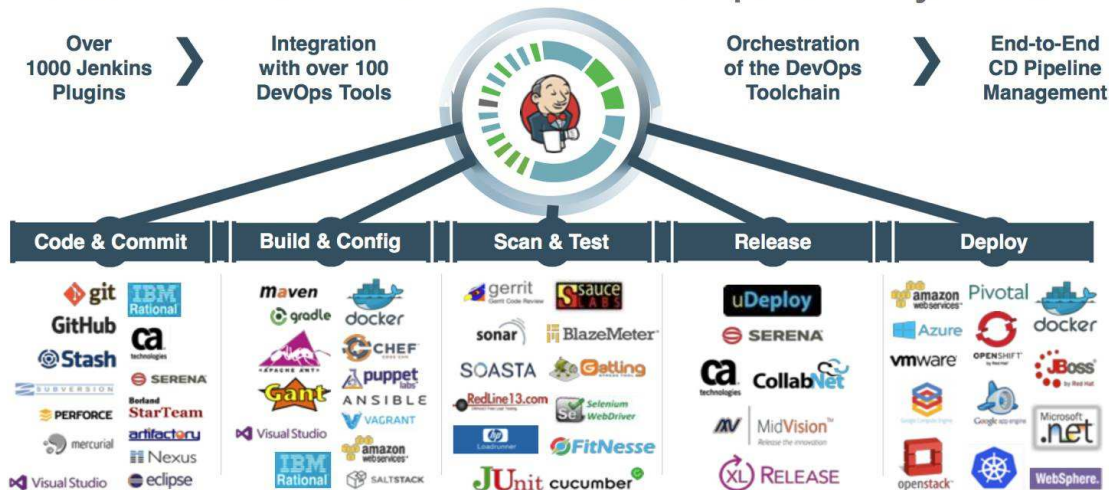


GOPS2018
Shenzhen

6、防止

- 深度防御措施
- 应用安全控制
- 网络防护

Jenkins is the Hub of CD/DevOps Ecosystem



cloudbees

© 2016 CloudBees, Inc. All Rights Reserved.

57

实施DevSecOps项目



GOPS2018
Shenzhen

7、检测

- 渗透测试
- RASP (Runtime application self-protection运行时应用自我保护)
- UEBA (User and Entity Behavior Analytics用户行为风险分析)



实施DevSecOps项目



GOPS2018
Shenzhen

8、响应

- RASP/WAF
- 屏蔽和混淆



快速响应

A quick response

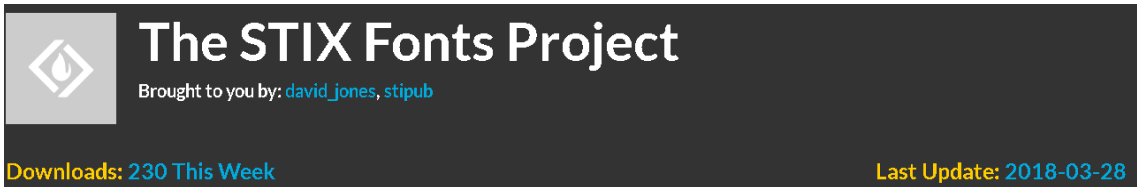
实施DevSecOps项目



GOPS2018
Shenzhen

9、预测

- CVA (Correlated Vulnerability Analysis相关漏洞分析)
- IoC (Indicators of Compromise)
- STIX
(StructuredThreatInformation eXpression结构化威胁信息表达式)
- TAXII
(TrustedAutomatedeXchange ofIndicatorInformation , 指标信息的可信自动化交换)



Solutions

Services

Partners

Support

IOC tools (Indicator of Compromise)



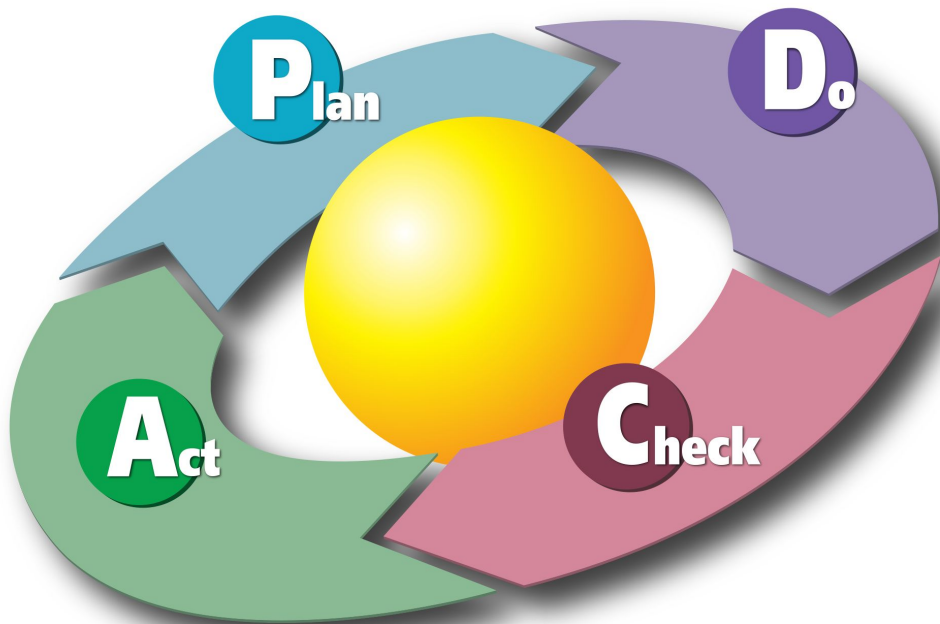
实施DevSecOps项目



GOPS2018
Shenzhen

9、适应性

- 持续改进
- 项目优化



帮助大家实施DevSecOps

YDB

中国通信标准化协会标准

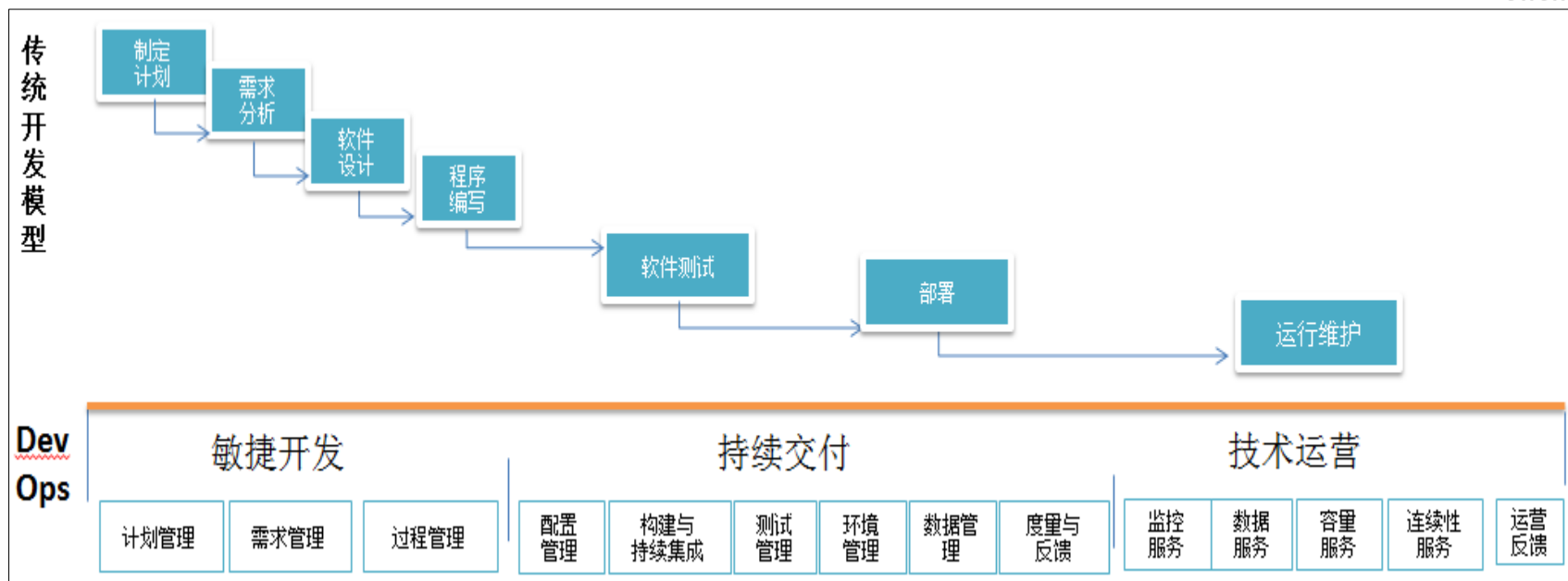
YDB XXX -XXX

研发运营一体化能力成熟度模型
第6部分：风险管理

制定DevSecOps标准



GOPS2018
Shenzhen



制定DevSecOps标准

研发运营一体化的风险

- 人员
- 工具
- 过程

系统风险

- 流程
- 技术

风险管理

- 分类
- 分级



GOPS2018
Shenzhen



Thanks

高效运维社区
开放运维联盟

荣誉出品



GOPS2018
Shenzhen

想第一时间看到高效运维社区
的新动态吗？

