GOPS 2020
Shanghai

GOPS 全球运维大会 2020

-AIOps 风向标

上海站

指导单位：

主办单位：

大会时间：2020年11月27日-28日

大会地点：上海中庚聚龙酒店

GOPS 2020
Shanghai

如何避免DevSecOps失败

锐少　某跨国企业安全和合规负责人

锐少-赵锐

某跨国企业安全和合规负责人

超过15年的资深科技风险、信息安全、业务安全经验。

DevOps国际标准核心编写专家、国家网络安全周网络安全金牌讲师、CSA云安全联盟专家、诸子云上海会长，出版有《DevOps三十六计》、《反黑客的艺术》等多部书籍

锐少

- 民革党员，超15年的资深科技风险、信息安全、业务安全经验，多家金融机构、世界500强安全负责人
- 国家网络安全周网络安全金牌讲师、网络安全专家志愿者
- DevOps国际标准核心编写专家
- CSA云安全联盟专家
- ISG网络安全技能竞赛专家
- 网络安全进校园活动特约讲师
- 金融网络安全优秀解决方案评委
- GOPS金牌讲师
- 上海新金融风险实验室安全专家
- CCSF优秀首席信息安全官
- 网络安全公益大使

拥有CDPSE、CISM、CEH、PMP、CISP、CCSK、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》，参与多部信息安全专业书籍、报告的编写、翻译、校对工作，已出版有《DevOps三十六计》、《反黑客的艺术》、《2018上海金融信息行业发展报告》、《云安全现状年度报告2018》、《CSA GDPR合规行为准则》、《从网络安全转向业务安全的价值实现》、《信息安全人员如何与业务人员沟通》、《云端数据安全浅谈》，即将出版《CISSP认证考试指南（第8版）》和《ISO27001撬动安全管理》。

GOPS 2020
Shanghai

CONTENTS

目录

目前的DevSecOps

目前的DevSecOps

Tweet Share

DevOps Needs to Become DevOpsSec

by **Neil MacDonald** | January 17, 2012 | Comments Off on DevOps Needs to Be

RSAConference2017
Moscone Center | San Francisco
February 13 – 17, 2017

DEV SEC OPS DAYS
San Francisco
March 4, 2019

DevOps Conf AC

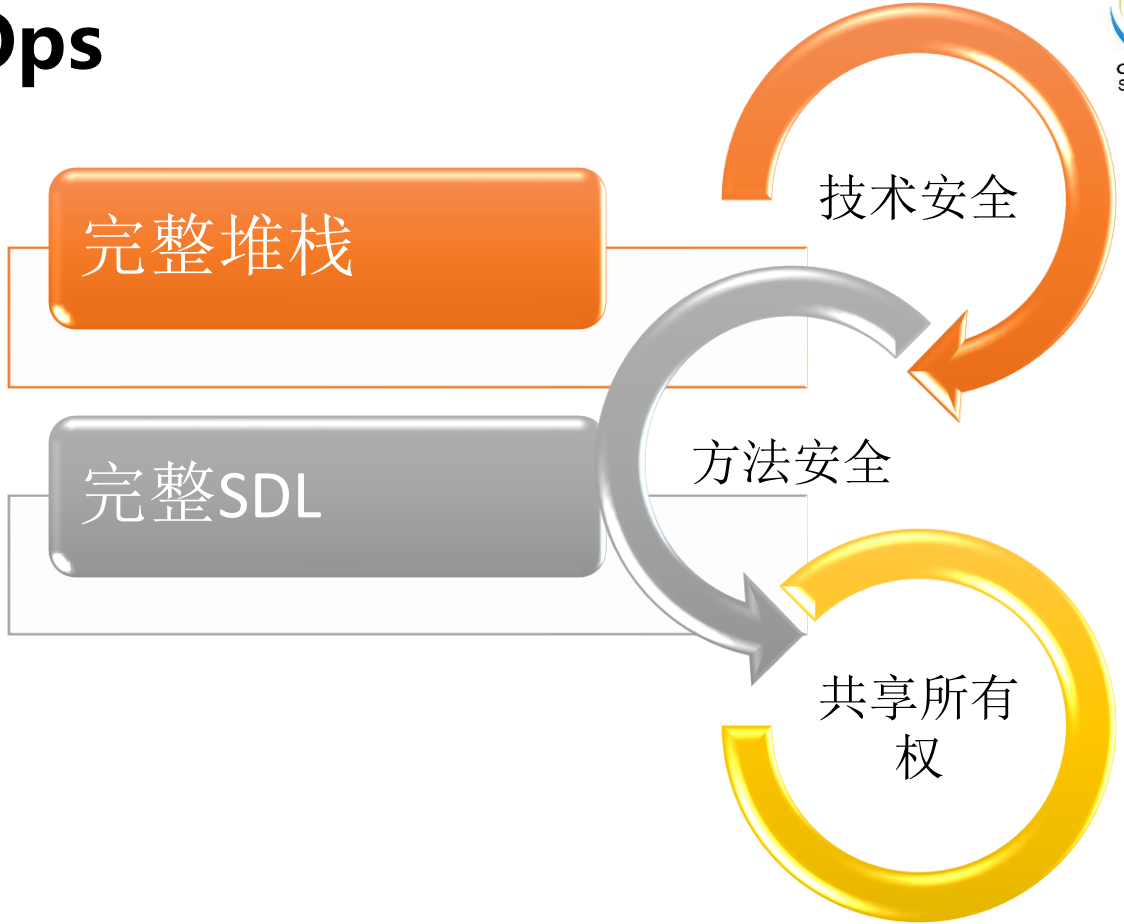
Monday, Mar 04 | 09:00 A.M. -

← View all Sessions

DEV SEC OPS DAYS
SAN FRANCISCO
24 February 2020

目前的DevSecOps

- Dev
- Sec
- Ops

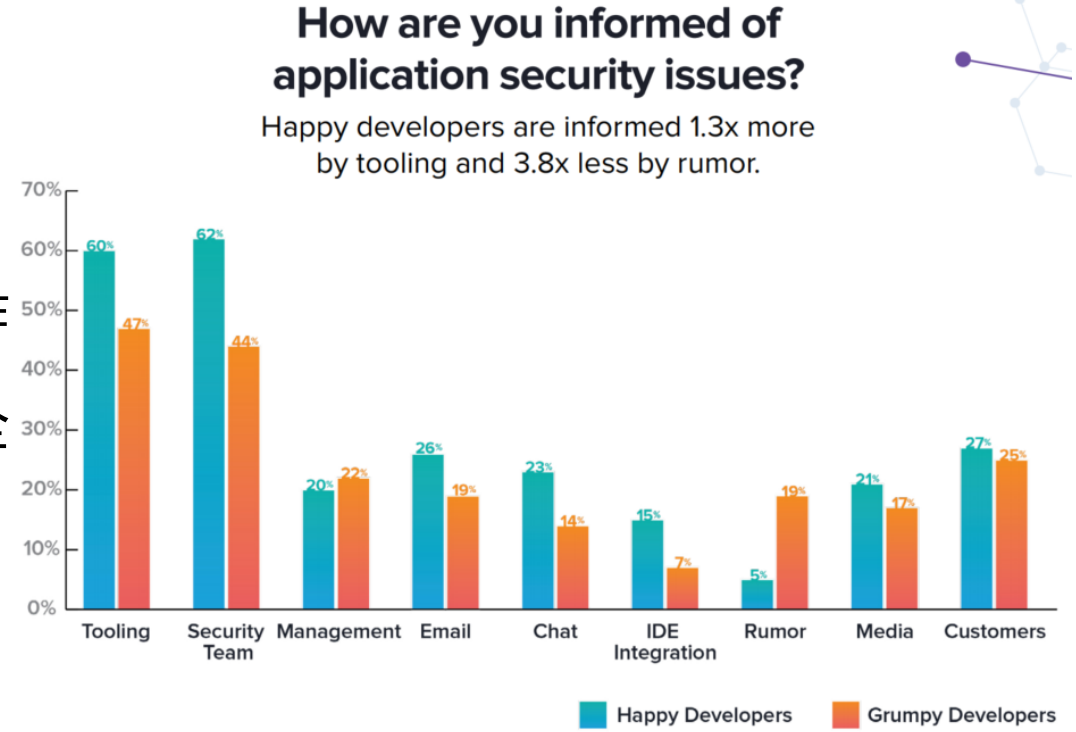


目前的DevSecOps

- 2020年，Sonatype进行了DevSecOps调查，有5045名IT专业人员参与。 调查显示，实施DevSecOps实践的组织，大家有更高的工作满意度，IT人员受益最大。
- 来源：sonatype.com

目前的DevSecOps

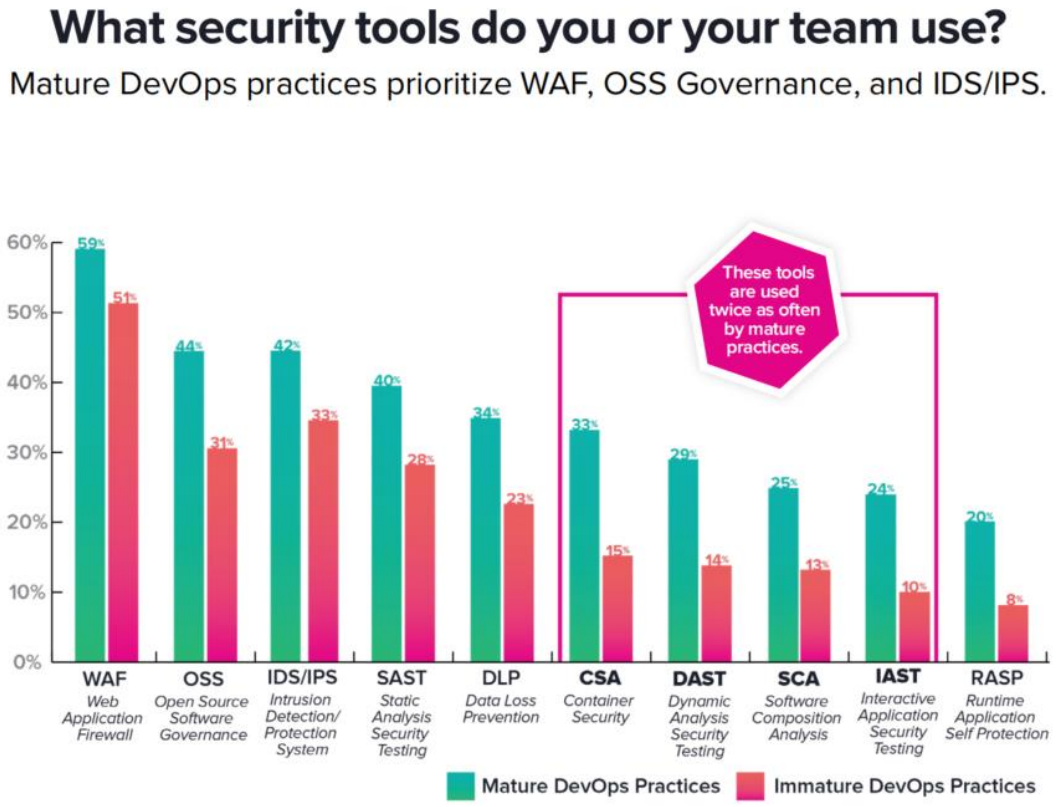
1. 每个人都对安全负责
2. 高层决策
3. 科技团队之间相互协作
4. 专注于风险，而非安全



- 来源：gartner.com,
- devsecops.com, sonatype.com

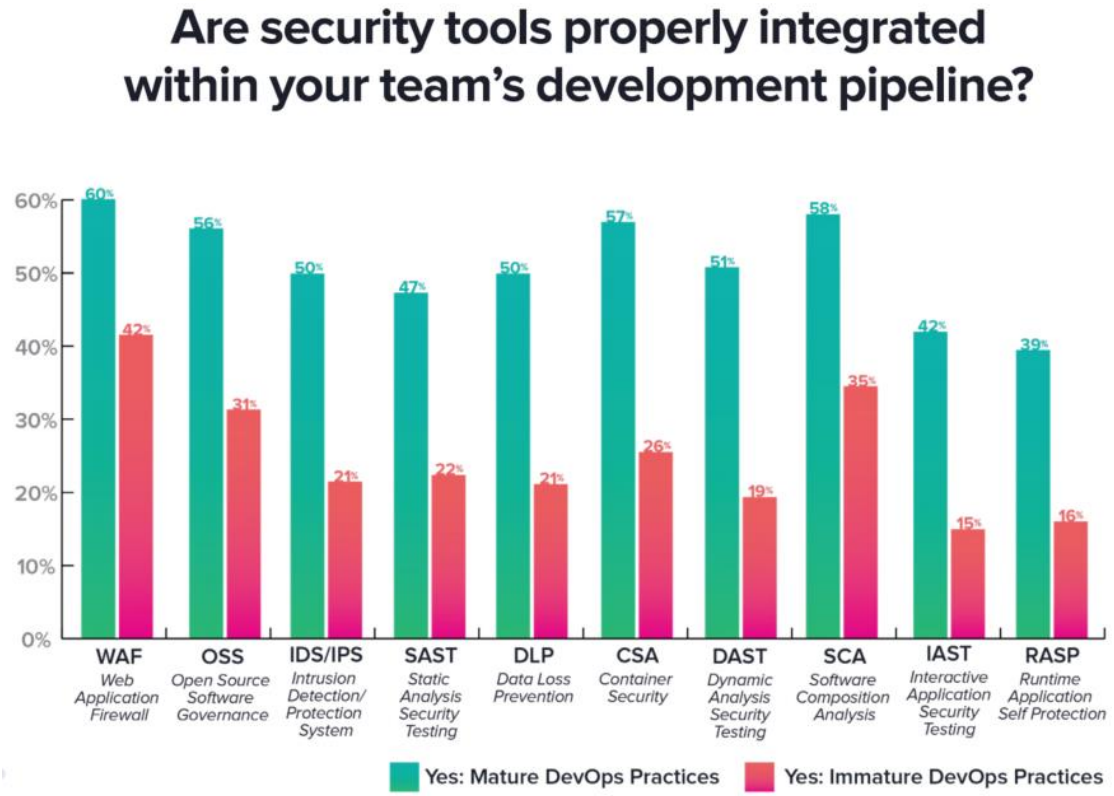
目前的DevSecOps

使用什么安全工具



目前的DevSecOps

在DevOps管道中集成了哪些安全工具?



目前的DevSecOps

关注：专题会议分享、媒体介绍越来越多

实践：态势感知和自动发布

标准：国内　　国际

目前的DevSecOps

制定标准ITU-T研发运营一体化能力成熟度模型

第1部分 总体架构

第2部分 敏捷发开管理

第3部分 持续交付

第4部分 技术运营

第5部分 应用设计

第6部分 安全与风险管理

第7部分 组织结构

级别	英文	中文	定义
1级	Initial Level	初始级	在组织局部范围内开始尝试DevOps活动并获得初期效果
2级	Fundamental Level	基础级	在组织较大范围内推行DevOps实践并获得局部效率提升
3级	Comprehensive Level	全面级	在组织内全面推行DevOps实践并贯穿软件全生命周期获得整体效率提升
4级	Excellent Level	优秀级	在组织内全面落地DevOps并可按需交付用户价值达到整体效率最优化
5级	Fabulous Level	卓越级	在组织内全面形成持续改进的文化并不断驱动DevOps在更大范围内取得成功

信通院 云计算开源产业推进联盟（OSCAR）DevOps标准工作组 & 高效运维社区

目前的DevSecOps

2020年安全和风险管理的关键规划注意事项

Major Changes in Compliance and Risk Impact Security Program and Roadmap

- Evangelize pragmatic approaches to risk
- Triage high-exposure risk areas
- Improve third-party assessment and control

Security Solution Architecture Is Increasingly Driven by Integrated Platform Approaches

- Create a security capability model
- Use threat and attack models
- Evaluate integrated cybersecurity platforms

Ecosystems Cement the Need for Data-Centric Security Architecture and Application Security

- Create discovery, visibility and control
- Design flexible security for data and analytics
- Enhance application and API security practices

Effective Security Monitoring and Response Depend on Automation and Analytics

- Develop and enhance incident response
- Focus on activity and access monitoring
- Assess machine learning and deception

Containers, DevSecOps, Hybrid Cloud and Multicloud Transform Infrastructure Security

- Embrace DevSecOps for automation
- Modernize network, workload, data security
- Emphasize visibility, monitoring, management

Mobile Devices, Things, Agents & SaaS Drive Need for Native Security & Security Add-Ons

- Implement endpoint threat and data protection
- Design mobile security with cloud AppSec
- Factor IoT devices, agents into security plans

Source: Gartner
ID: 407409

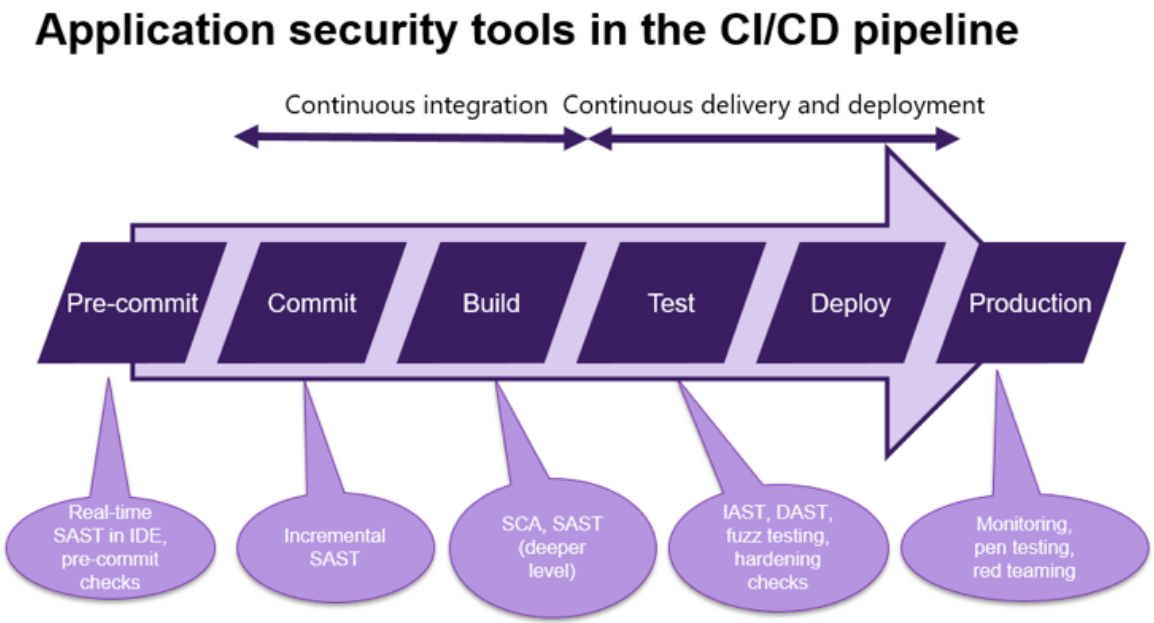
DevSecOps失败案例

失败案例-为了DevSecOps而DevSecOps

1. 面子工程
   - 别人有我们也要有
   - 用不用再说，先上线
2. 没有基础
   - 无实际运用场景
   - 未理清CI/CD流程

失败案例-工具

1. 缺少自动化安全工具
   - 命令行
   - 手工
2. 不合适的工具
   - 效率
   - 误报



失败案例-工具

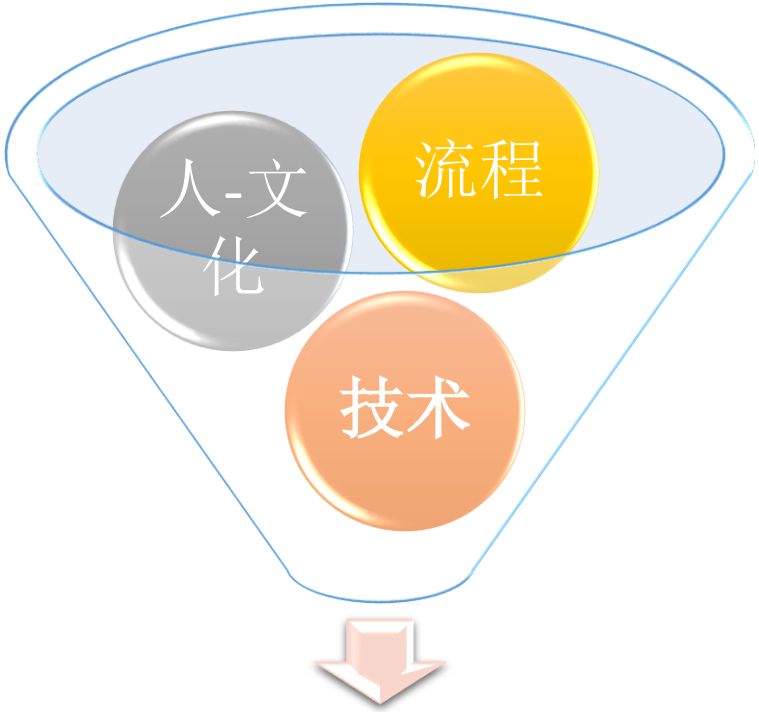
1. 不必要的扫描
   - 开源组件
   - 公共组件
2. 资源配置不合理
   - 性能弱
3. 工具解决所有问题
   - 全自动

3

经验总结

经验总结

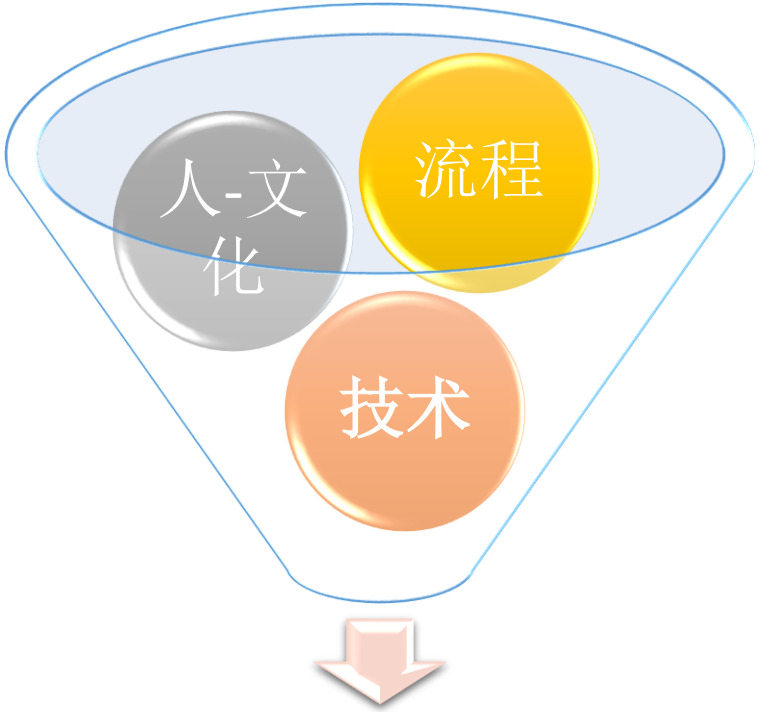
1. 合适的工具
2. 合适的位置
3. 自定义规则
4. 按项目优先级
5. 分析扫描结果减少误报
6. 治理和培训



成功的DevSecOps

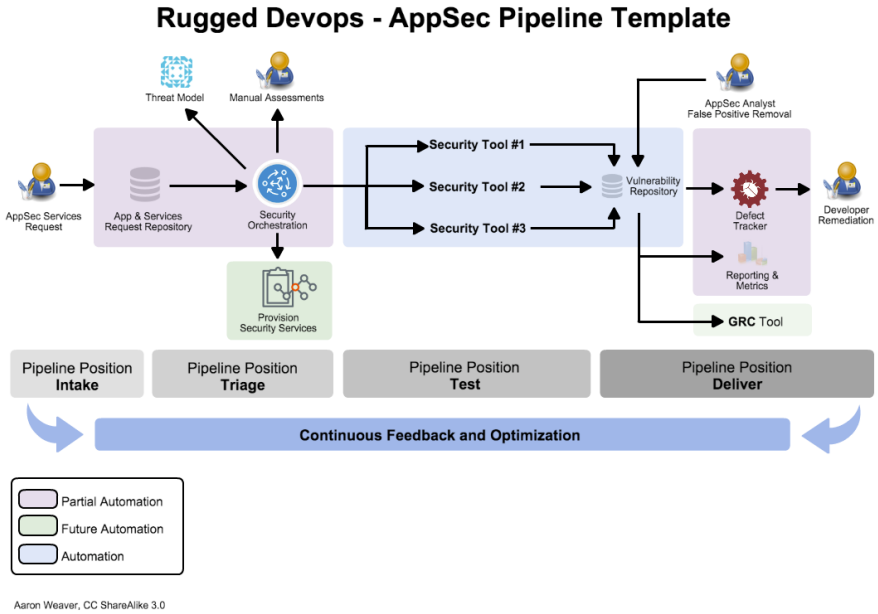
经验总结

1. 总结漏洞问题
2. 培训开发人员
3. 定义明确的流程
4. 帮助开发人员修复漏洞
5. 加强安全标准
6. 风险处理
7. 按业务级别定义问题级别



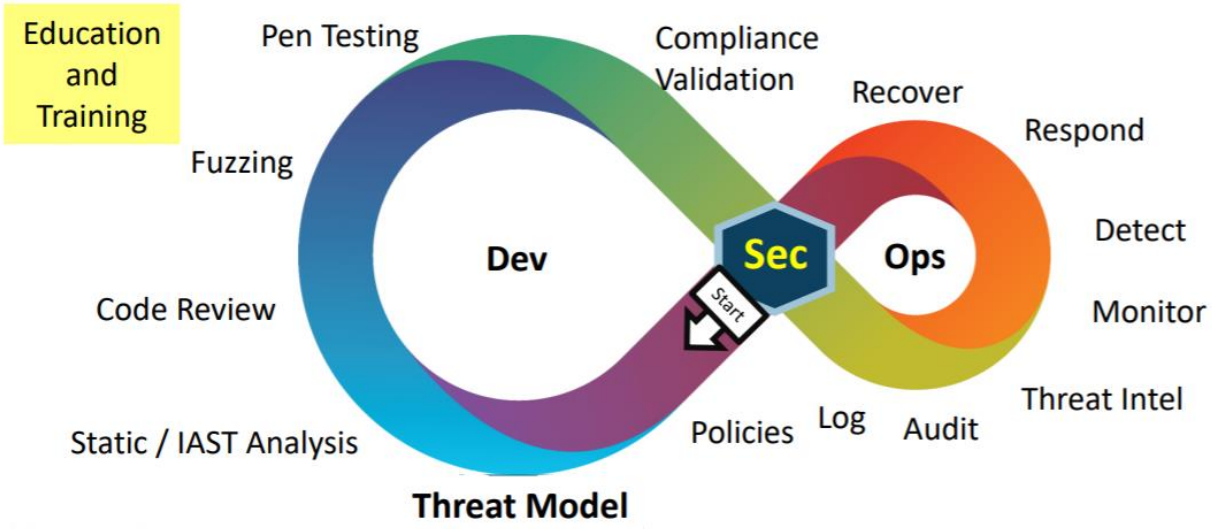
成功的DevSecOps

经验总结



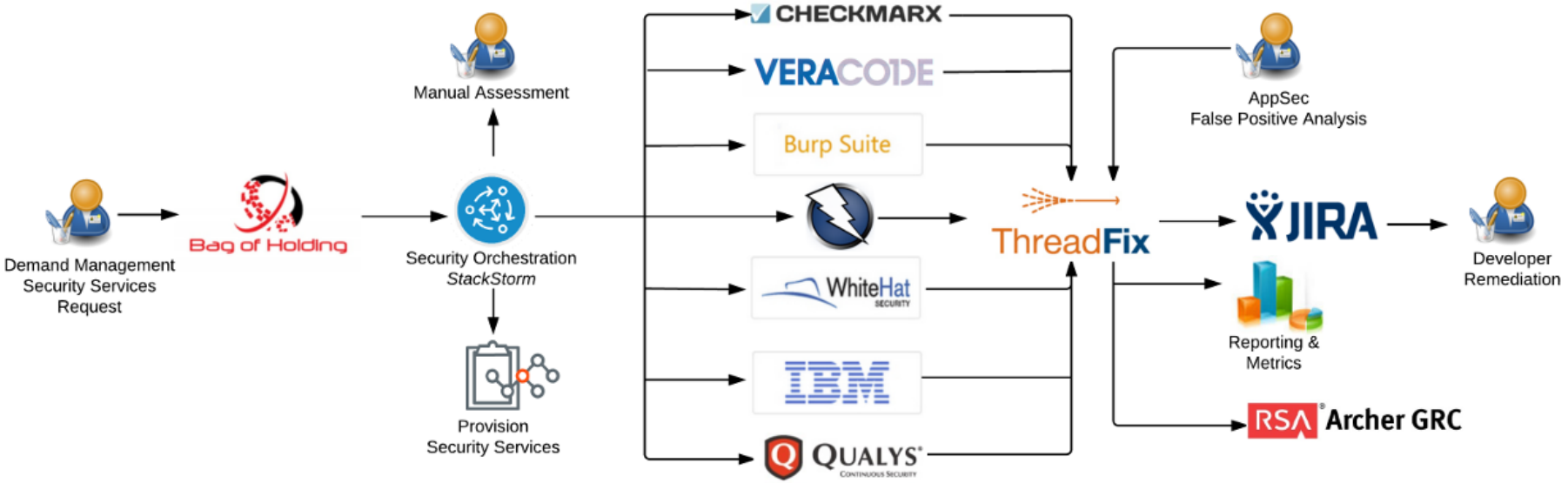
- 选择关键资源
- 减少冲突
- 提高可视化
- 每个步骤均可重复
- 提高一致性

经验总结



- 培训
- 需求
- 架构、设计
- 编码、开发
- 测试
- 发布
- 运维

经验总结


Demand Management
Security Services
Request
Bag of Holding
Manual Assessment
Security Orchestration
StackStorm
Provision
Security Services
CHECKMARX
VERACODE
Burp Suite
WhiteHat
SECURITY
IBM
QUALYS
CONTINUOUS SECURITY
ThreadFix
AppSec
False Positive Analysis
JIRA
Reporting &
Metrics
RSA Archer GRC
Developer
Remediation

经验总结

CIS Center for Internet Security®

tenable Nessus

开发标准、资源

环境

- 加固
- 安全配置
- 开源工具安全扫描
- 源代码、IDE扫描

开发工具

- 安全开发手册
- 编码规范
- 安全IDE检查工具

sonarlint

OWASP Open Web Application Security Project

CHECKMARX

FORTIFY

开发编码

- 代码混淆
- 构建开发
- 源代码SAST
- 打包

经验总结

AppScan
IBM Security

owtf.org

GOPS 2020 Shanghai

OWASP ZAP

CIS Center for Internet Security®

Unit Test

- 应用加固
- GUI API接口测试

SIT

- Docker安全扫描
- GUI API接口测试
- 黑盒DAST
- 内部PenTest

DOCKER CLOUD
Repositories / sanscontext /

UAT

- 性能测试
- 容量测试
- 外部PenTest

CHECKMARX
ca technologies
VERACODE
FORTIFY
GAUNTLT

经验总结

splunk>

OPEN Refine

上线发布

- 上线审批
- 残余安全风险确认

安全运营

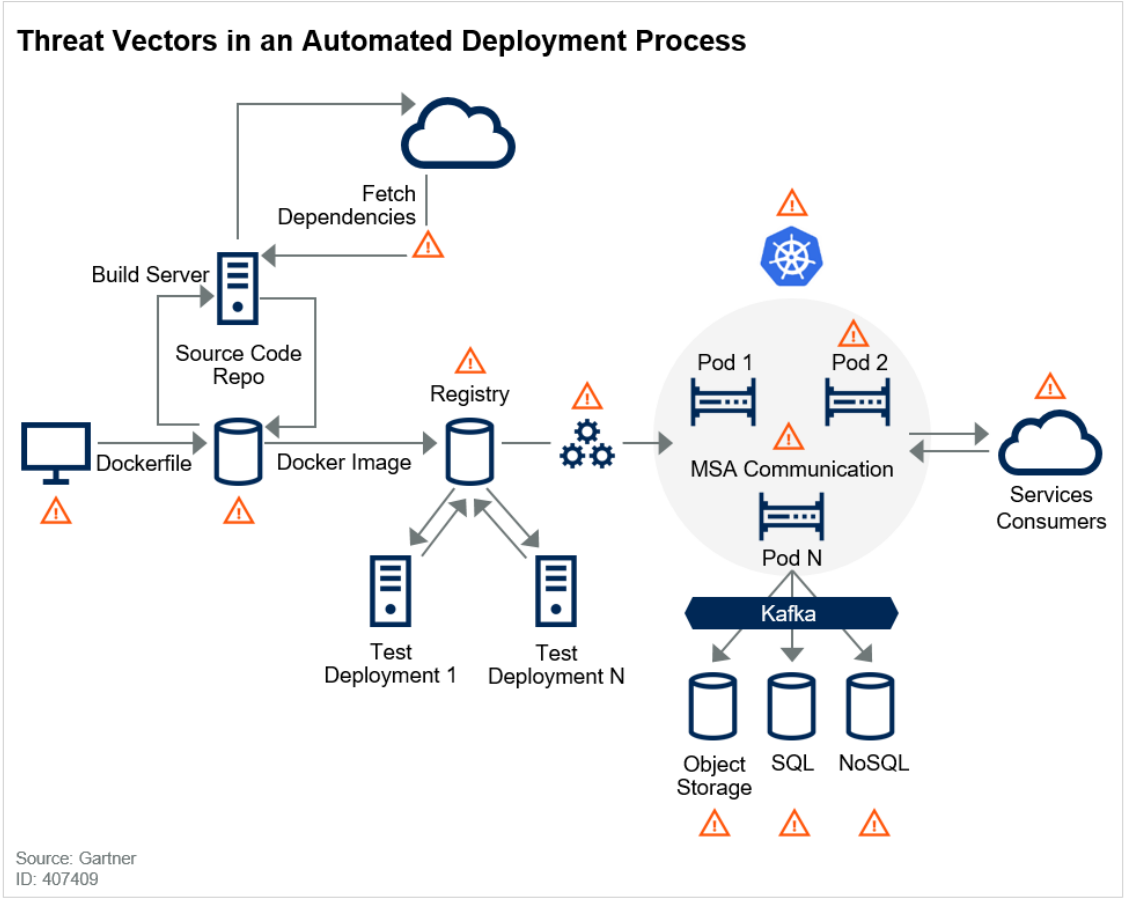
- 监控可视化仪表板
- 阻断工具
- SRC

废弃

- 系统下线
- 资源回收
- 数据清理或备份

经验总结

1. 不要忘记基础安全
2. 可重复的安全工作
3. 参考最佳实践构建



Thanks

高效运维社区

开放运维联盟

荣誉出品