

2018 | 中国·北京站  
DevOps 落地，从这里开始

# DevOps 国际峰会

暨 DevOps 金融峰会

指导单位： 云计算开源产业联盟  
Open Source Cloud Alliance for Industry (OSCAI)

主办单位： DevOps时代

 高效运维社区  
GreatOps Community

2018年6月29日-30日

地址：北京悠唐皇冠假日酒店

# DevSecOps的落地实施建议

赵锐（锐少）

# 目录

**1**

DevSecOps

**2**

实施前的准备工作

**3**

实施案例剖析及建议

# DevSecOps

DOIS

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

从2017年开始DevSecOps成为  
热门词汇。

来源：gartner.com,  
rsaconference.com



**RSA**Conference 2017  
Moscone Center | San Francisco  
**February 13 - 17, 2017**

# DevSecOps的实施调查

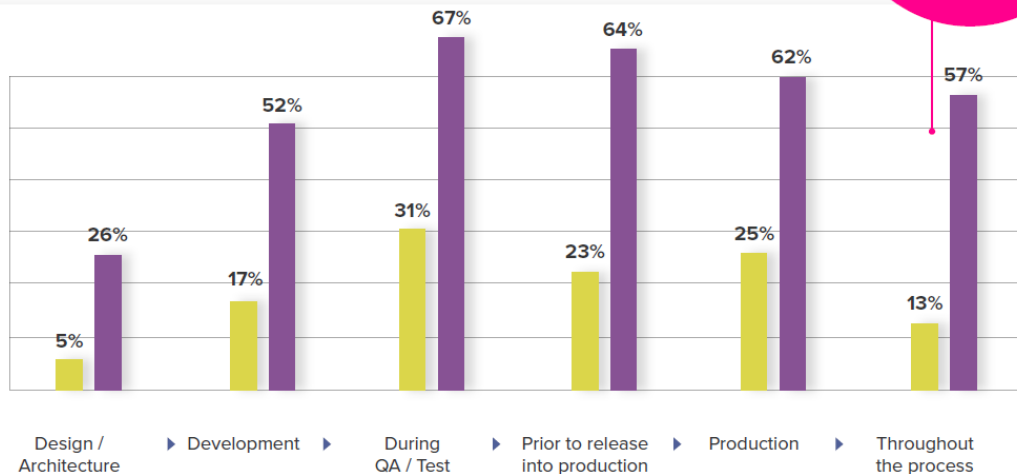
## Is the company ready for DevSecOps?



# DevSecOps的实施调查

At what point in the development process does your organization perform automated application security analysis?

Mature DevOps practices are 338% more likely to integrate automated security.



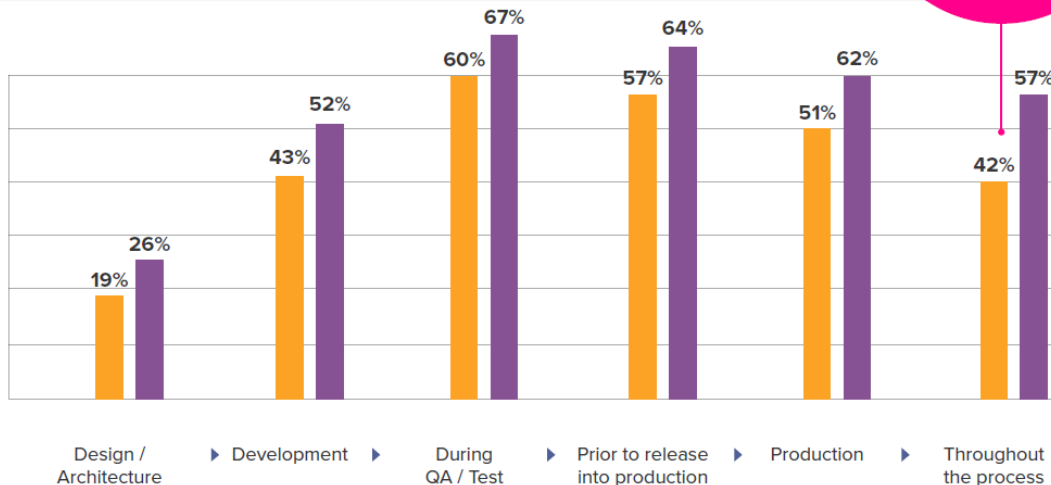
■ 2018 No DevOps Practice

■ 2018 Mature DevOps Practices

# DevSecOps的实施调查

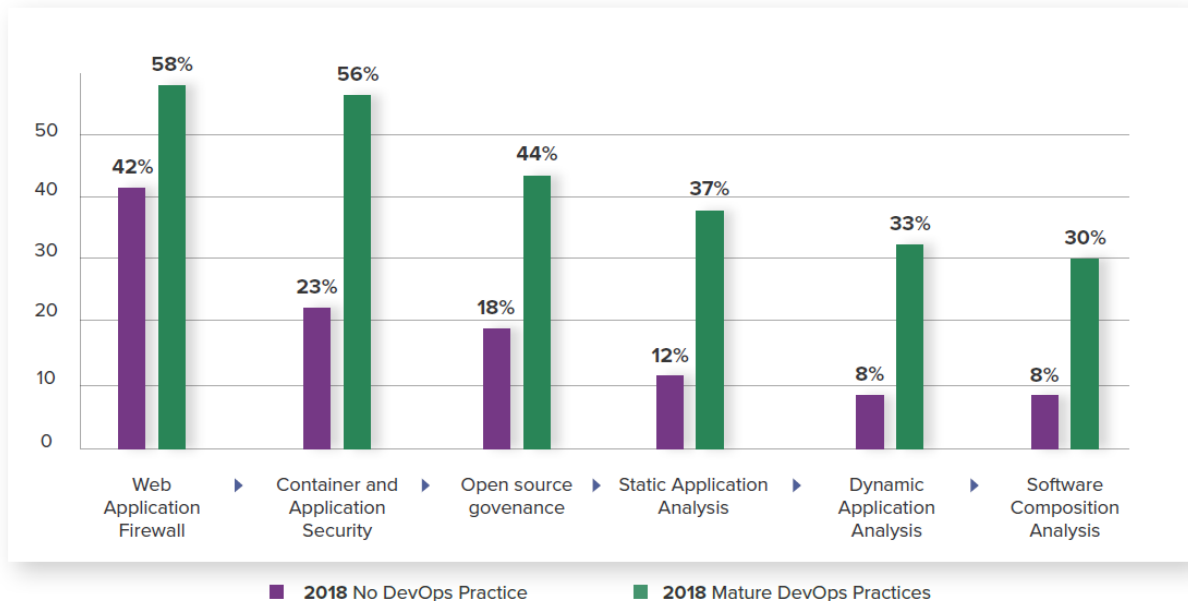
At what point in the development process does your organization perform automated application security analysis?

Mature DevOps practices ramped their investment in automated security by 15%.



# DevSecOps的实施调查

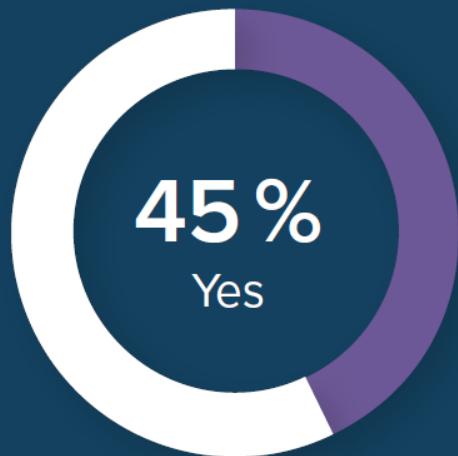
Which application security tools are critical to your organization?



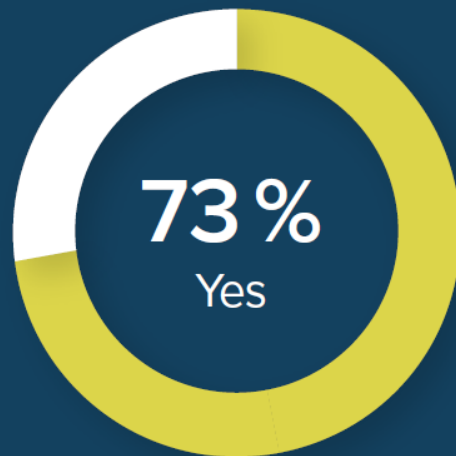


# DevSecOps的实施调查

Have recent high profile breaches heightened interest in DevSecOps practices for your organization?



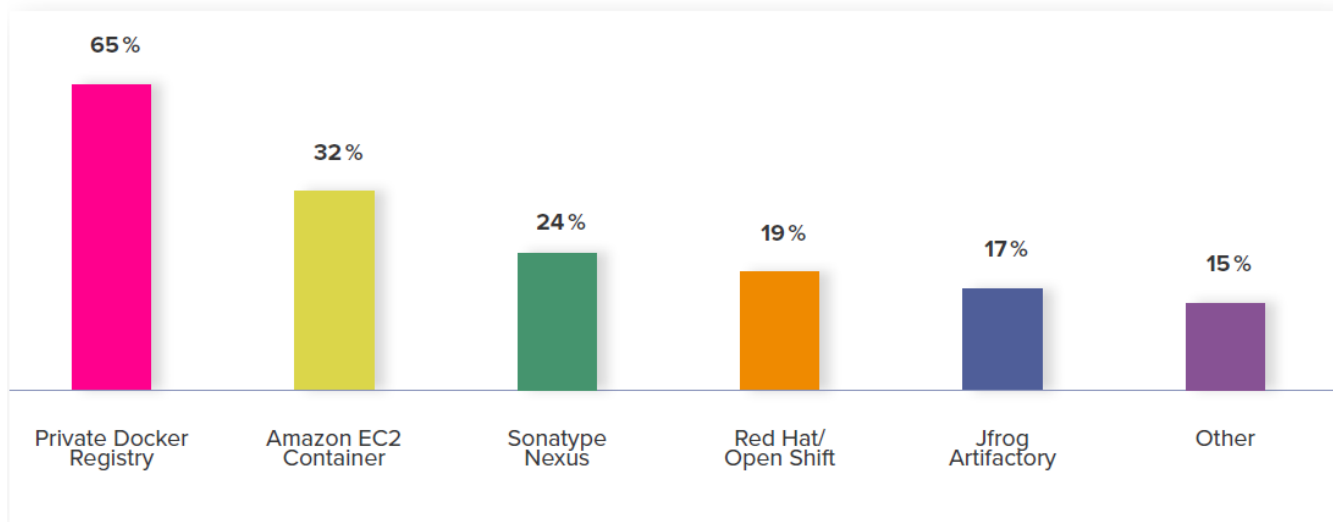
2018  
No DevOps Practice



2018  
Mature DevOps Practices

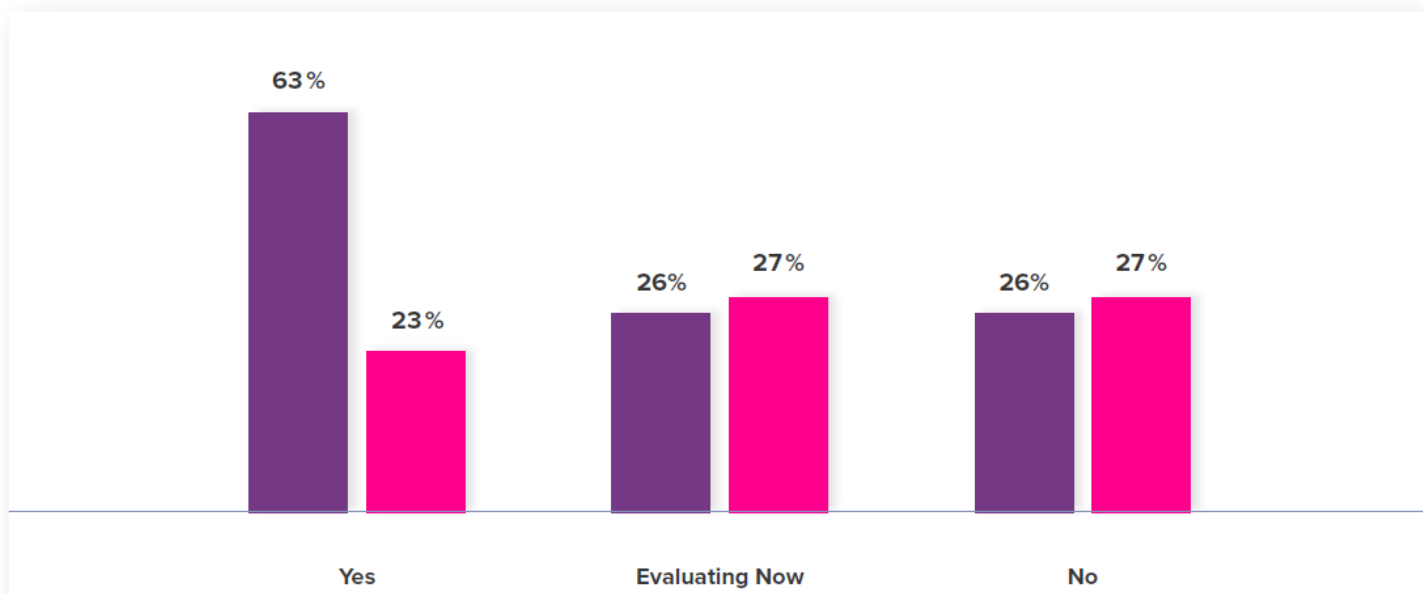
# DevSecOps的实施调查

Which private container registries  
does your organization use?



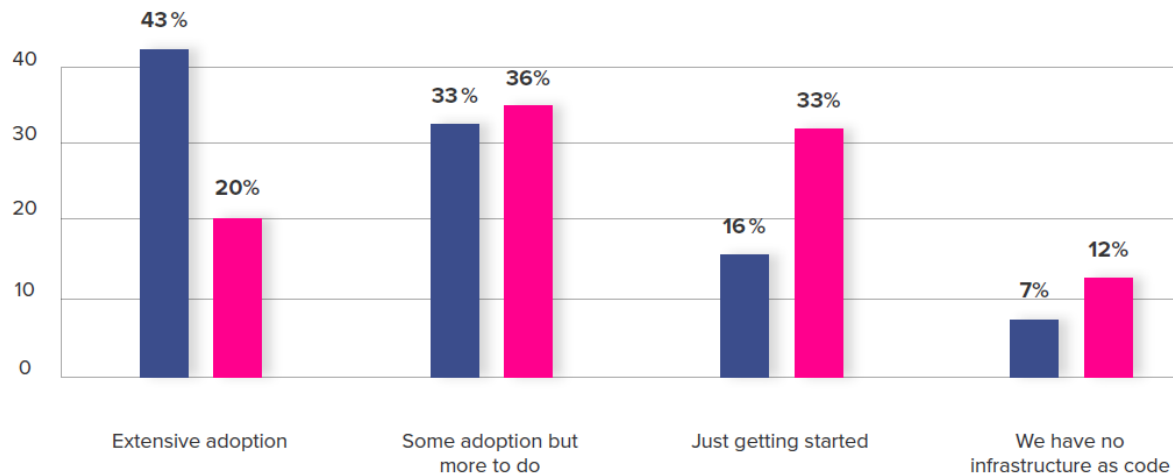
# DevSecOps的实施调查

Do you leverage security products to identify vulnerabilities in containers?



# DevSecOps的实施调查

Infrastructure as code adoption  
(e.g., Docker containers, Chef cookbooks, Vagrant boxes).



# 目录

1 DevSecOps

➔ 2 实施前的准备工作

3 实施案例剖析及建议

# 实施前的准备工作

## 1. 理解业务

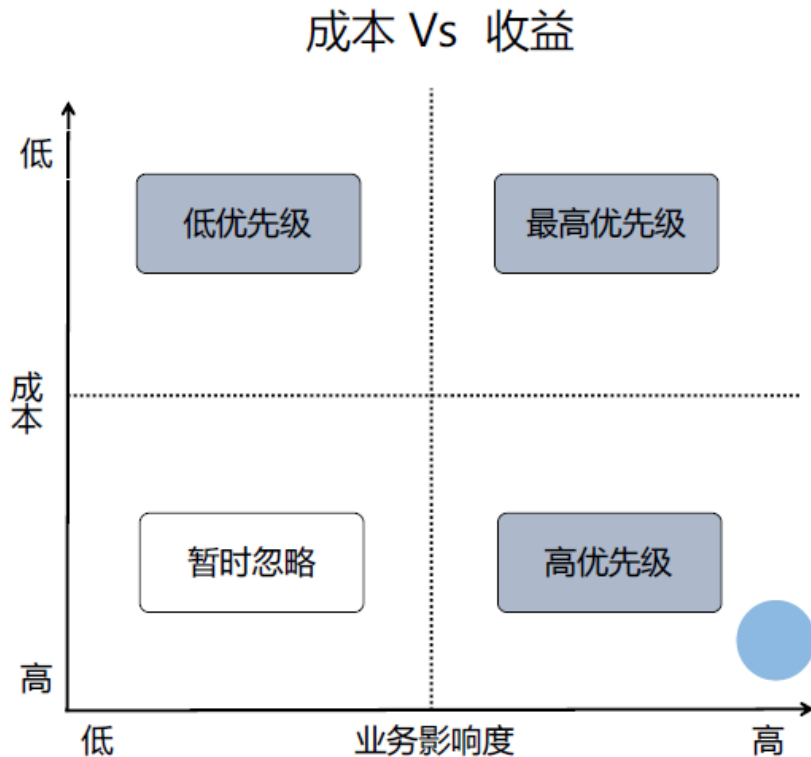
- 知道老板关心什么

## 2. 得到老板支持

- 在DevOps中增加Sec的好处

## 3. 得到相关同事的支持

- 提高质量、效率
- 职业发展



# 实施前的准备工作-人

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.)

# 实施前的准备工作-流程

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



# 实施前的准备工作-技术

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

# 实施前的准备工作



# 实施前的准备工作

1. 文化
2. 自动化
3. 精益
4. 度量
5. 分享

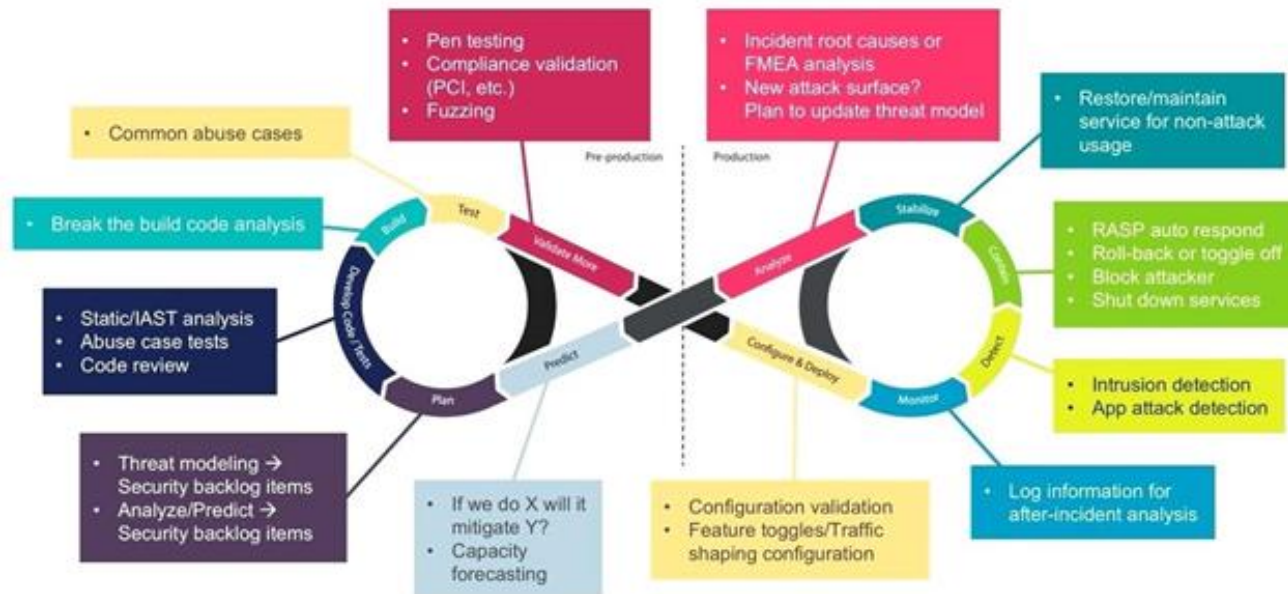


**C** – Culture  
**A** – Automation  
**L** – Lean  
**M** – Measurement  
**S** – Sharing

# 实施前的准备工作

## 确定目标计划 DevSecOps cycle

- 运营监控
- 响应
- 扫描
- 开发
- 设计
- 需求



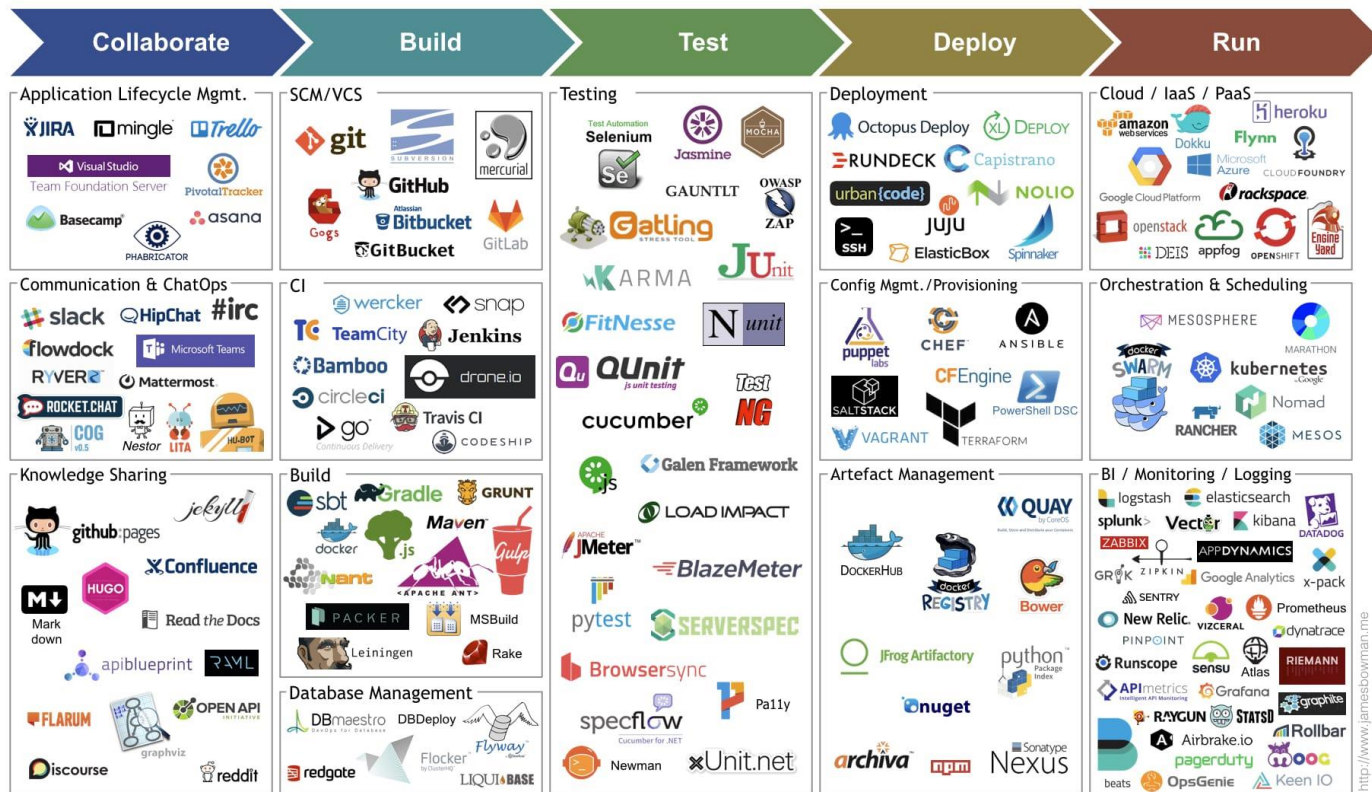
# 目录

1 DevSecOps

2 实施前的准备工作

➔ 3 实施案例剖析及建议

# 实施案例剖析及建议



<http://www.jamesbowman.me>

# 实施案例剖析及建议

## 选用合适的工具

- 告警
- 响应



The screenshot shows the Alerta web interface with a list of alerts. The interface includes a search bar, tabs for Recent, Top 10, and Watch, and a table of alerts.

Severity	Status	Time	Environment	Service	Resource	Event	Value	Text
Critical	Open	09:55	Development	Web	mysql	SlowResponse	3003ms	Service unavailable.
Major	Open	09:55	Development	Network	fw010	NodeDown	Down	Firewall is not responding to ping.
Major	Open	09:55	Production	Network	host678:eth0	HW-NIC:FAILED	error	Network interface eth0 is down.
Minor	Open	09:55	Production	Platform	host44	SwapUtil	94%	Swap utilisation is high.
Warning	Open	09:55	Development	Database	mysql	OracleError	ERROR 011	Oracle 011 error.

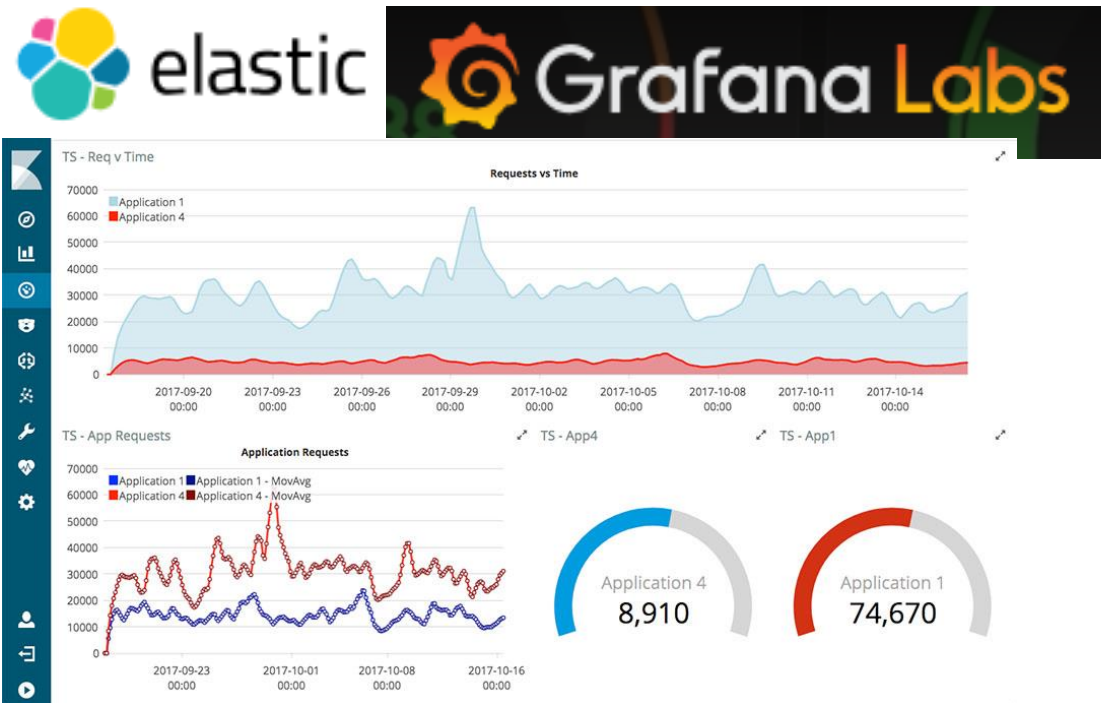
Showing 5 out of 5 alerts



# 实施案例剖析及建议

选用合适的工具

- 运营监控





# 实施案例剖析及建议

## 选用合适的工具

- 测试
- OWASP Zed Attack Proxy Project
- OWASP OWTF
- GAUNTLT

# OWASP



# ZAP

# GAUNTLT



# 实施案例剖析及建议

选用合适的工具

- 源代码扫描



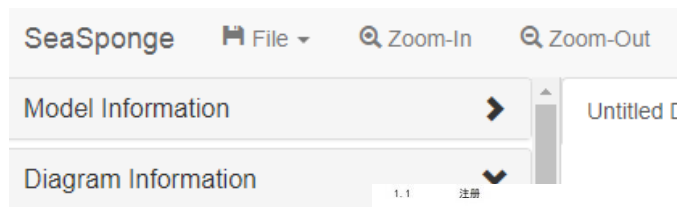
VERACODE



# 实施案例剖析及建议

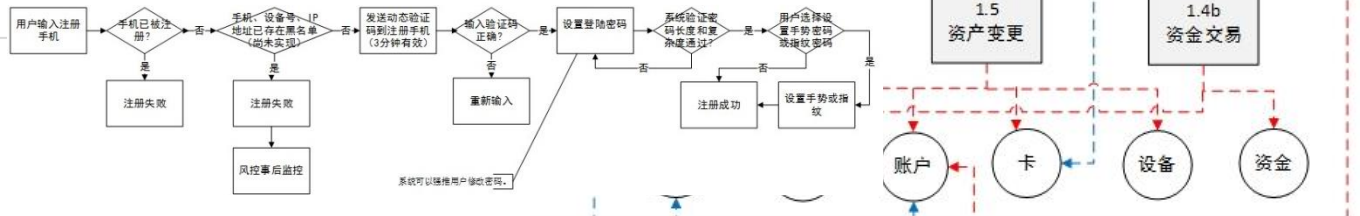
## 选用合适的工具

- 设计-威胁建模



### Diagram Title

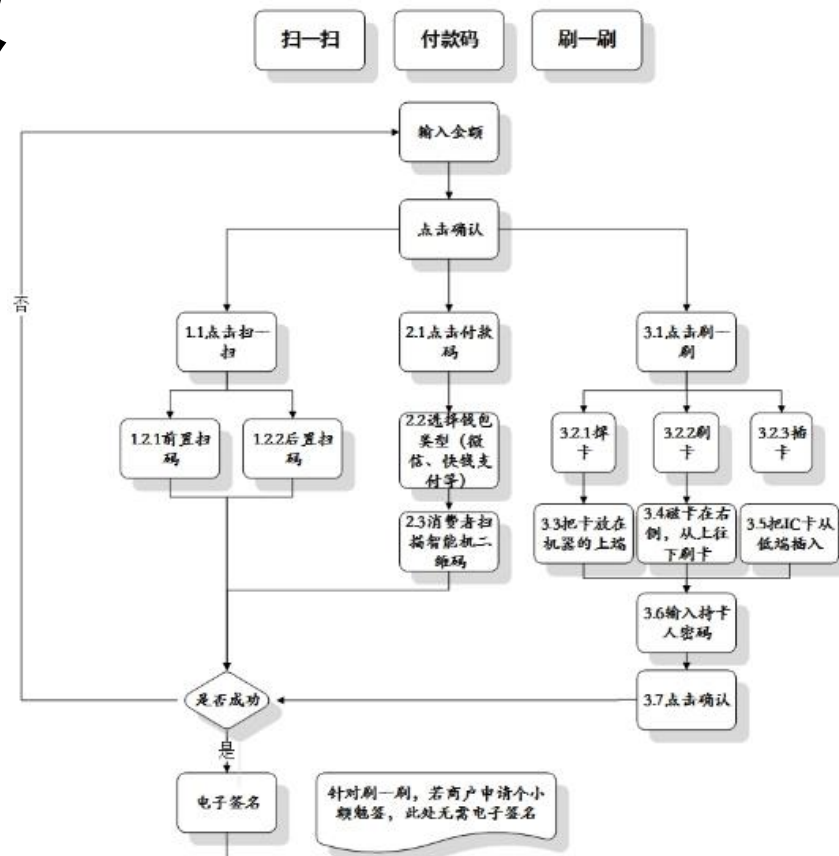
Untitled Diagram



# 实施案例剖析及建议

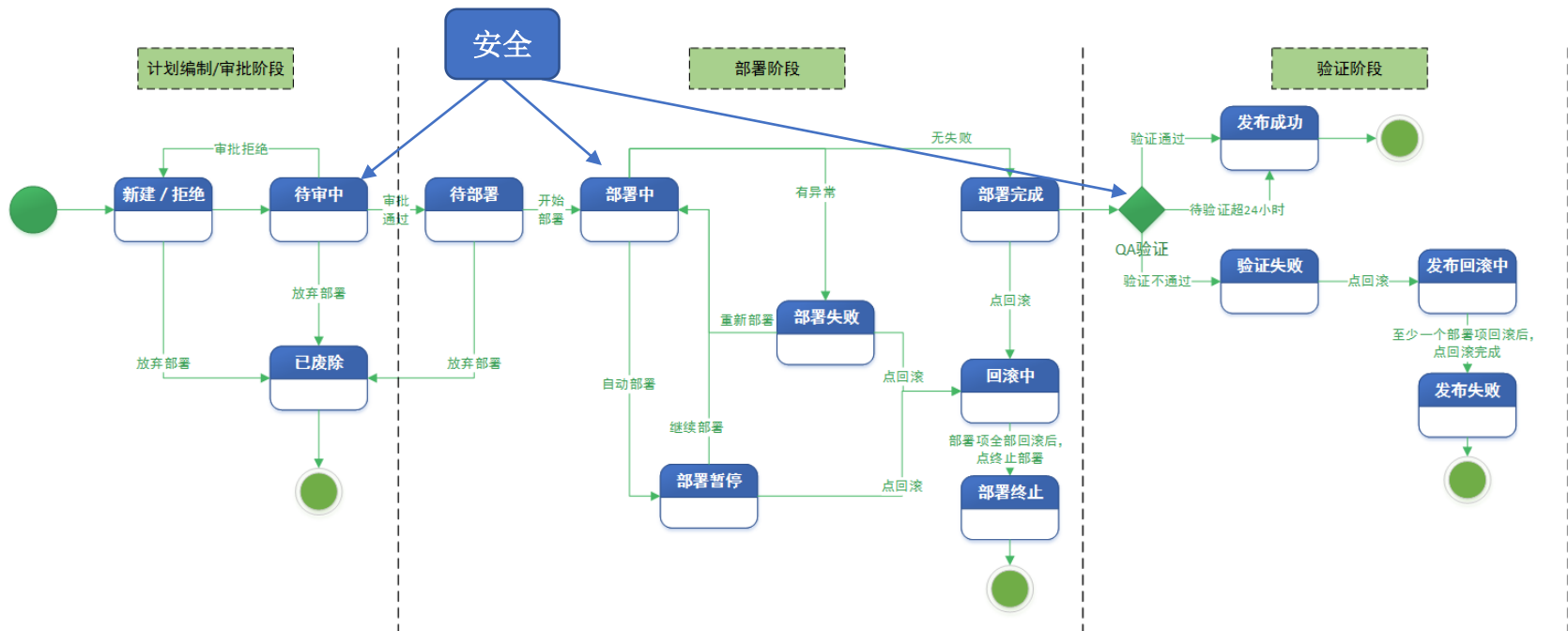
## 选用合适的工具

- 需求



# 实施案例剖析及建议

常规发布状态模型



# 实施案例剖析

## 1. 从易到难

- 利用现有平台、工具
- 减少手工操作
- 手工补充
- 自动代码扫描（最容易接受并使用）

## 2. 后续计划

- 自动编码
- 自动需求分析
- 自动架构设计



# 实施案例剖析-人员收获

开发人员：

代码质量提高效率提升



安全测试：

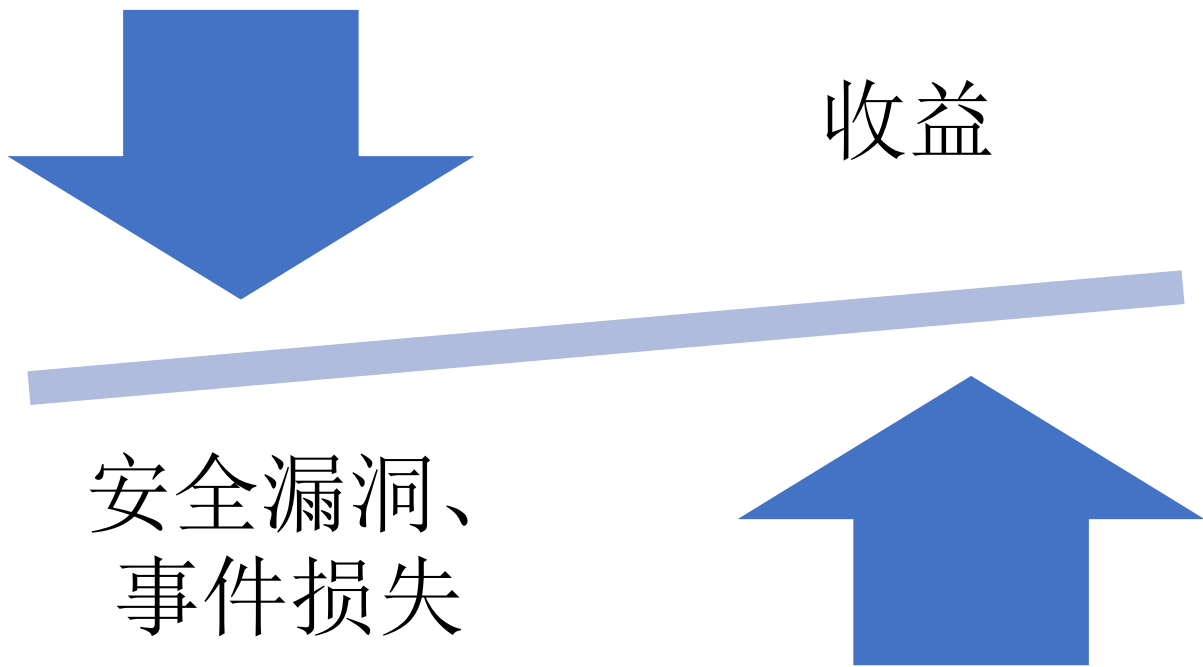
工作量明显减少



运维：

OnCall的时候电话少了

# 实施案例剖析-经济收益







# Thanks

DevOps 时代社区 荣誉出品



想第一时间看到高效运维社区  
的新动态吗？

