S-SDLC VS DevSecOps

金融企业 - 趋势研究与实践

whoami — whoami@Svens-MacBook-Pro — ~ — -zsh — 120×36

```
Last login: Sun Sep  6 10:03:38 on ttys000
➜  ~
```

Last login: Wed Dec 23 on ttys000

➜ ~ **whoami**

刘亦翔**#Sven**

➜ ~ **uname –a**

安信证券 - 安全管理岗 安全从业**6+**年

负责安全攻防、安全运营、**DevSecOps**相关工作。

独立运营微信公众号《极思》。

2017年**ASRC**、**AFSRC**、**JSRC top** 白帽子。

极思

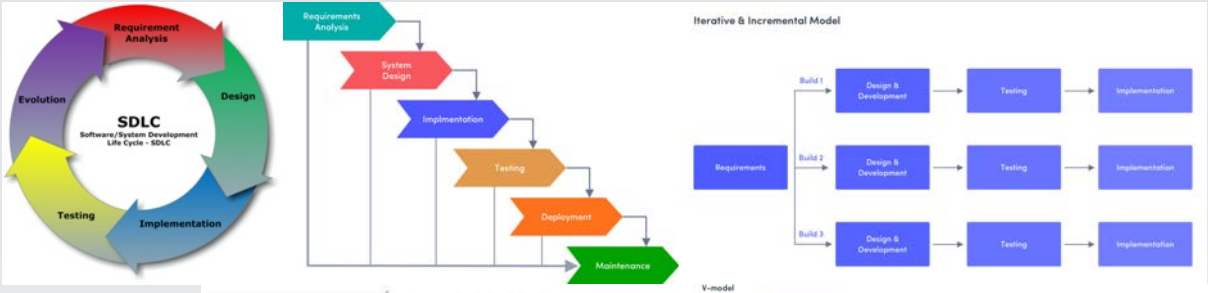
微信扫描二维码，关注我的公众号

主题

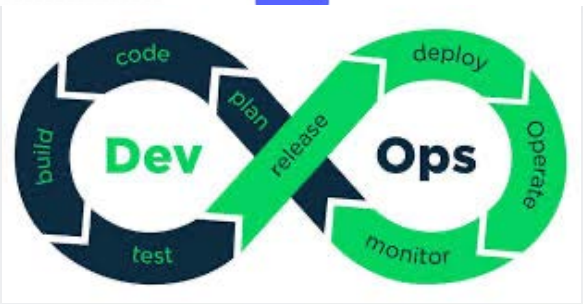
SDLC & DevSecOps 发展趋势
SDLC & DevSecOps 适用企业
SDLC & DevSecOps 应用实践

对象：都是圈内懂行人
范围：金融企业

SDLC



瀑布模型（1950年代）
迭代增量式（1970年代）
螺旋和V模型（1980年代末）
Scrum（1995年）
敏捷方法的兴起（ 1990-2000年代）
DevOps： DevOps 之父 Patrick在比利时举办了首个DevOps日(2009年）



SDLC 与 安全

安全为SDLC量身打造的一套战甲
基于SDLC
安全措施融入其中

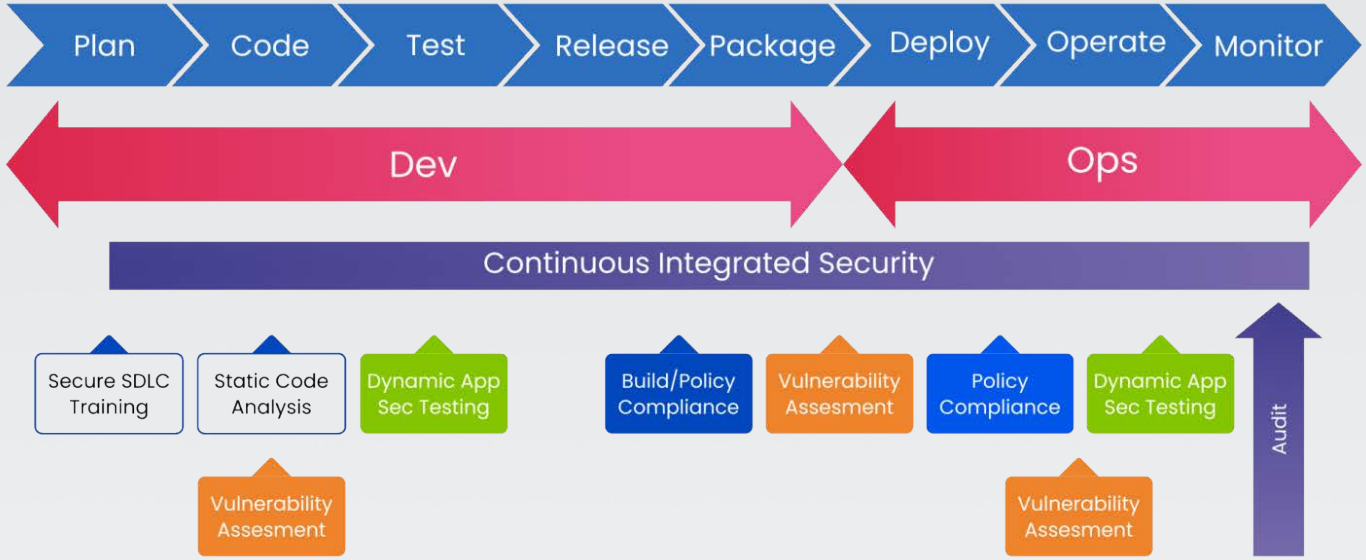
Software Development Lifecycle (SDLC)

Secure Software Development Lifecycle (SSDLC)

Requirments Phase Offerings	Design Phase Offerings	Develop Phase Offerings	Test Phase Offerings	Deploy Phase Offerings
Security Requirements	Design Review & Threat Models	- Static Analysis Tools - Secure Coding	- Ask in Slack - Security Testing	- Pentest in Product - Incident Response Support

DevOps 与 安全

安全为DevOps量身打造的一套战甲
基于DevOps
安全措施融入其中



定位与目标

S-SDLC
帮助软件企业降低安全问些，提升软件安全质量。

DevSecOps
核心理念为安全是整个IT团队（包括开发、运维及安全团队）每个人的责任，需要贯穿从开发到运营整个业务生命周期的每一个环节。
包含运维

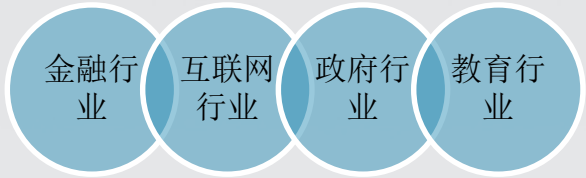
安全历程：渗透测试》源码检测》上线检测》SDLC 》DevOps
安全在不同开发模式下表现出的不同形式

适用企业

选择 S-SDLC or DevSecOps
一、看企业当前使用的软件研发模型
二、看企业IT规划使用的软件研发模型
三、看企业安全建设的进度

企业特点

银行、证券、保险等



金融行业

业务

- 容易招攻击者
- 线上业务众多
- 业务关联复杂

IT

- 历史包袱重
- 机房和IDC多
- 供应商强依赖

驱动力

- 监管合规
- 安全事件
- 安全风险

人员

- 老领导众多
- 元老员工众多
- 人员关系复杂

驱动力

- DevOps 建设引入新风险控制
- DevOps 三级评级的安全需求
- 原安全检测措施自动化升级
- 提升安全控制节点的控制力

驱动/驱动力和安全策略


规划驱动
风险驱动
事件驱动
合规驱动

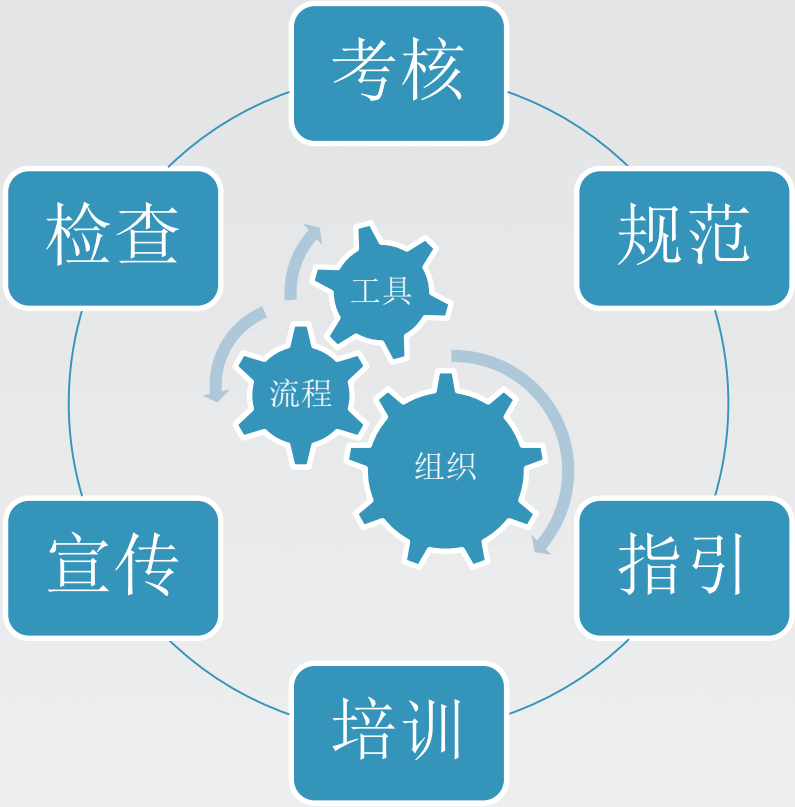

驱动力类型
考核
双向考核 多奖少罚
协作
求同存民 合作共赢
专家
利害驱动 严谨专业
人情
诚信为基 守望相助
魅力
人畜无害 乐于助人

主要风险

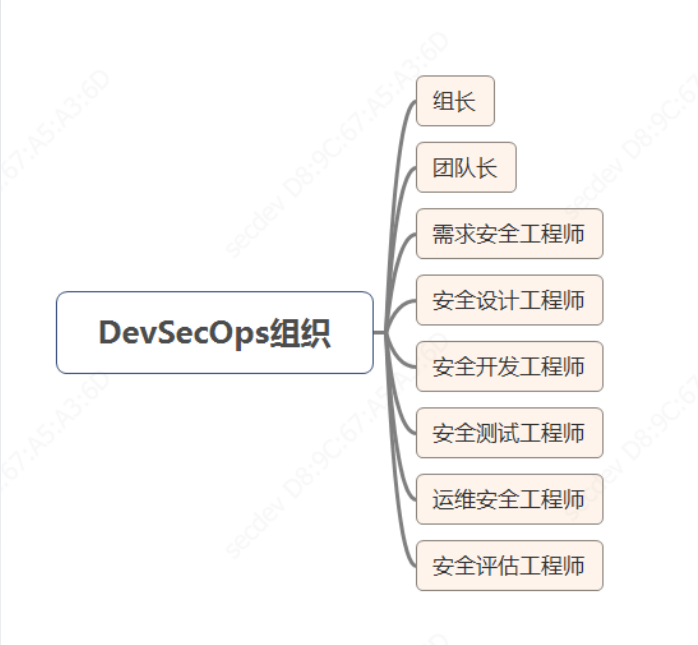
新风险	原风险	问题
• 容器技术 • 云平台	• 三方类库 • 组件架构	• 检测效率 • 工具支持

管理方案

风险驱动组织
组织驱动流程
流程驱动工具



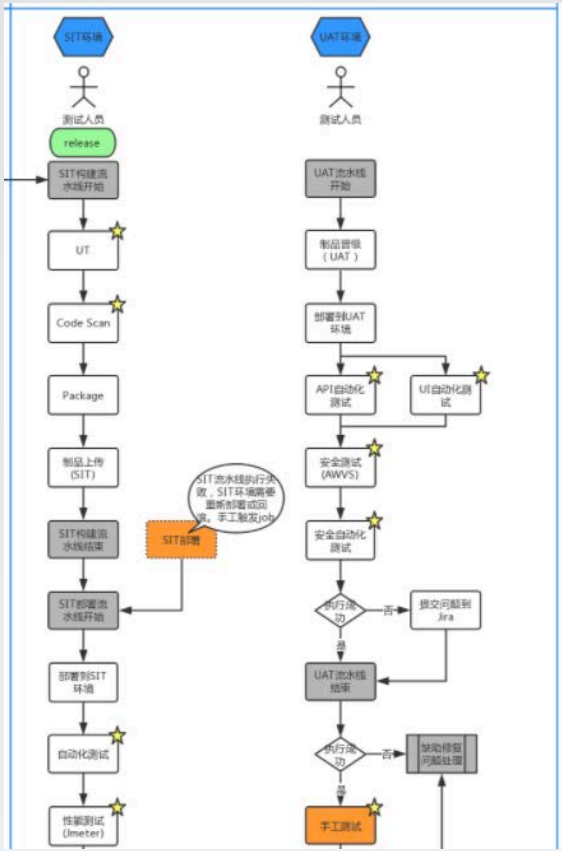
组织

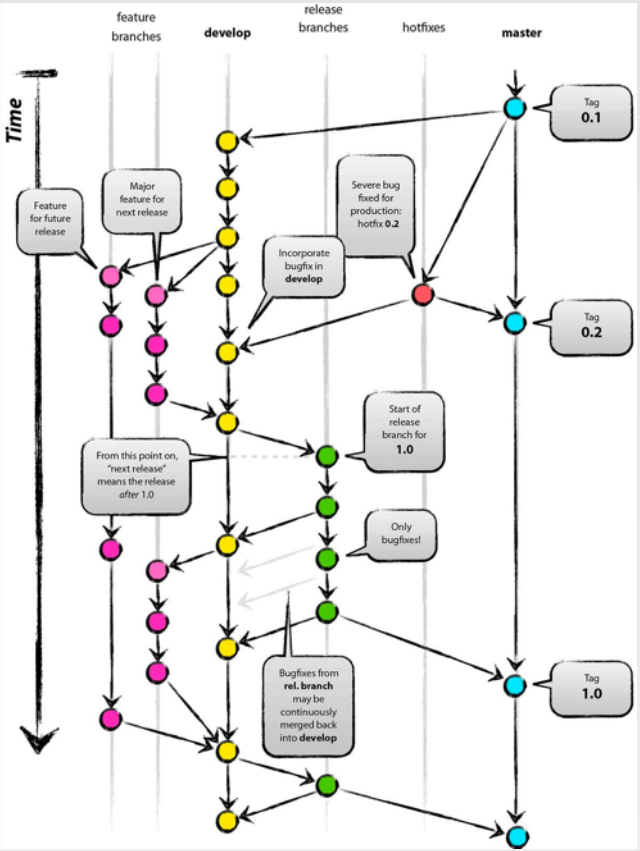


1. 组长：企业IT部门总经理\总监担任。
2. 团队长：邀请团队长参加（协调）。
3. 安全需求工程师：需求评审人兼职。
4. 安全设计工程师：设计评审人兼职。
5. 安全开发工程师：开发小组长兼职。
6. 安全测试工程师：安全团队专人担任。
7. 安全运维工程师：安全团队专人担任。
8. 安全评估工程师：安全团队专人担任。

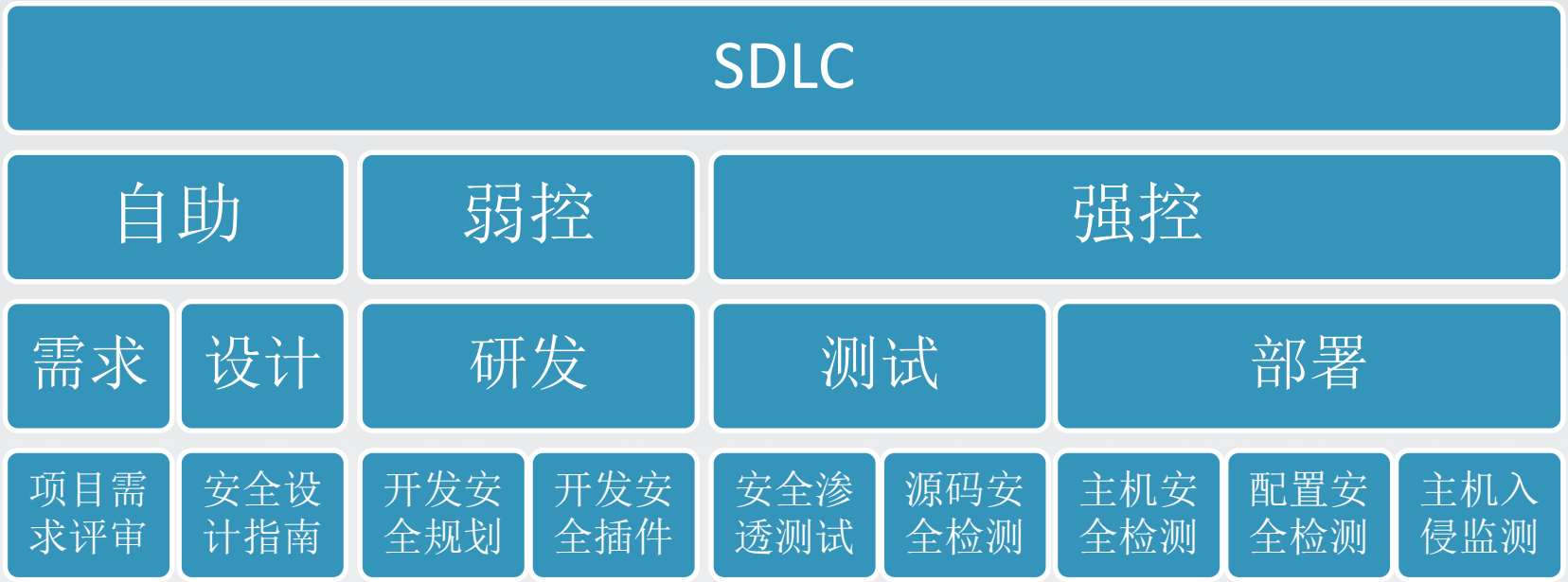
流程

Release and UAT

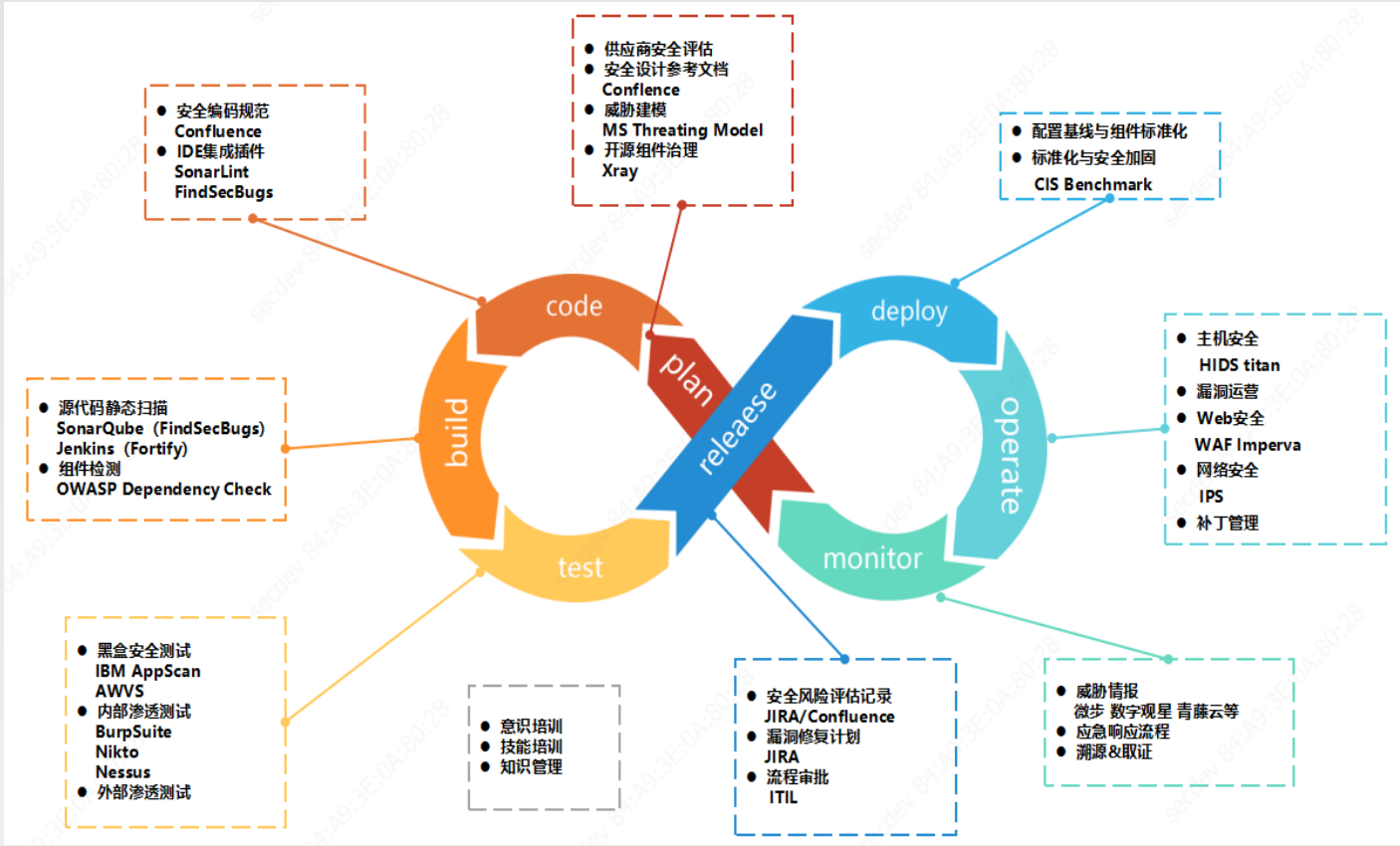




SDLC 实践


SDLC
自助
弱控
强控
需求
设计
研发
测试
部署
项目需求评审
安全设计指南
开发安全规划
开发安全插件
安全渗透测试
源码安全检测
主机安全检测
配置安全检测
主机入侵监测

DevOps


code
plan
releaese
deploy
operate
monitor
test
build
● 安全编码规范
Confluence
● IDE集成插件
SonarLint
FindSecBugs
● 供应商安全评估
● 安全设计参考文档
Conflence
● 威胁建模
MS Threating Model
● 开源组件治理
Xray
● 配置基线与组件标准化
● 标准化与安全加固
CIS Benchmark
● 主机安全
HIDS titan
● 漏洞运营
● Web安全
WAF Imperva
● 网络安全
IPS
● 补丁管理
● 源代码静态扫描
SonarQube（FindSecBugs）
Jenkins（Fortify）
● 组件检测
OWASP Dependency Check
● 黑盒安全测试
IBM AppScan
AWVS
● 内部渗透测试
BurpSuite
Nikto
Nessus
● 外部渗透测试
● 意识培训
● 技能培训
● 知识管理
● 安全风险评估记录
JIRA/Confluence
● 漏洞修复计划
JIRA
● 流程审批
ITIL
● 威胁情报
微步 数字观星 青藤云等
● 应急响应流程
● 溯源&取证

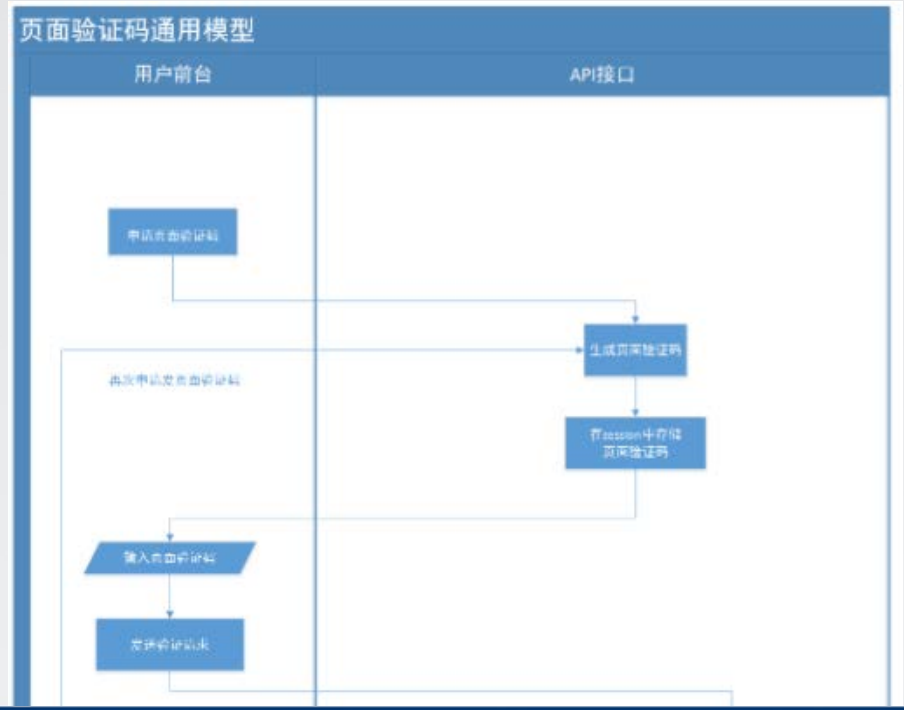
安全模块

安全开发管理 （SDL）

由 苏浩创建, 最终由 刘亦翔修改于 2019/11/12

- Docker容器镜像安全扫描
- Jenkins配置集成项目扫描
- Microsoft 威胁建模
- OWASP Threat Dragon
- SDL解决方案
- ThreatModeler
- VSAQ供应商安全评估
- 安全嵌入研发流程详细实施方案
- 开发findbug扫描使用说明
- 开发使用fortify扫描说明
- 梆梆安全应用安全测评平台

安全设计参考



研发规范

Java安全编码实践总结

由 官康强创建, 最后修改于2020/07/22

本文漏洞复现的基础环境信息：jdk版本：1.8，

安全编码实践

Sql注入防范

常见安全编码方法：预编译+输入验证

预编译适用于大多数对数据库进行操作的场景，
会产生语法错误。常见的预编译写法如下

jdbc：

```
String
```

漏洞模块

由 刘亦翔创建, 最后修改于2019/03/21

目录

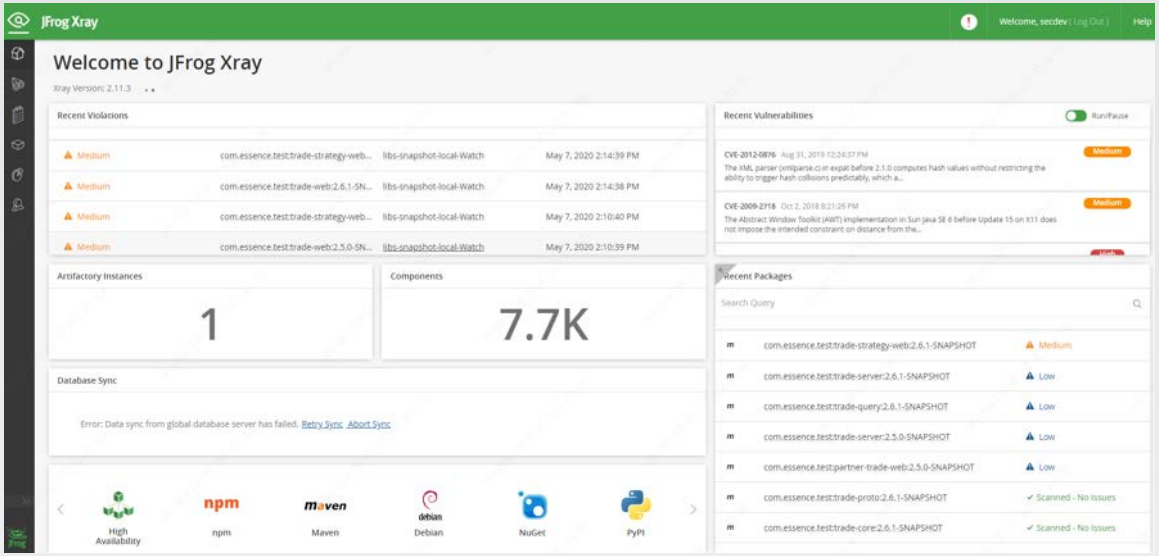
功能模块

由 刘亦翔创建, 最终由 官康强修改于 2019/05/23

目录

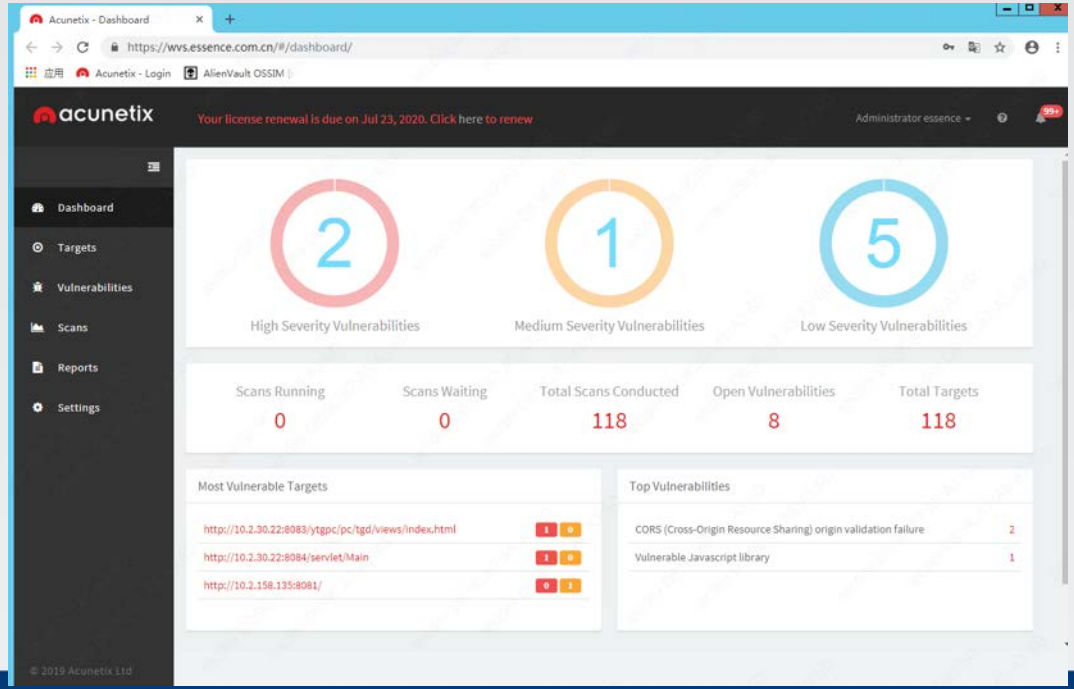
第三方类库

JFrog Xray 通过对容器和软件制品进行多层分析，来了解漏洞、许可证合规性和质量保证持续管理和审计CI/CD流水线中使用和生成的所有制品



应用安全扫描

自动化爬虫式应用安全扫描
自动化代理式应用安全扫描



配置安全


应用配置安全指引
由 官康强创建, 最终由 刘亦翔修改于 2019/11/11
APM
Beats
ElasticSearch
GitLab
Grafana
Hadoop
iCube
Jenkins
MongoDB
MySQL
NAS
Prometheus
Redis
smartBI
Tomcat
选择基线规则:
搜索规则
系统基线
CIS Centos 6 Level 1
CIS Centos 6 Level 2
CIS Centos 7 Level 1
CIS Centos 7 Level 2
CIS RedHat 6 Level 1
CIS RedHat 6 Level 2
CIS RedHat 7 Level 1
CIS RedHat 7 Level 2
选择基线规则:
搜索规则
中国等保 Oracle 应用基线检查
中国等保 Resin 应用基线检查
中国等保 WebSphere 应用基线检
中国等保-Apache 应用基线检查-
中国等保-Apache 应用基线检查-
中国等保-DB2 应用基线检查
中国等保-MongoDB 3.0/3.2 应用
中国等保-MongoDB 3.4 应用基线
中国等保-MySQL 5.5/5.6应用基线

入侵检测

入侵总览

业务组 | 2020-12-23-2020-12-24 | 查找主机

数据总览

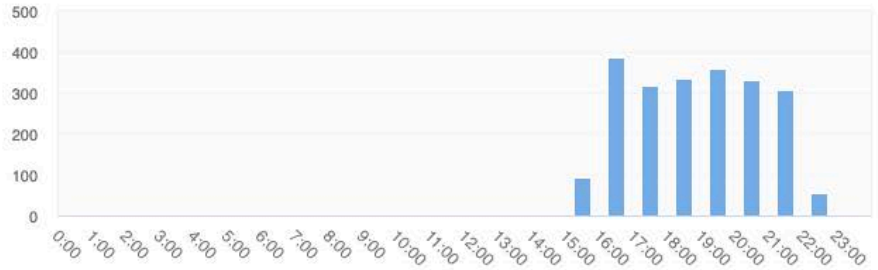
告警总数

2,519

已忽略告警

337

告警时间分布



受攻击影响主机TOP5

实时监控 查看更多

DevOps 评级


安信证券股份有限公司
2020 IT行业年度优秀案例
DevOps类
(安信证券DevOps研发转型实践)
2020 GOLF+
IT新治理领导力论坛
2020.12


兹证明
安信证券股份有限公司

Q&A

极思

微信扫描二维码，关注我的公众号