EISS-2018企业信息安全峰会
之上海站

"Face the challenge,Embrace the best practice"

November 30th,2018|SHANGHAI

2018年11月30日|上海

安全加

DevSecOps在金融机构落地实践

华泰证券 庄飞

CONTENT

DevOps

快速交付价值

DevOps 道法术器

价值观，对目标 价值的定位	道	VALUE	快速交付价值，灵活响应变化
实现价值观的 战略、方法	法	WHY	全局打通敏捷开发 & 高效运维
战术、技术、 具体的手段	术	HOW	系统应用指导原则、最佳实践
用工具提高效率 复杂问题简单化	器	WHAT	端到端工具链相互联通和整合

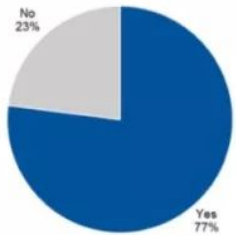
系统思考的层次

解决问题的层次

张乐（乐帅@高效运维社区）

DevOps下安全面临的挑战

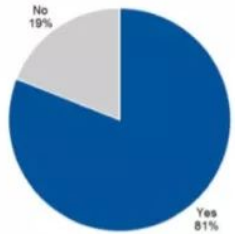
Figure 1. Information Security Professionals: Do You Believe Your Information Security Policies/Teams Are Slowing IT Down?



n = 41

Source: Gartner (September 2016)

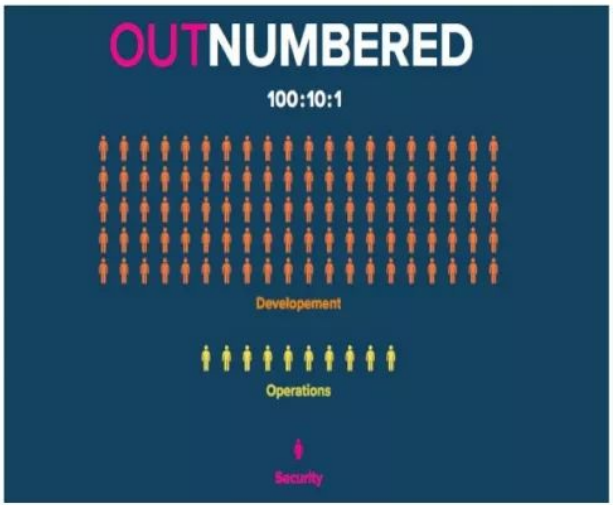
Figure 2. IT Operations Professionals: Do You Believe Your Information Security Policies/Teams Are Slowing IT Down?

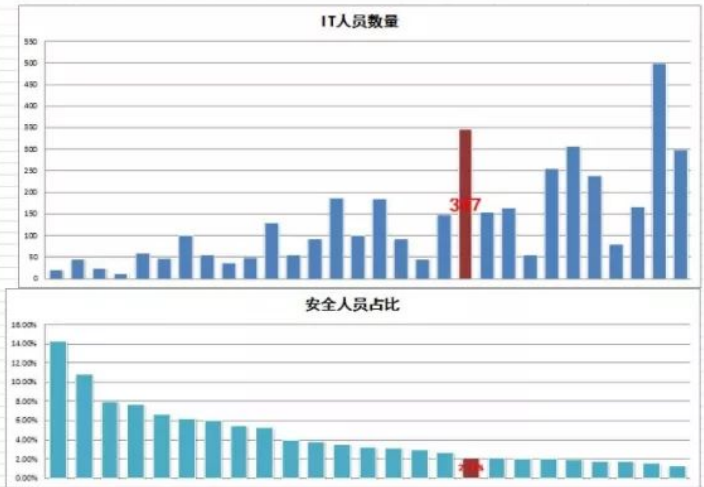


n = 93

Source: Gartner (September 2016)

DevOps安全面临的挑战

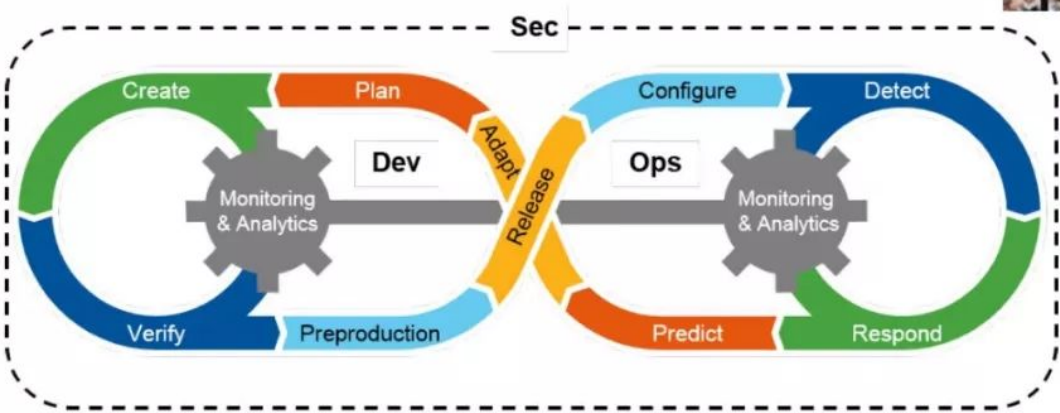




DevSecOps Community Survey 2018 @Sonatype

证券行业调研报告 2017 上交所课题

DevSecOps



"everyone is responsible for security"

GOAL: safely distributing security decisions at **speed** and **scale** to those who hold the highest level of context **without** sacrificing the safety required.

How DevSecOps?

Building a DevSecOps Program (CALMS)

Culture

Break down barriers between Development, Security, and Operations through education and outreach

Automation

Embed self-service automated security scanning and testing in continuous delivery

Lean

Value stream analysis on security and compliance processes to optimize flow

Measurement

Use metrics to shape design and drive decisions

Sharing

Share threats, risks, and vulnerabilities by adding them to engineering backlogs

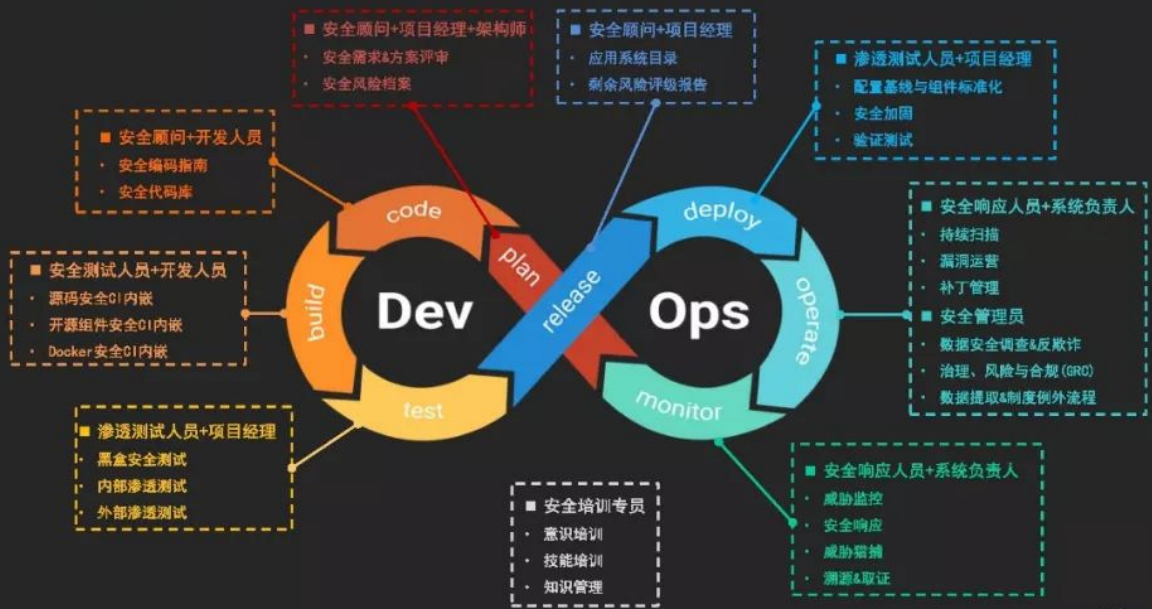
Culture

Process

Technology

SDL-软件安全生命周期BSI框架

安全活动干系人


■ 安全顾问+项目经理+架构师
· 安全需求&方案评审
· 安全风险档案
■ 安全顾问+项目经理
· 应用系统目录
· 剩余风险评级报告
■ 渗透测试人员+项目经理
· 配置基线与组件标准化
· 安全加固
· 验证测试
■ 安全顾问+开发人员
· 安全编码指南
· 安全代码库
■ 安全响应人员+系统负责人
· 持续扫描
· 漏洞运营
· 补丁管理
■ 安全管理员
· 数据安全调查&反欺诈
· 治理、风险与合规(GRC)
· 数据提取&制度例外流程
■ 安全测试人员+开发人员
· 源码安全CI内嵌
· 开源组件安全CI内嵌
· Docker安全CI内嵌
code
plan
release
deploy
operate
monitor
test
build
Dev
Ops
■ 渗透测试人员+项目经理
· 黑盒安全测试
· 内部渗透测试
· 外部渗透测试
■ 安全培训专员
· 意识培训
· 技能培训
· 知识管理
■ 安全响应人员+系统负责人
· 威胁监控
· 安全响应
· 威胁猎捕
· 溯源&取证

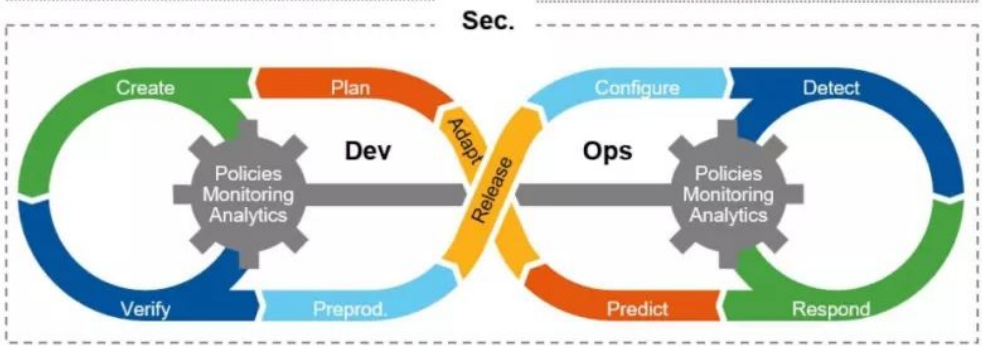
DevSecOps 应用安全活动

Secure Design

- Security requirements
- Threat modeling
- Secure-coding practices
- Open-source software governance

Externalized Security

- Application protection
- Network-based application protection
- Container and infrastructure security



- Open-source software analysis
- Application security testing
- Binary or protocol fuzzing
- Vulnerability correlation and security testing orchestration

Development Verification

- Vulnerability assessment
- Security monitoring

Production Security Monitoring

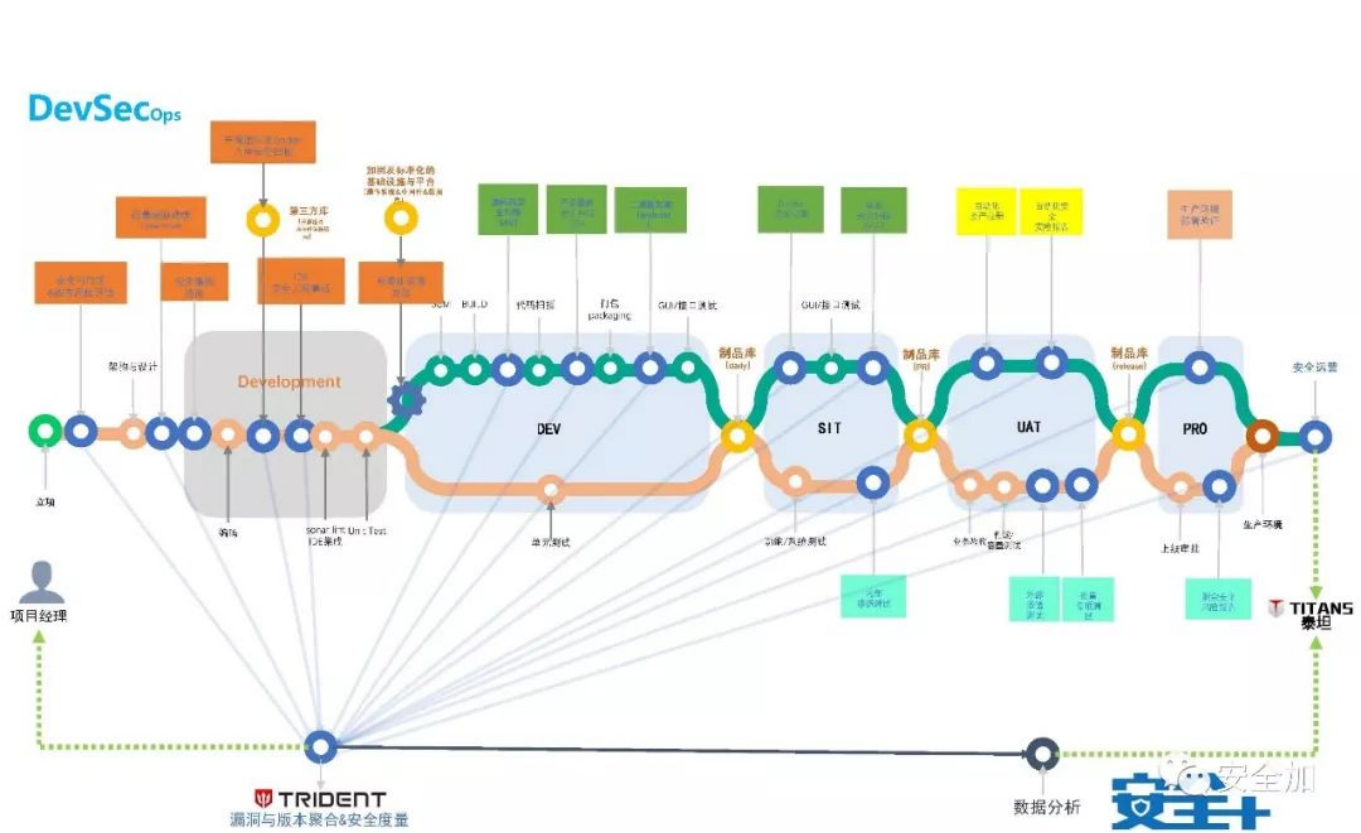
安全内嵌研发流程

分级				流程策略表 (Process)	安全策略表 (Security)	配置策略表 (Configuration)	测试策略表 (Test)	数据策略表 (Data)	连续性策略表 (Continuity)
研发类	1、纯自研、自研+在岸外包	A	直接面向客户的系统、面向集团的核心系统 （备注：如此类系统出现异常，将会影响外部客户体验）	P1档	S1档	C1档	T1档	D2档（非直接面向技术类系统） D3档（直接面向技术类系统）	C1档
		B	支撑以多开单的系统（备注：此类系统主要面向内部用户使用）	P2档	S2档	C1档	T1档	D2档	C2档
		C	前台全集团的系统	P2档	S2档	C1档	T1档	D1档（数据分析、资源类系统） D2档（自助营分析、展现类系统）	C3档
		D	面向信息技术部的系统	P2档	S2档	C2档	T1档	-	C2档

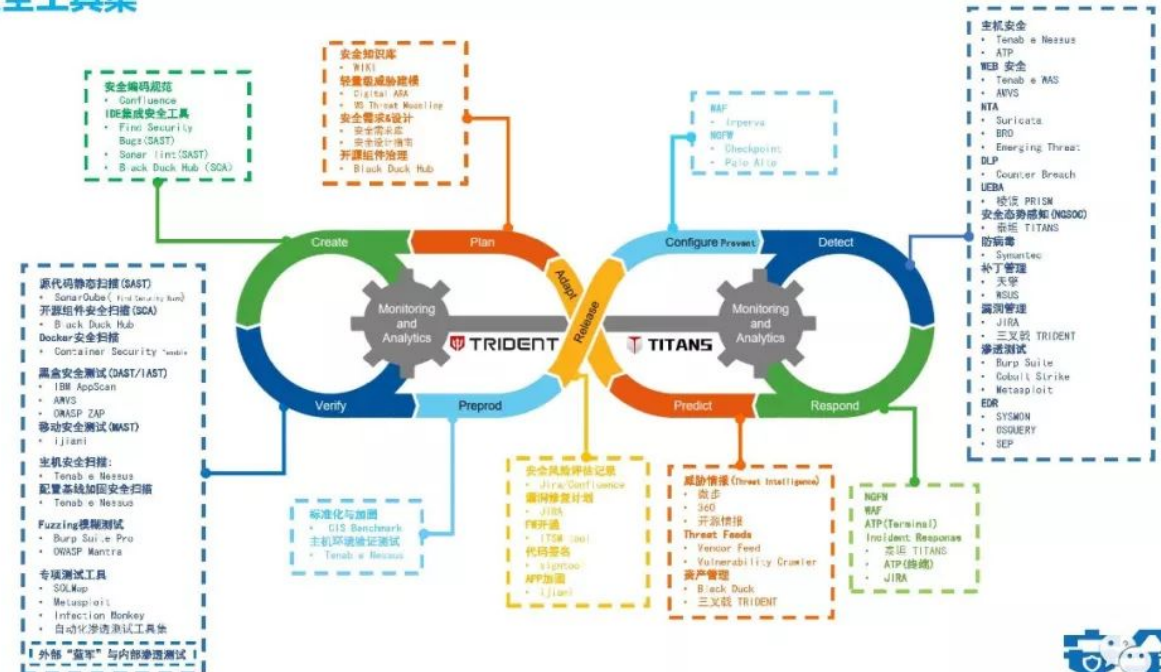
项目过程

套餐级别	套餐详情
S1档	活动执行如下： 1 安全需求（轻量级威胁建模）(安全顾问确定相应的安全需求策略) 2 安全架构与设计(安全顾问确定安全架构策略) 3 安全编码(按照安全编码规范进行安全编码) 4 源代码与开源组件扫描(CI集成sonar进行源代码安全扫描) 5 应用系统自录 6 黑盒安全测试 7 内部渗透测试 8 外部渗透测试 9 生产环境部署验证 10 剩余风险评级与接受报告

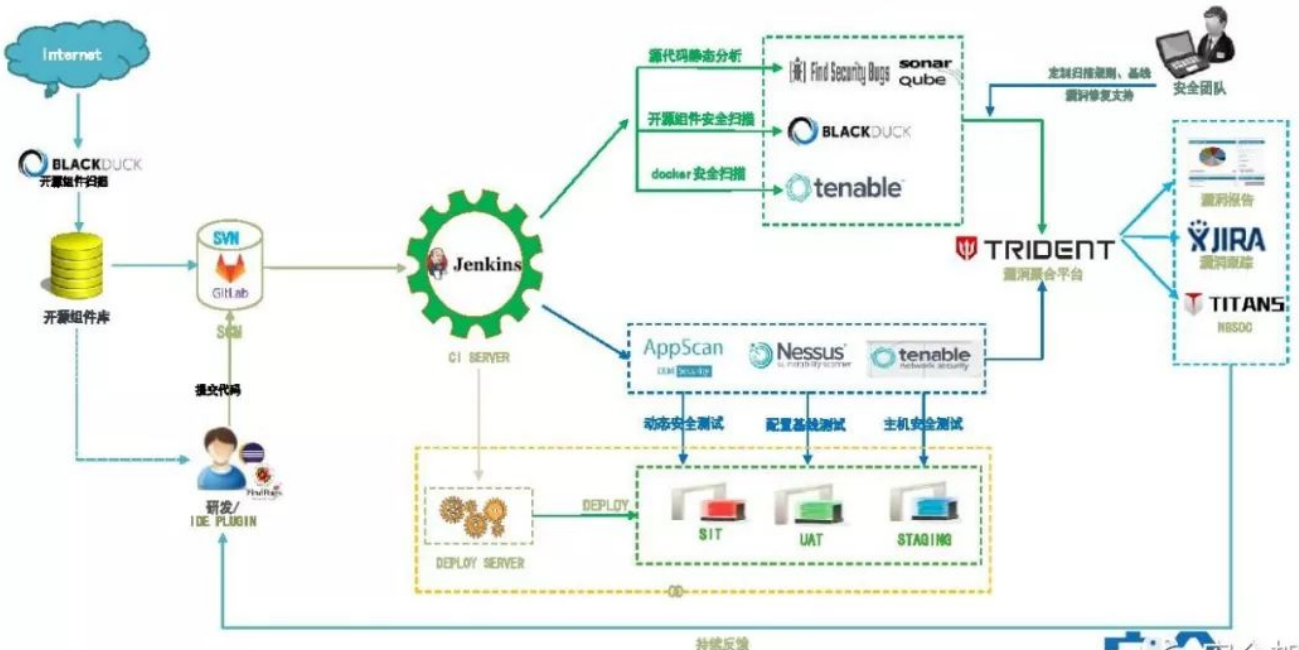
安全策略


DevSecOps
第三方库
Development
DEV
SIT
UAT
PRO
制品库
(daily)
制品库
(PRE)
制品库
(release)
安全运营
项目经理
TRIDENT
漏洞与版本聚合&安全度量
数据分析
TITANS
泰坦

安全工具集


安全编码规范
• Confluence
IDE集成安全工具
• Find Security Bugs(SAST)
• Sonar lint(SAST)
• Black Duck Hub (SCA)
安全知识库
• WIKI
轻量级威胁建模
• Digital ARA
• MS Threat Modeling
安全需求&设计
• 安全需求点
• 安全设计指南
开源组件治理
• Black Duck Hub
WAF
• Imperva
NGFW
• Checkpoint
• Palo Alto
主机安全
• Tenab e Nessus
• ATP
WEB 安全
• Tenab e WAS
• AWVS
NTA
• Suricata
• BRO
• Emerging Threat
DLP
• Counter Breach
UEBA
• 绿盾 PRISM
安全态势感知(NGSOC)
• 启明 TITANS
防病毒
• Symantec
补丁管理
• 天擎
• WSUS
漏洞管理
• JIRA
• 三叉戟 TRIDENT
渗透测试
• Burp Suite
• Cobalt Strike
• Metasploit
EDR
• SYSMON
• OSQUERY
• SEP
源代码静态扫描(SAST)
• SonarQube(Find Security Bugs)
开源组件安全扫描(SCA)
• Black Duck Hub
Docker安全扫描
• Container Security Vendor
黑盒安全测试(DAST/IAST)
• IBM AppScan
• AWVS
• OWASP ZAP
移动安全测试(MAST)
• ijiami
主机安全扫描:
• Tenab e Nessus
配置基线加固安全扫描
• Tenab e Nessus
Fuzzing模糊测试
• Burp Suite Pro
• OWASP Mantra
专项测试工具
• SQLMap
• Metasploit
• Infection Monkey
• 自动化渗透测试工具集
外部"蓝军"与内部渗透测试
标准化与加固
• CIS Benchmark
主机环境验证测试
• Tenab e Nessus
安全风险评估记录
• Jira/Confluence
漏洞修复计划
• JIRA
FW开通
• ITSM tool
代码签名
• signtool
APP加固
• ijiami
威胁情报(Threat Intelligence)
• 微步
• 360
• 开源情报
Threat Feeds
• Vendor Feed
• Vulnerability Crawler
资产管理
• Black Duck
• 三叉戟 TRIDENT
NGFW
WAF
ATP(Terminal)
Incident Response
• 启明 TITANS
• ATP(终端)
• JIRA
Create
Plan
Configure
Prevent
Detect
Verify
Preprod
Predict
Respond
Monitoring and Analytics
TRIDENT
Agility
Release
TITANS
Monitoring and Analytics

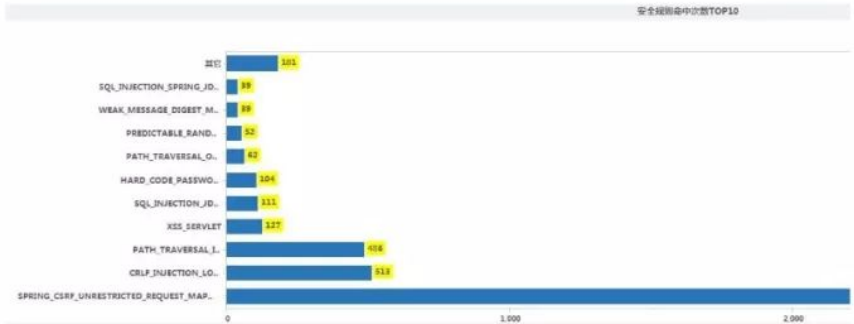
DevSecOps工具链集成



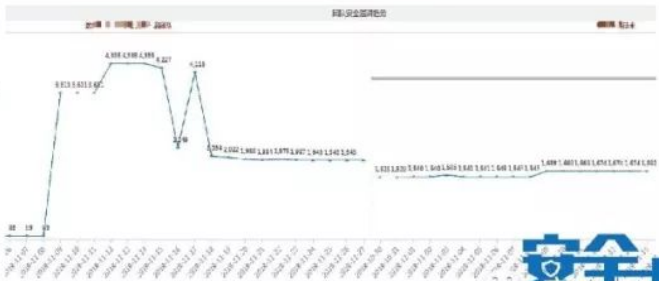
DevOps中安全活动、门限及度量指标

安全活动	DevOps平台门限	DevOps数据接口	度量指标
标准化资源发放	OS、中间件等组件全部从制品库获取	制品库API	A1：全自动发放和验证资源发放标准资源（除模板更新需要手工）比例 A2：标准化覆盖通用中间件和数据库模板比例 A3：新发机器标准化覆盖率 A4：Windows全网标准化覆盖率 A5：Linux在DMZ标准化覆盖率 B1：安全加固规范数量 C1：项目资源标准化程度
源代码安全扫描	vulnerability中漏洞级别为blocker、critical、major数量为0 (sonar qube提供API接口)	从sonar qube api调用获取	A1：源代码安全扫描项目覆盖率 A2：源代码安全扫描项目CI集成覆盖率 B1：源代码安全漏洞密度(Vulnerability Density) B2：源代码安全检测规则数量 C1：源代码安全扫描速度 C2：漏洞误报率
开源组件安全扫描	暂时通过治理，不作门限要求 漏洞通过开源组件平台API获取，在DevOps平台展示漏洞状态	1、从blackduck restful api获取项目对应的开源组件漏洞 2、devops平台进行展示	A1：开源组件安全扫描项目覆盖率 B1：项目含有漏洞的开源组件数量 B2：项目开源组件安全漏洞数量 C1：开源组件扫描速度 D1：开源组件安全风险指标 D2：开源组件License合规指标
Docker安全扫描	docker安全漏洞Medium、High数量为0 (docker安全工具提供API接口)	docker安全扫描工具提供API接口	A1：docker镜像扫描项目覆盖率 B1：docker镜像安全漏洞数量 C1：docker镜像安全扫描速度 D1：docker镜像安全风险指标
黑盒安全扫描	黑盒安全漏洞Medium、High数量为0 (三叉戟安全测试平台提供API接口)	三叉戟安全测试平台提供restful API接口	A1：黑盒安全扫描项目覆盖率 B1：黑盒安全扫描漏洞数量 C1：黑盒安全扫描速度 C2：黑盒安全扫描漏洞发现率 C3：黑盒安全扫描漏洞误报率

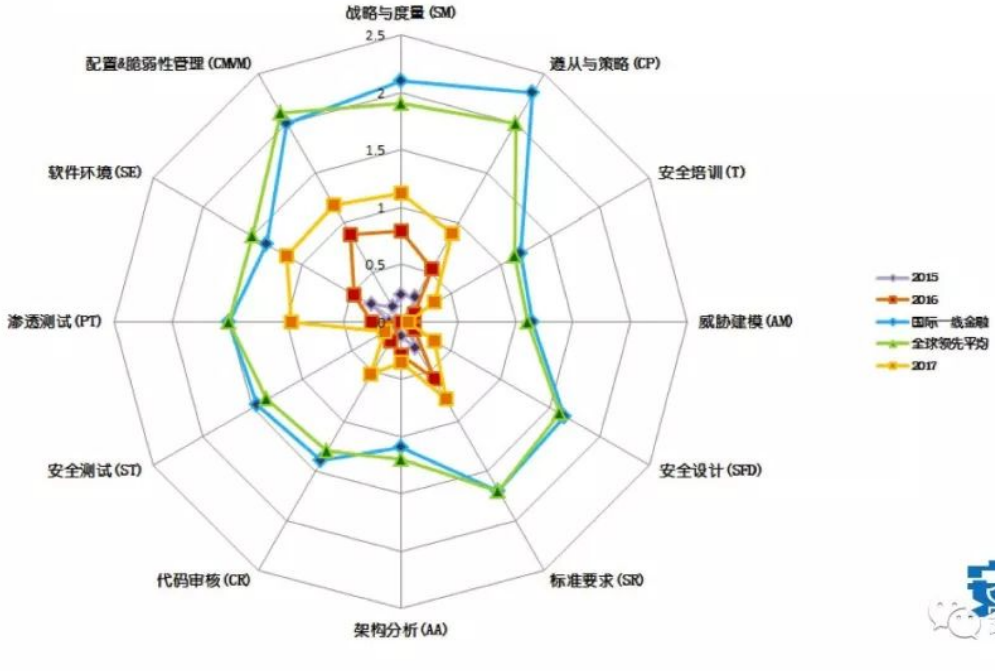
度量及反馈


安全规则命中次数TOP10
其它
SQL_INJECTION_SPRING_JD..
WEAK_MESSAGE_DIGEST_M..
PREDICTABLE_RAND..
PATH_TRAVERSAL_O..
HARD_CODE_PASSWO..
SQL_INJECTION_JD..
XSS_SERVLET
PATH_TRAVERSAL_I..
CRLF_INJECTION_LO..
SPRING_CSRF_UNRESTRICTED_REQUEST_MAP..
101
39
39
52
62
104
111
127
416
513
0
1,000
2,000


部门安全漏洞趋势


团队安全漏洞趋势

软件安全成熟度度量



DevSecOps 能力成熟度模型

中华人民共和国　　行业标准

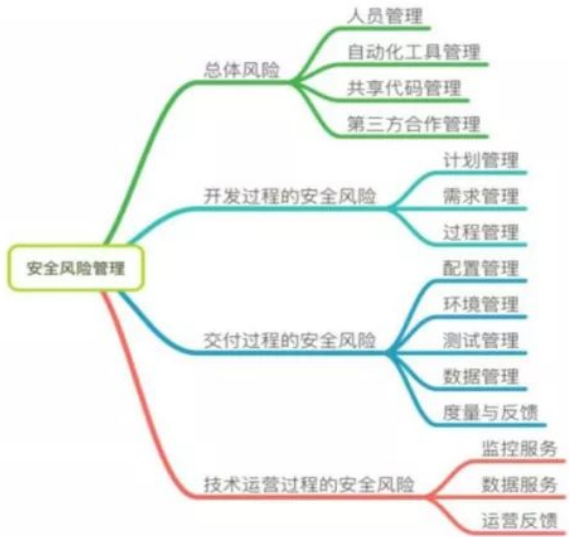
XX/T XXXXX—XXXX

研发运营一体化（DevOps）能力成熟度模型
第 6 部分 安全风险管理

6 研发运营一体化控制开发过程风险

为降低后续交付、运营中的安全风险，保障研发运营一体化的整体安全，必须提前实施安全风险管理工作，在制定计划的每个步骤时纳入安全风险管理，确定整体的安全风险需求，并在过程中实施安全风险管理，通过自动化、智能化的方式实现。这是研发运营一体化的基础。

级别	计划管理	需求管理	过程管理
3	将安全纳入质量、测试计划	在需求收集、需求分析、需求与用例、需求验收四部分均实现安全，根据权限业务逻辑和已知风险，确定安全需求，包括基础平台、开源工具、编码安全。	过程中每位成员均参与安全过程，产品每次迭代中按照安全线性过程进行管控
4	将安全纳入开发、质量、测试计划	在需求收集、需求分析、需求与用例、需求验收四部分均实现安全，根据权限业务逻辑和已知风险，确定安全需求，包括基础平台、开源工具、编码安全、接口服务安全。	过程中每位成员均参与安全过程，产品每次迭代中按照安全线性过程进行管控，并将这些安全过程进行可视化



平台建设

CARTA

持续自适应风险与信任评估框架

DevSecOps

安全业务与工程能力

1

TITANS

泰坦人工智能安全态势感知

泰坦，利用大数据、智能分析引擎 和 可视化等手段，结合威胁情报，对企业面临的网络攻击进行检测，快速、有效地为企业建立威胁检测、分析、处置和全网安全态势感知能力，使得企业的信息安全可知、可见、可控。

2

PRISM

棱镜UEBA用户行为分析平台

棱镜，通过机器学习技术，对用户的行为进行智能化分析，建立用户风险画像，实时检测异常行为和未知威胁，及时发现内部用户违规行为，如违规操作、帐号盗用、内部欺诈、数据泄露等。

3

Aiyiş

宙斯盾业务反欺诈

宙斯盾，基于设备指纹技术以及海量的设备安全数据、威胁情报数据和用户行为数据，利用流式分析处理、数据挖掘和机器学习等关键技术，构建出独有的以设备安全为核心的智能实时身份反欺诈模型，精准识别和预防各类互联网身份欺诈风险，检测如恶意[illegible]，提升营销效果。

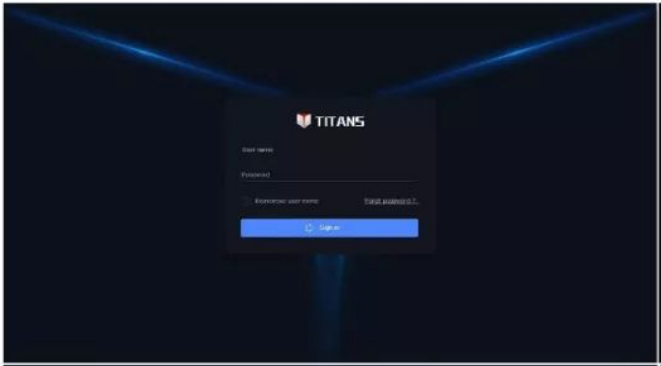
4

TRIDENT

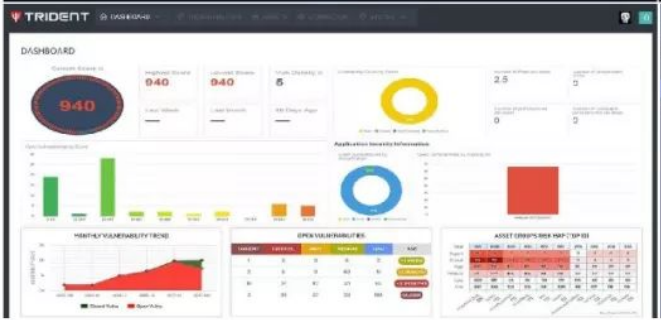
三叉戟安全测试平台

三叉戟，集成漏洞全生命周期管理、资产管理、漏洞知识库、应用安全风险画像、DevSecOps工具链集成、自动化渗透测试工具集等功能，为企业提供一体化安全测试及漏洞管理自服务平台。

平台


TITANS


TITANS
Dashboards
Alerts
Response
Analysis
Reports
Admin
90
RISK
3
Critical Vulnerabilities
9
Risky Assets
Vulnerabilities
3
1
23
7
508
Alerts
Critical Attack Sources
Traffic
Asset Correlation Map
Outbound Alert Trend
Services
Inbound Attacks
Top Risky Hosts
148
10
26
9
2
0


TRIDENT
DASHBOARD
940
940
940
5
2.5
0
2
MONTHLY VULNERABILITY TREND
OPEN VULNERABILITIES
ASSET CRISPR RISK MAP TOP 20


告警类型
告警趋势


谢 谢
安全加