2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

从漏洞视角看敏捷安全

个人简介

武　鑫

奇安信网络安全部

产品安全负责人、QAXSRC负责人

ID：aerfa

5年安全攻防经验，网络尖刀z小队成员

VSRC2016年第二季度“安全专家”、HCSRC总排行榜第一

RSAC主题分享万人云峰会演讲嘉宾、e安在线金牌讲师

微信公众号作者：我的安全视界观

擅长从攻防视角发现并闭环安全隐患，结合甲、乙方工作经验进行企业安全建设、SDL、DevSecOps建设与运营，

对外输出四十余篇原创文章

敏捷安全关键

- 文化
- 流程
- 技术

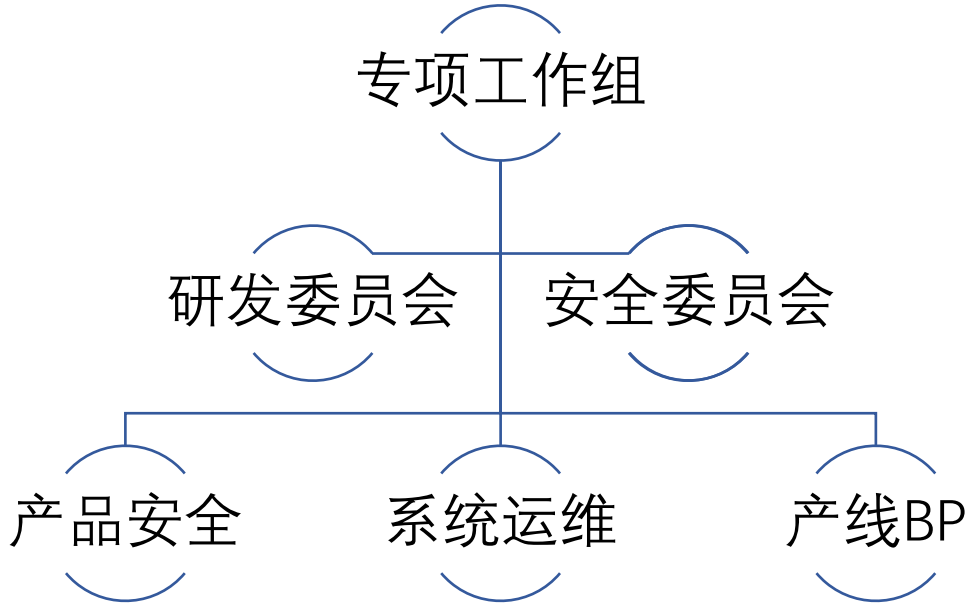
文化：开发运维安全，责任共担

产品自身的安全与研发流程中的各个环节、每个人都息息相关，筑建产品的安全是每个人的责任。

专项工作组：建立开发、运维、安全虚拟工作组，明确工作目标与工作职责

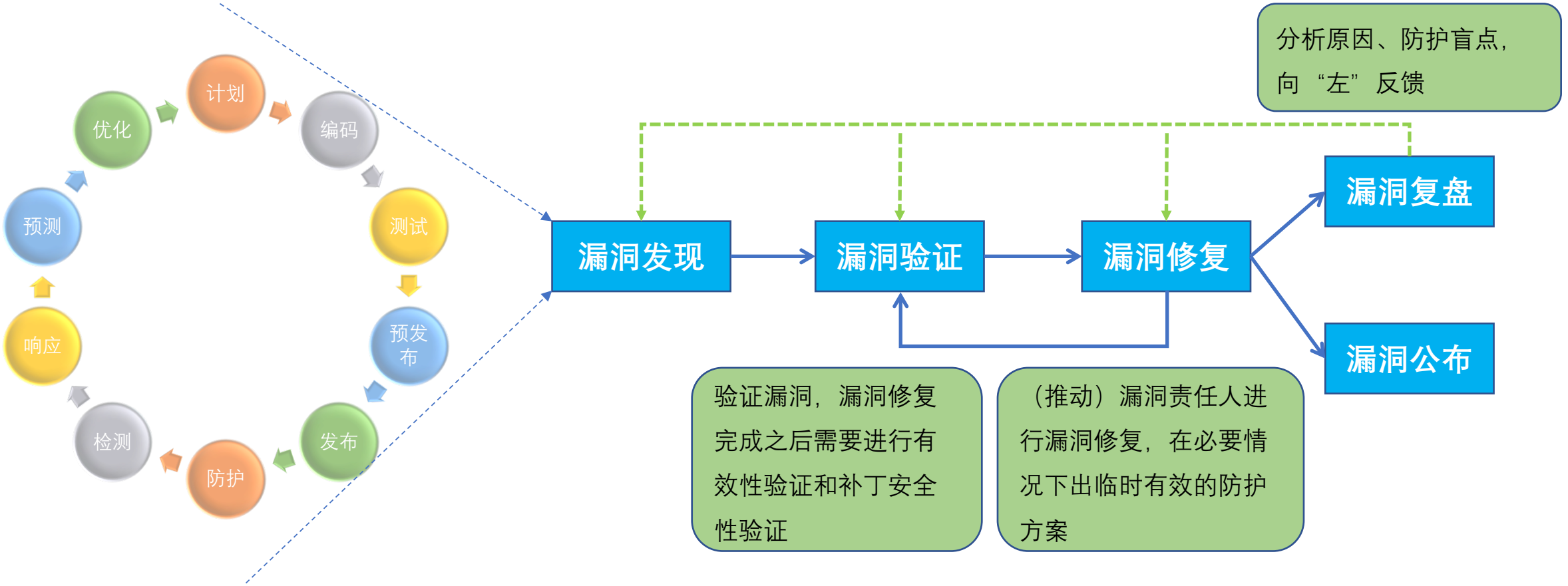
部门BP制度：建立部门安全接口人，负责上传与下达消息、在本部门落地相关安全要求

安全内部分工：在安全团队内部设置不同方向以对应开发安全各环节的安全活动，包括但不仅限于主机安全、安全设计、白盒测试、自动化安全测试、SRC运营等



流程：安全左移，层层主动检测

移植“纵深防御”思想到软件开发流程中，在推动安全“左移”的同时加强各环节安全活动的运营，将层层发现的潜在安全风险与漏洞聚合处置。



技术：构建工具链，发现漏洞

计划	编码	测试	预发布	发布	防护	检测	响应	预测	优化
安全培训	安全编码	三方组件	模糊测试	上线决策	签名验证	主机漏扫	安全编排	AVC	方案调整
安全需求	IDE插件	安全测试	集成测试	软件签名	纵深防御	Web漏扫	威胁狩猎	威胁情报	流程优化
安全设计	安全组件	容器安全	混沌工程	修复计划	完整性检查	渗透测试	溯源取证	安全预警	运营反馈

奇安信代码卫士 — Qi'anxin Codesafe —

奇安信开源卫士 — Qi'anxin OSS Security —

安全测试 = DAST（主机漏扫、web漏扫）+ MAST + SAST + IAST

漏洞来源： 三方组件 + 安全测试 + 容器安全 + 渗透测试 + 威胁情报…

漏洞敏捷管理

- 敏捷安全漏洞问题汇总
- 敏捷安全漏洞管理实践

敏捷安全漏洞问题汇总

漏洞数量多

- 漏洞来源广，安全测试工具种类多
- 漏洞数量多，尤其是SAST、DAST环节
- 漏洞种类杂，从容器镜像到应用均涉及

漏洞难修复

- 缺少上层制度支撑漏洞的修复
- 系统发布上线速度快迭代频繁
- 漏洞数量多难以推动全部闭环

资产管理

- 无主资产数量多
- 资产平台数据同步不及时
- 资产属性不准确（APP/中间件/负责人）

漏洞数量多主要集中体现在测试阶段和检测阶段，然而在响应阶段依旧会发现“遗漏”的情况：

1、测试阶段漏洞案例：测试发现较多漏洞

2、检测阶段漏洞案例：扫描发现较多漏洞

3、响应阶段漏洞案例：未发现的安全漏洞

测试阶段漏洞案例：源代码安全漏洞

项目信息：开发语言为PHP，代码总行数为234.19万行

奇安信代码卫士发现：高危漏洞31971个，中危漏洞12021个，低危漏洞7598个（共为：51590个）

奇安信代码卫士 — Qi'anxin Codesafe —

首页 | 快速检测 | 项目管理 | 报告管理 | 统计分析 | 系统管理

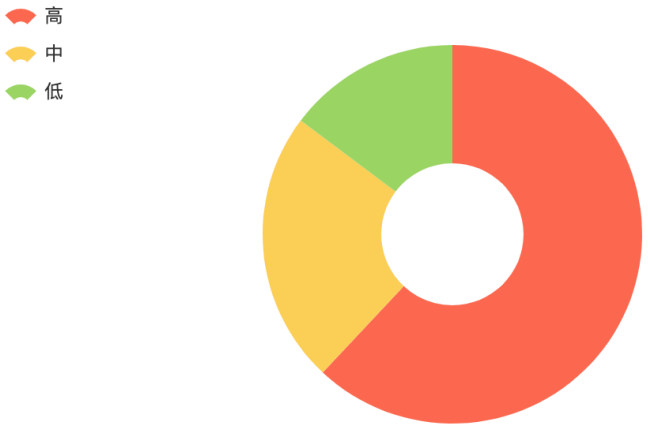
当前用户：admin

资源下载

源代码类型信息

.php	152.39 万行
.js	66.03 万行
.html	8.90 万行
.htm	4.84 万行
.xml	8863 行
.sql	7973 行
.java	1375 行
.c	530 行
.py	487 行
.cfc	232 行
.inc	228 行
.jsp	175 行
.h	156 行
.cfm	148 行
.properties	130 行

缺陷等级统计



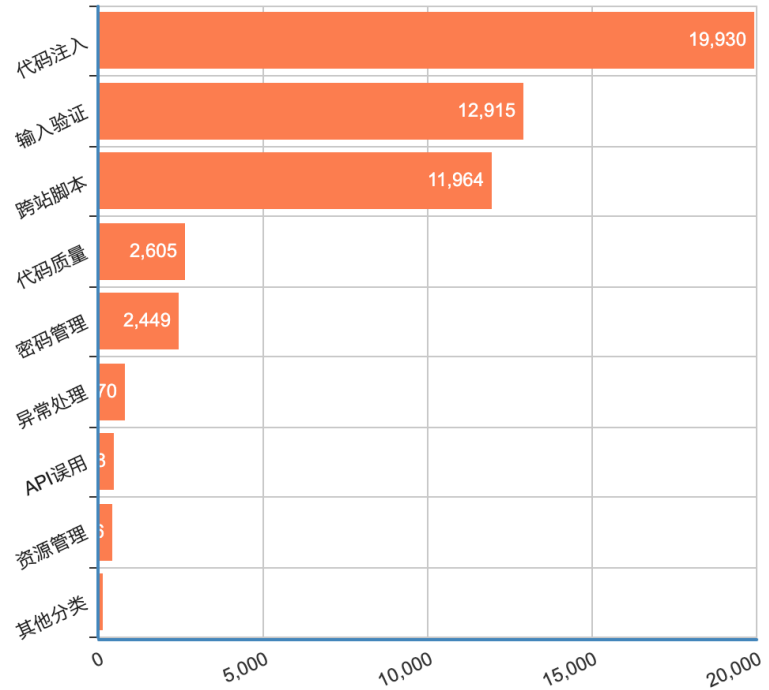
5.16 万 缺陷数

3.20 万 高危缺陷数

1.20 万 中危缺陷数

7598 低危缺陷数

缺陷分类统计



测试阶段漏洞案例：开源软件安全漏洞

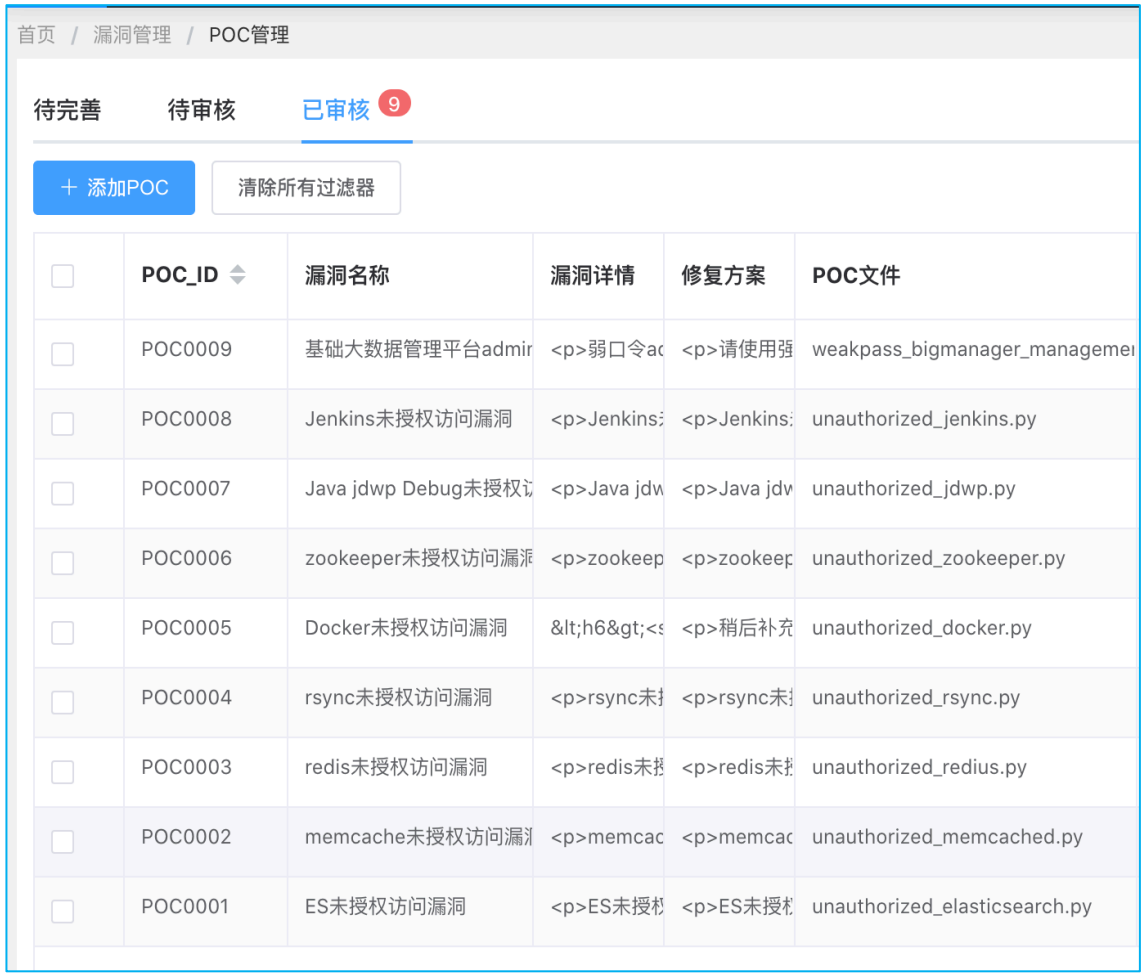
项目信息：开发语言为Java

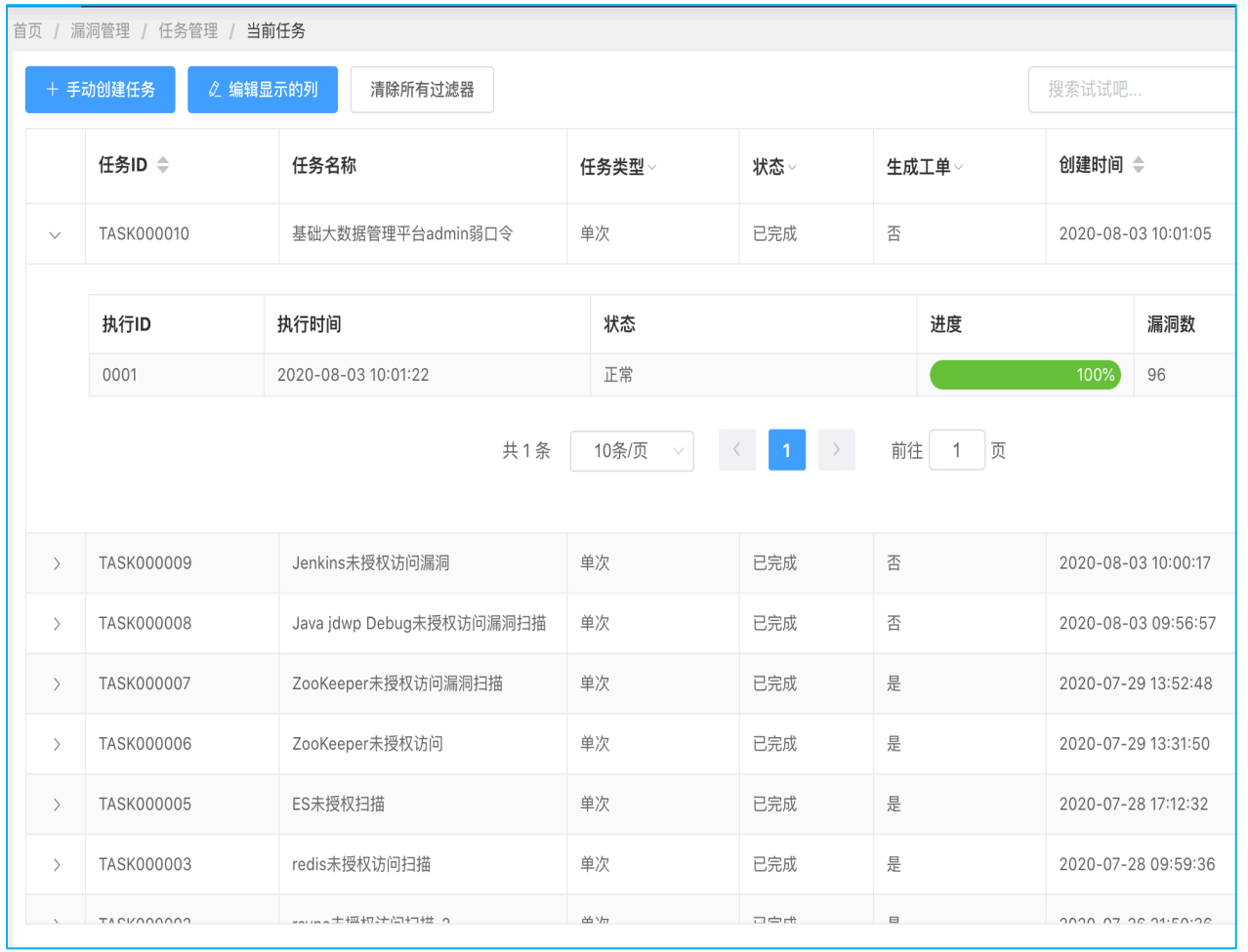
奇安信开源卫士发现：超危漏洞36个，高危漏洞30个，中危漏洞21个

检测阶段漏洞案例：扫描发现较多漏洞

场景描述：为保证主机及其它服务的安全性，进行日常漏洞扫描。

主机扫描：面对10万+的IP资产，从IP:PORT维度通过服务识别进行精准扫描，发现较多高危漏洞。

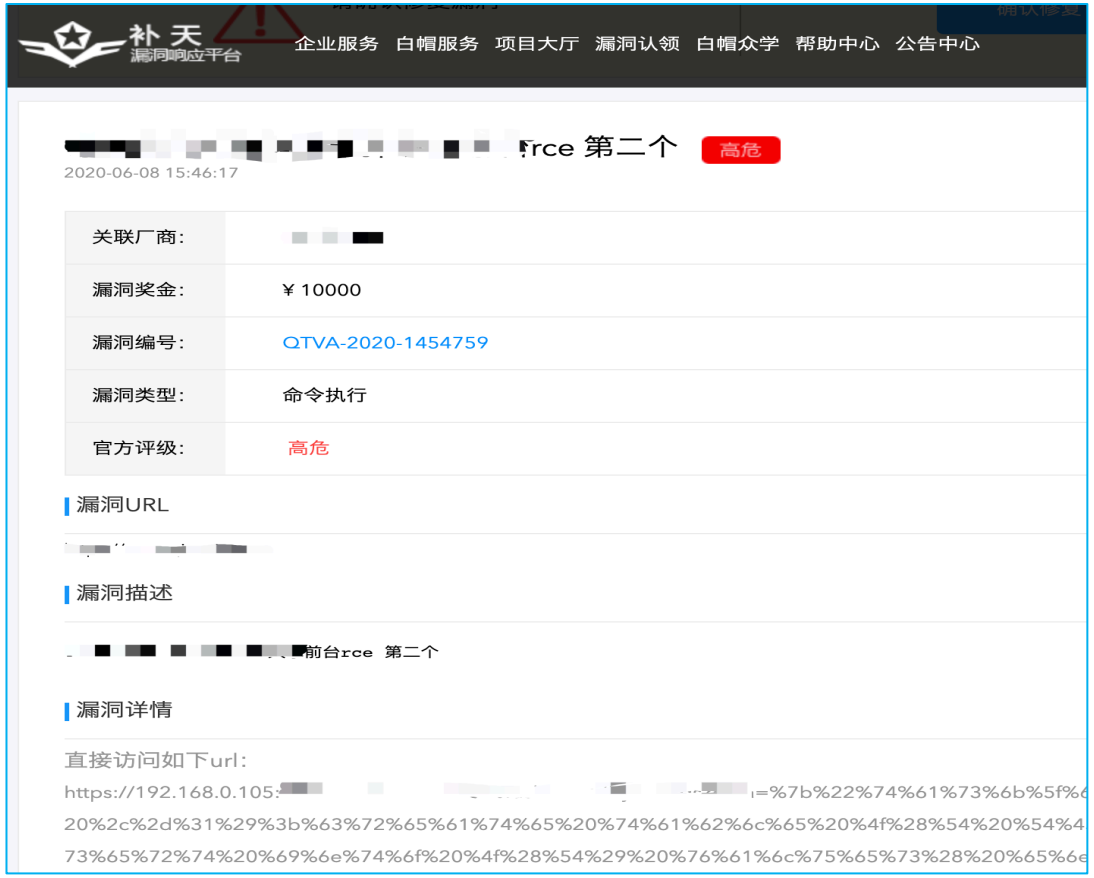


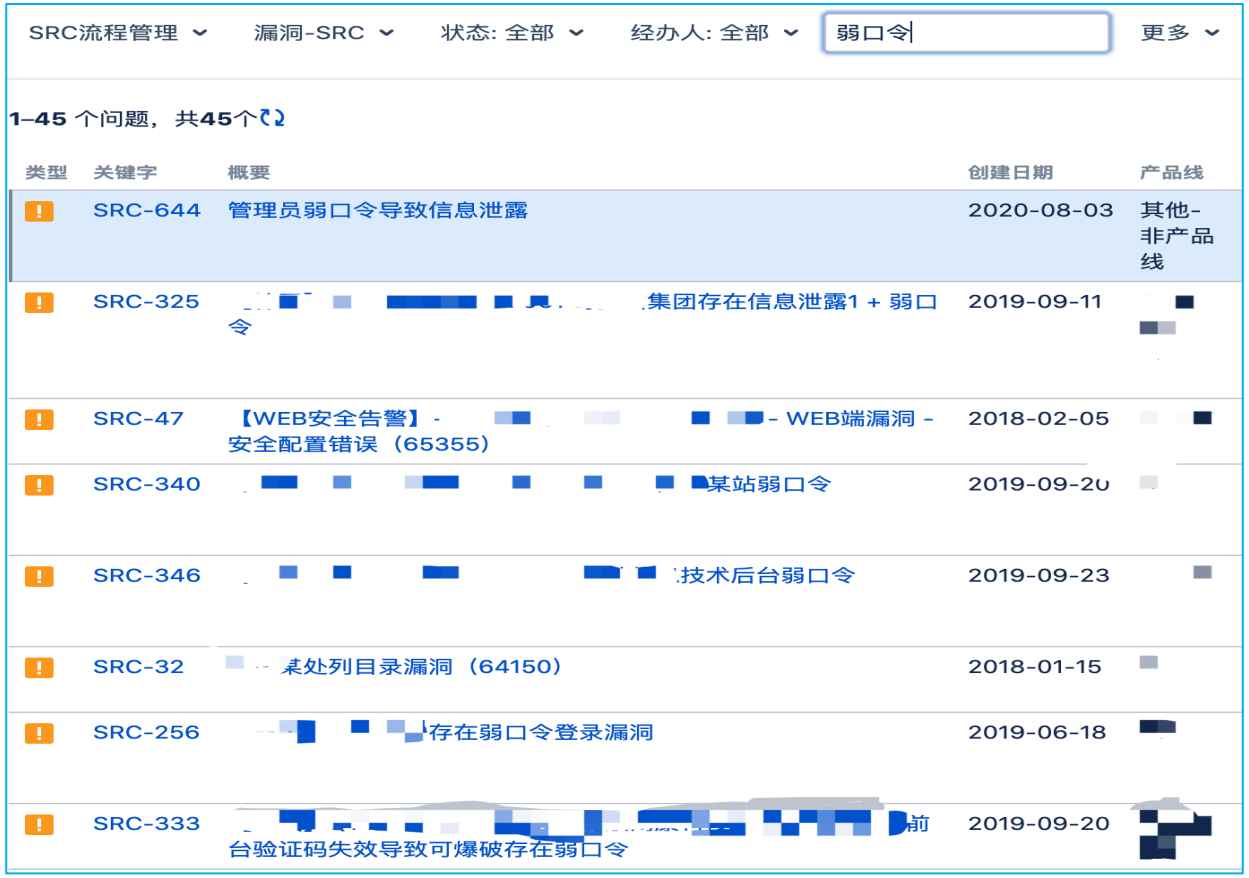


响应阶段漏洞案例：未发现的安全漏洞

漏洞来源：渗透测试 + SRC

原因分析：扫描器不支持postgresql注入扫描、测试环境未能覆盖到弱口令相关的安全测试





敏捷安全漏洞管理实践

管理原则：持续优化检测规则，提升“高可用”漏洞发现和漏洞修复能力，实现漏洞收敛闭环。

一、建制度、策略、系统，加强**漏洞修复**能力：

- **公司管理制度制定**：规范漏洞管理、明确职责分工、制定奖惩机制
- **漏洞分级抓大放小**：高危必修+资产属性，筛选高危中的危险漏洞，实现精细化管理
- **线上漏洞跟进处置**：安全资产平台漏洞导入、高危必修清单、对接安全测试API、漏洞工单

二、关注漏洞预防工作**源头解决**漏洞：

- **应用系统**：安全编码，第三方开源组件
- **操作系统及服务**：安全配置规范，主机安全加固
- **供应链安全管理**：外购第三方系统安全质量要求

三、通过自研POC，完善漏扫高危必修**漏洞发现**能力：

- **弱口令类**：服务器带外管理及其他web系统
- **高危必修漏洞**：包括最新漏洞情报和扫描模板

四、在实际应用中，**人工优化**各类扫描工具检测规则：

- SAST检测规则精简
- IAST检测规则增加
- **漏洞聚合，关联分析**

运营反馈，精简规则

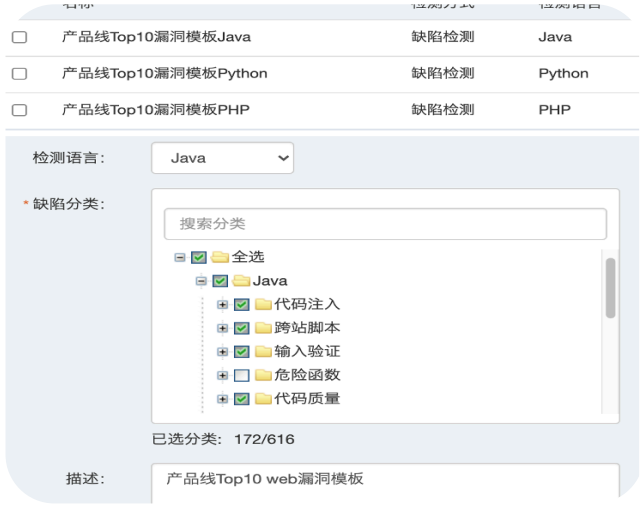
SAST规则优化：汇总分析所有渗透测试 + SRC收到的漏洞，总结输出内部Top 10，内化为检测规则

奇安信代码卫士 — Qi'anxin Codesafe —

首页　快速检测　项目管理　报告管理　统计分析　系统管理

默认规则

除去非安全相关为524条



Top 10

检测规则为172条

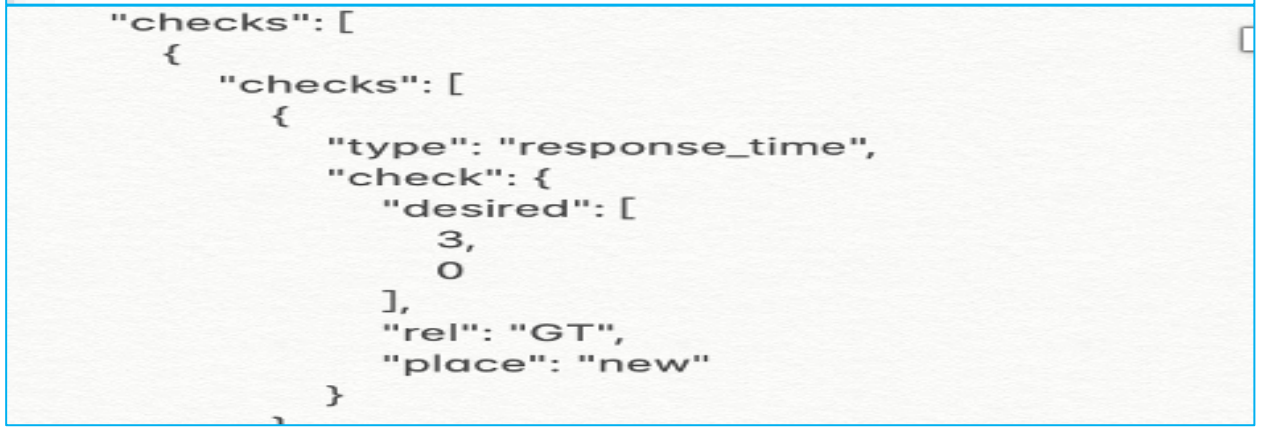
安全要求

仅关注并修复高危漏洞 23

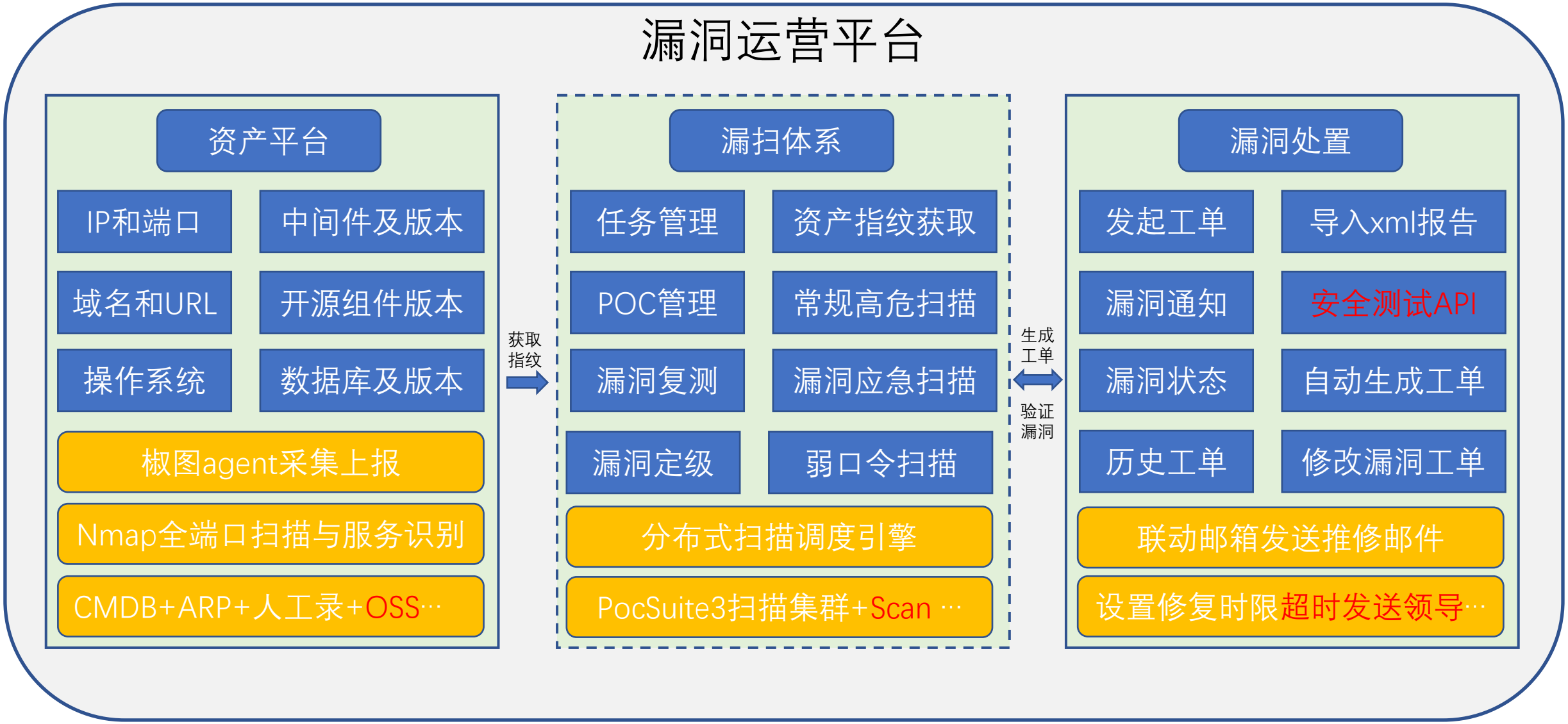
运营反馈，丰富规则

IAST规则优化：在渗透测试与SRC收到的漏洞中，发现有一类需要特殊闭合的postgresql注入存在，需要手工安全测试发现。通过在IAST工具中针对性自定义检测规则，实现自动化检测。

Payload：'));select pg_sleep(5);--



漏洞聚合，关联分析


漏洞运营平台
资产平台
IP和端口
中间件及版本
域名和URL
开源组件版本
操作系统
数据库及版本
椒图agent采集上报
Nmap全端口扫描与服务识别
CMDB+ARP+人工录+OSS…
获取指纹
漏扫体系
任务管理
资产指纹获取
POC管理
常规高危扫描
漏洞复测
漏洞应急扫描
漏洞定级
弱口令扫描
分布式扫描调度引擎
PocSuite3扫描集群+Scan …
生成工单
验证漏洞
漏洞处置
发起工单
导入xml报告
漏洞通知
安全测试API
漏洞状态
自动生成工单
历史工单
修改漏洞工单
联动邮箱发送推修邮件
设置修复时限超时发送领导…

新一代企网络安全架构

十工：

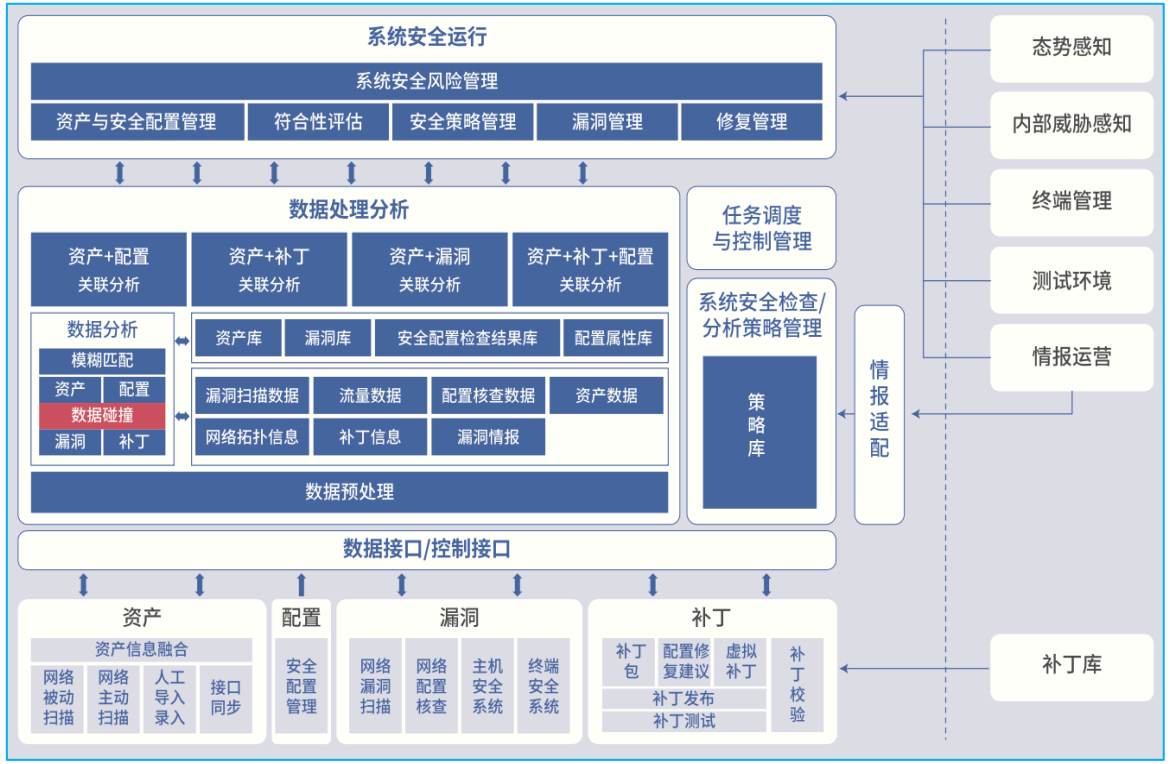
工程七：面向资产/漏洞/配置/补丁的系统安全

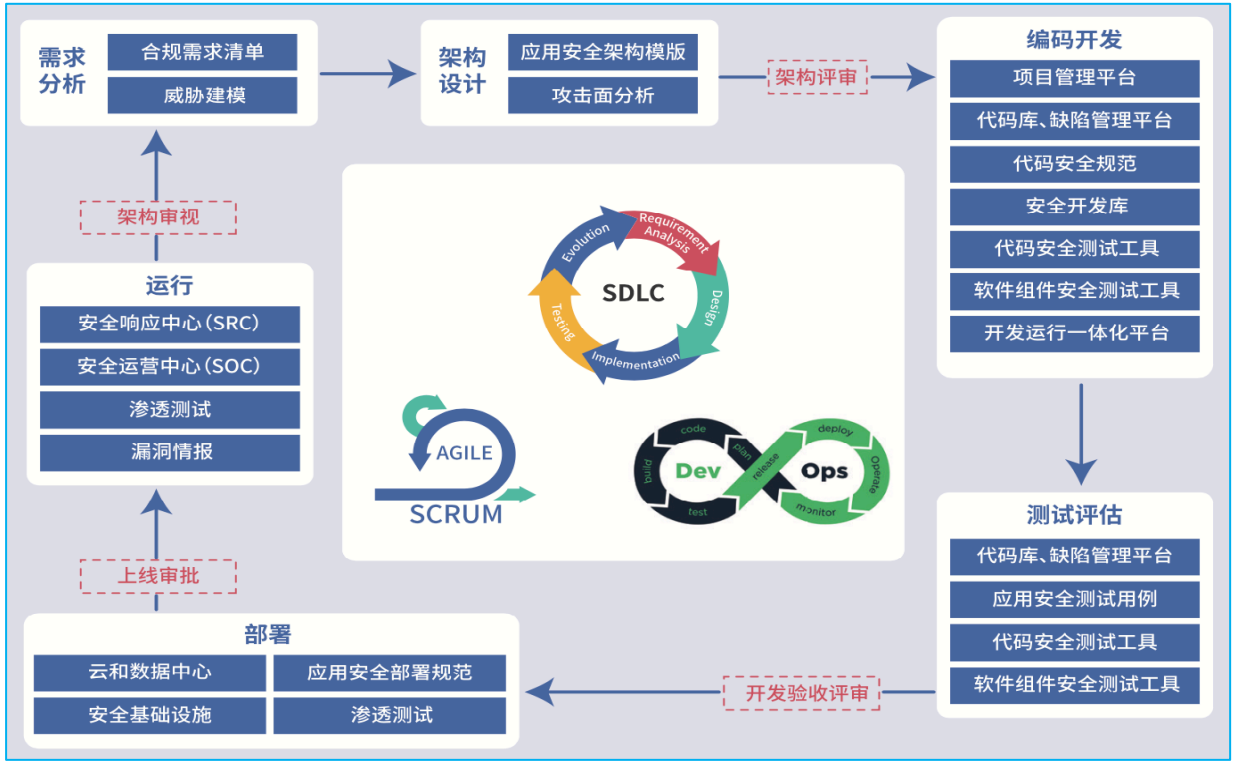
构建漏洞管理提体系和漏洞缓解体系

五任：

任务二：应用安全能力支撑

围绕软件开发生命周期，建立漏洞评估和修复体系






2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音