



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

从漏洞视角看敏捷安全



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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：我的安全世界观

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

DATA SECURITY

IoT CLOUD

HUMAN PROGRESS

TECHNOLOGY

文化：开发运维安全，责任共担



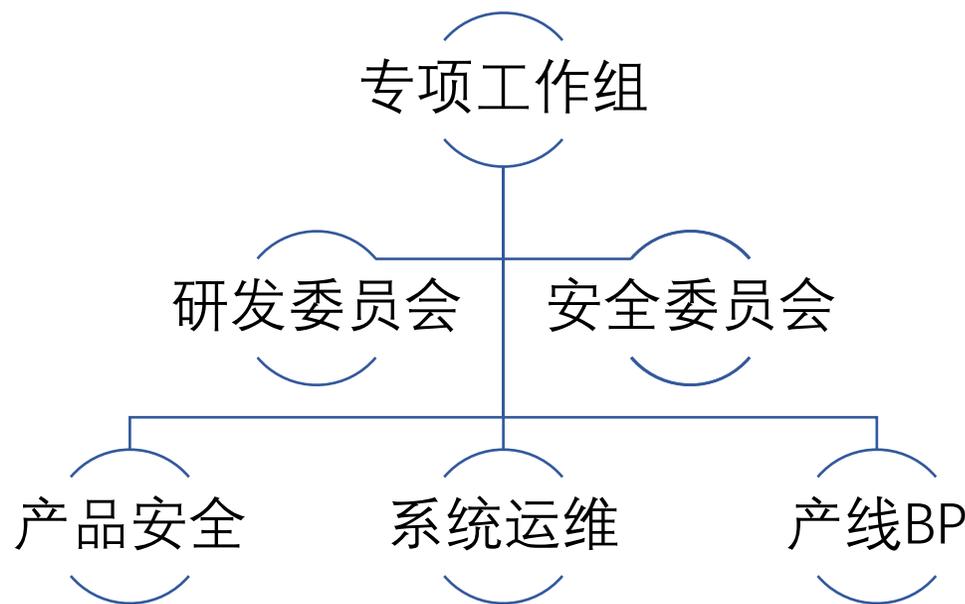
2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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

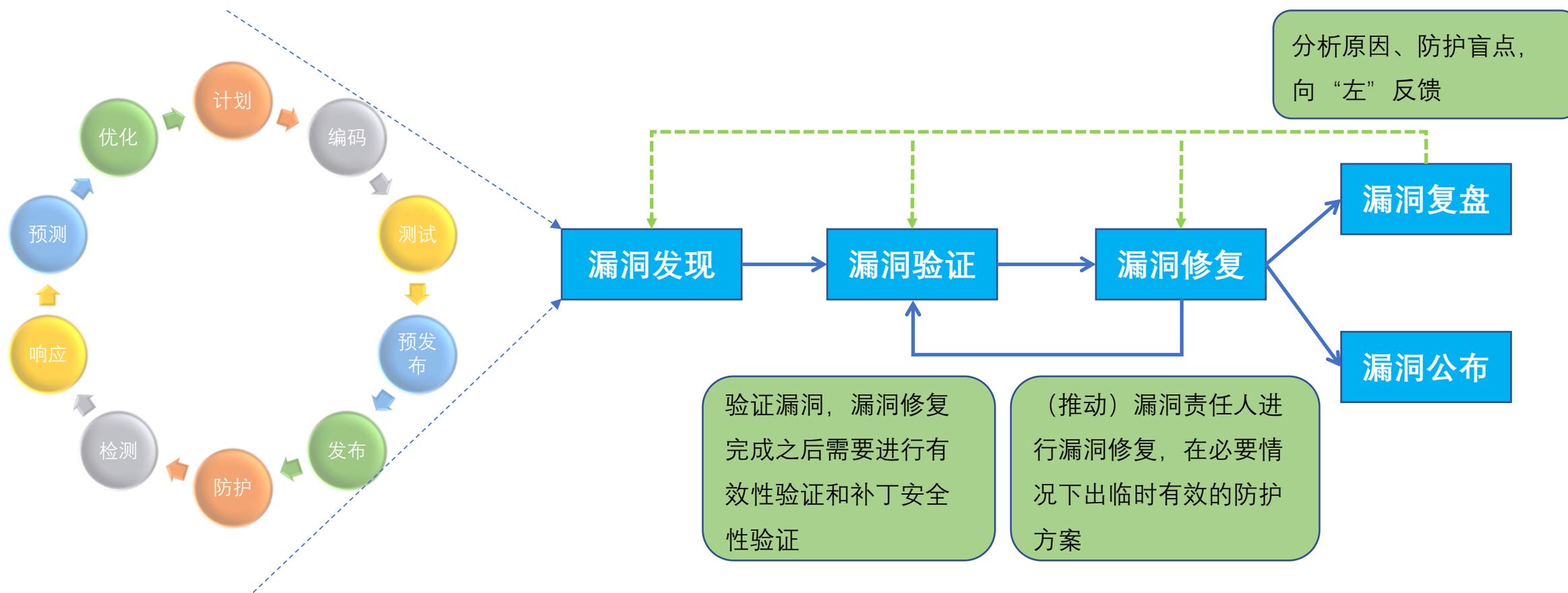


流程：安全左移，层层主动检测



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



- | ● 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 —



网神SecVSS 3600 漏洞扫描系统 V3.0



长鉴

移动应用安全检测系统

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

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



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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）



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

- 高
- 中
- 低



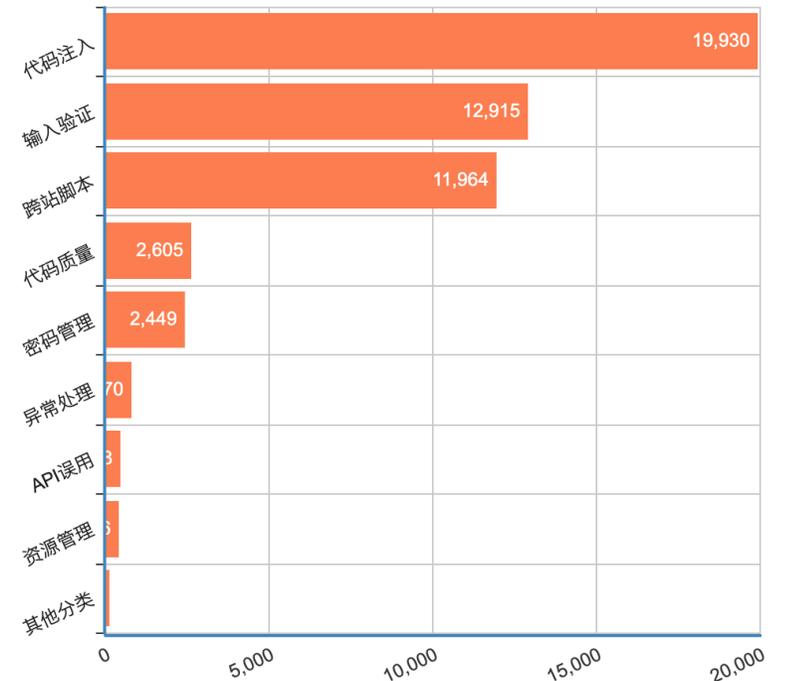
5.16 万
缺陷数

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



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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

The screenshot displays the '奇安信开源卫士' (Qianxin OSS Security) interface. The main content area shows the analysis results for a project named 'SSS'. The interface includes a navigation menu on the left, a top navigation bar, and a main content area with several charts and data tables.

奇安信开源卫士 — Qianxin OSS Security —

首页 项目管理 组件管理 漏洞列表 协议列表 统计报表 私服安全

txg01@code...

项目管理 / ssss / 成分分析 / sss

SSS
txg01@codesafe.cn 创建于2020-07-29 10:43:28 完成于2020-07-29 10:44:17 本地: cve-2017-5638-master.zip

生成Excel报告 生成Word报告

结果概览 组件详情 组件来源 漏洞信息 许可协议

组件等级分布
各个等级的组件数量分布

超危组件	6个
高危组件	3个
无漏洞组件	14个

许可协议组件统计
使用许可协议的组件统计

Apache-2.0	14
EPL-1.0	2
MIT	1
Public-...	1
MPL-1.1	1
BSD-3-C...	1
LGPL-2....	1

漏洞等级分布
各个等级的漏洞数量分布

超危漏洞	36
高危漏洞	30
中危漏洞	21
低危漏洞	1
未知风险	6

导出任务组件 批量操作 请选择管控状态 请选择标记状态 请选择组件类型 请选择组件等级 请输入组件名称进行查询 查询

检测阶段漏洞案例：扫描发现较多漏洞



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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。

首页 / 漏洞管理 / POC管理

待完善 待审核 **已审核 9**

+ 添加POC 清除所有过滤器

<input type="checkbox"/>	POC_ID	漏洞名称	漏洞详情	修复方案	POC文件
<input type="checkbox"/>	POC0009	基础大数据管理平台admin弱口令	<p>弱口令ac	<p>请使用强	weakpass_bigmanager_managemel
<input type="checkbox"/>	POC0008	Jenkins未授权访问漏洞	<p>Jenkins:	<p>Jenkins:	unauthorized_jenkins.py
<input type="checkbox"/>	POC0007	Java jdwp Debug未授权访问	<p>Java jdwp	<p>Java jdwp	unauthorized_jdwp.py
<input type="checkbox"/>	POC0006	zookeeper未授权访问漏洞	<p>zookeep	<p>zookeep	unauthorized_zookeeper.py
<input type="checkbox"/>	POC0005	Docker未授权访问漏洞	<h6><le	<p>稍后补充	unauthorized_docker.py
<input type="checkbox"/>	POC0004	rsync未授权访问漏洞	<p>rsync未	<p>rsync未	unauthorized_rsync.py
<input type="checkbox"/>	POC0003	redis未授权访问漏洞	<p>redis未	<p>redis未	unauthorized_re dius.py
<input type="checkbox"/>	POC0002	memcache未授权访问漏洞	<p>memcac	<p>memcac	unauthorized_memcached.py
<input type="checkbox"/>	POC0001	ES未授权访问漏洞	<p>ES未授	<p>ES未授	unauthorized_elasticsearch.py

首页 / 漏洞管理 / 任务管理 / 当前任务

+ 手动创建任务 编辑显示的列 清除所有过滤器 搜索试试吧...

任务ID	任务名称	任务类型	状态	生成工单	创建时间
TASK000010	基础大数据管理平台admin弱口令	单次	已完成	否	2020-08-03 10:01:05
执行ID		执行时间	状态	进度	漏洞数
0001		2020-08-03 10:01:22	正常	100%	96

共 1 条 10条/页 1 前往 1 页

TASK000009	Jenkins未授权访问漏洞	单次	已完成	否	2020-08-03 10:00:17
TASK000008	Java jdwp Debug未授权访问漏洞扫描	单次	已完成	否	2020-08-03 09:56:57
TASK000007	ZooKeeper未授权访问漏洞扫描	单次	已完成	是	2020-07-29 13:52:48
TASK000006	ZooKeeper未授权访问	单次	已完成	是	2020-07-29 13:31:50
TASK000005	ES未授权扫描	单次	已完成	是	2020-07-28 17:12:32
TASK000003	redis未授权访问扫描	单次	已完成	是	2020-07-28 09:59:36

响应阶段漏洞案例：未发现的安全漏洞



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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



补天漏洞响应平台

企业服务 白帽服务 项目大厅 漏洞认领 白帽众学 帮助中心 公告中心

2020-06-08 15:46:17

关联厂商: [redacted]

漏洞奖金: ¥ 10000

漏洞编号: QTVA-2020-1454759

漏洞类型: 命令执行

官方评级: 高危

漏洞URL: [redacted]

漏洞描述: [redacted] 前台rce 第二个

漏洞详情: 直接访问如下url: https://192.168.0.105: [redacted]



SRC流程管理 漏洞-SRC 状态: 全部 经办人: 全部 弱口令 更多

1-45 个问题, 共45个

类型	关键字	概要	创建日期	产品线
!	SRC-644	管理员弱口令导致信息泄露	2020-08-03	其他-非产品线
!	SRC-325	[redacted] 集团存在信息泄露1 + 弱口令	2019-09-11	[redacted]
!	SRC-47	【WEB安全告警】 - 安全配置错误 (65355)	2018-02-05	[redacted]
!	SRC-340	[redacted] 某站弱口令	2019-09-20	[redacted]
!	SRC-346	[redacted] 技术后台弱口令	2019-09-23	[redacted]
!	SRC-32	[redacted] 某处列目录漏洞 (64150)	2018-01-15	[redacted]
!	SRC-256	[redacted] 存在弱口令登录漏洞	2019-06-18	[redacted]
!	SRC-333	[redacted] 前台验证码失效导致可爆破存在弱口令	2019-09-20	[redacted]

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

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**

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

运营反馈，精简规则



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

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



首页

快速检测

项目管理

报告管理

统计分析

系统管理

Java

搜索分类

- Java
 - 代码注入
 - 跨站脚本
 - 输入验证
 - 危险函数
 - 代码质量
 - API误用

已选分类: 524/616



产品线Top10漏洞模板Java 缺陷检测 Java

产品线Top10漏洞模板Python 缺陷检测 Python

产品线Top10漏洞模板PHP 缺陷检测 PHP

检测语言: Java

缺陷分类:

搜索分类

- 全选
 - Java
 - 代码注入
 - 跨站脚本
 - 输入验证
 - 危险函数
 - 代码质量

已选分类: 172/616

描述: 产品线Top10 web漏洞模板



高	中	低	所有
23	229	1418	1670

- 代码注入(5)
- 命令注入(5)
- 输入验证(18)
- 路径遍历(18)

高	中	低	所有
23	229	1418	1670

- 代码注入(6)
- 资源注入(6)
- 密码管理(19)
- 输入验证(25)
- 代码质量(20)

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

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);--

规则名称: postges SQL 注入 () * 检测漏洞类型: SQL注入 * 检测漏洞

规则类型: 扫目录 扫文件 独立特定请求

规则精度: 只扫URL GET参数 POST通用参数 POST文件上传参数 HEADER COOKII

规则模板示例:

```
    }
  }
},
"filters": []
},
{
  "checks": [
    {
      "type": "content",
      "check": {
        "place": "body",
        "desired": false,
        "type": "bool"
      }
    }
  ]
}
```

新增规则:

```
{
  "payloads": [
    {
      "prefix": [
        ""
      ],
      "payload": "'');select pg_sleep(5);--",
      "suffix": [
        ""
      ]
    }
  ]
}
```

规则配置

搜索: 搜索规则名称/创建人 搜索

等级: 全部 高危 中危 低危 信息 状态: 全部 开 关 类型: 全部

规则名称	规则类型	规则状态	风险等级	更新时间
postges SQL 注入 ()	SQL注入	<input checked="" type="checkbox"/>	高危	2020-06-03 11:07:08
SQL注入字符型疑似判断-1	SQL注入	<input checked="" type="checkbox"/>	高危	2020-06-03 11:40:02
SQL注入字符型疑似判断-2	SQL注入	<input checked="" type="checkbox"/>	高危	2020-06-03 14:23:12

```
"checks": [
  {
    "checks": [
      {
        "type": "response_time",
        "check": {
          "desired": [
            3,
            0
          ],
          "rel": "GT",
          "place": "new"
        }
      }
    ]
  }
]
```

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...

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...

获取
指纹
→

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

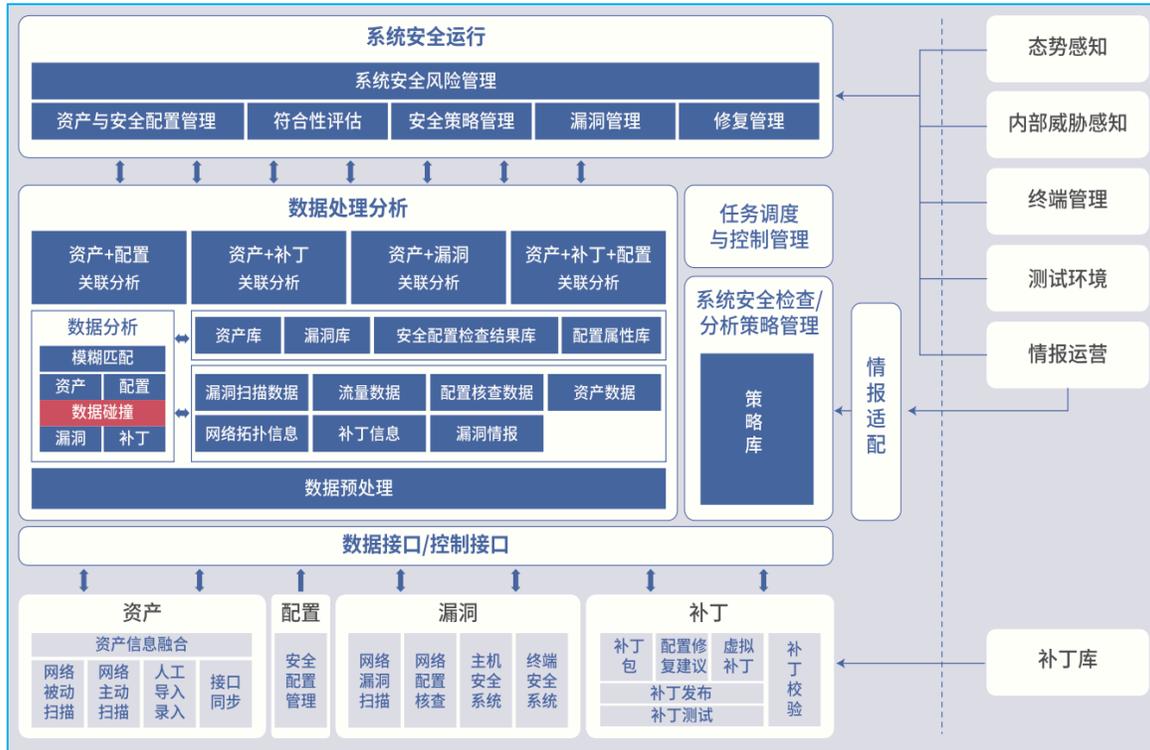
修改漏洞工单

联动邮箱发送推修邮件

设置修复时限 超时发送领导...

十工：

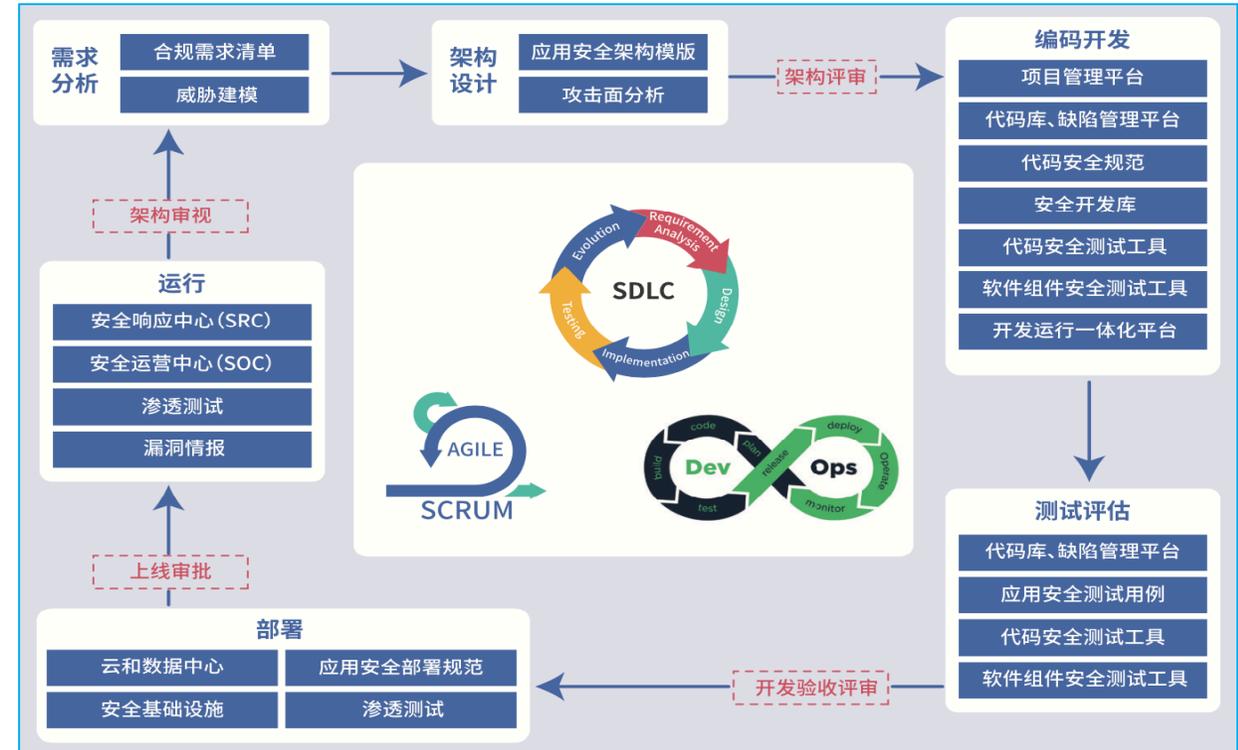
工程七：面向资产/漏洞/配置/补丁的系统安全
构建漏洞管理提体系和漏洞缓解体系



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