默安科技
企业信赖的安全伙伴

霁鉴

默安DevSecOps落地实践

How to integrate security with DevOpS

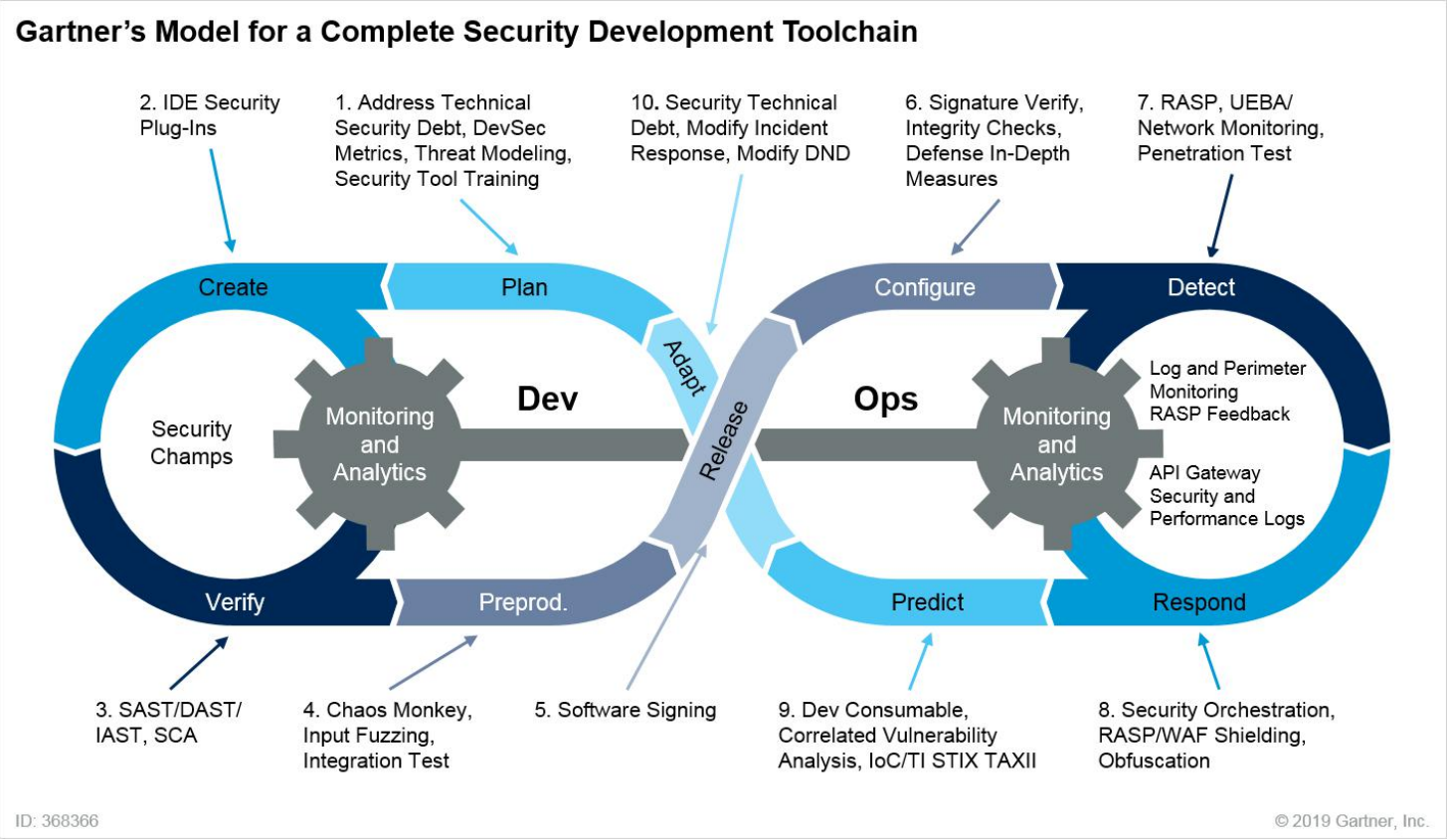
默安科技产品部

2020-03

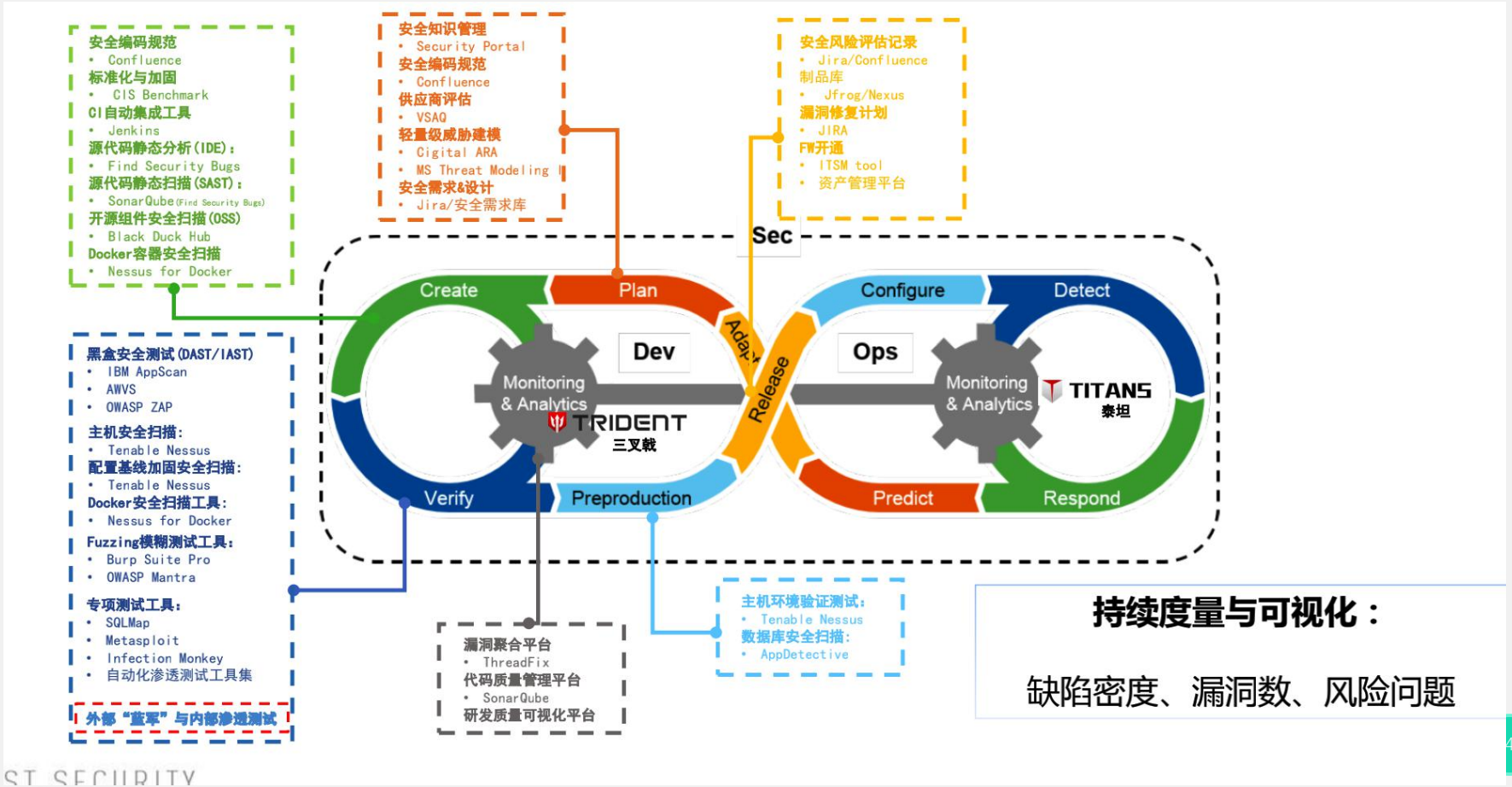
默安科技
企业信赖的安全伙伴

雳鉴软件开发安全解决方案

1-1 Gartner DevSecOps安全开发工具链模型



1-2 华泰证券DevSecOps落地实践



默安科技
企业信赖的安全伙伴

霁鉴软件开发安全解决方案

01 DevSecOps最佳实践探索

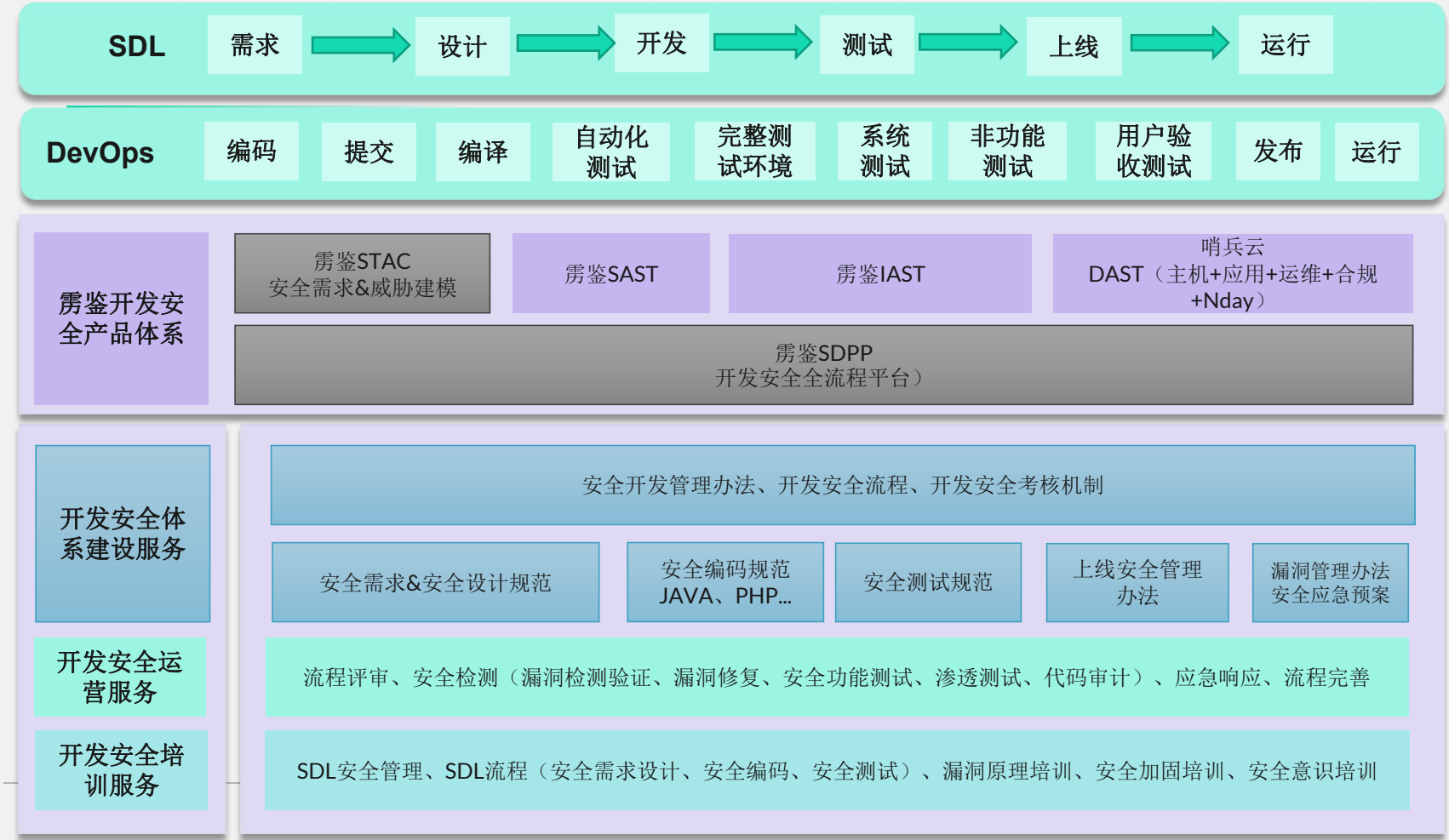
02 默安DevSecOps体系

03 落地实践案例

04 DevSecOps领域的新方向

2.1 默安DevSecOps产品与服务体系

默安科技
企业信赖的安全伙伴



2-2 默安DevSecOps工具链集成模型

默安科技
企业信赖的安全伙伴

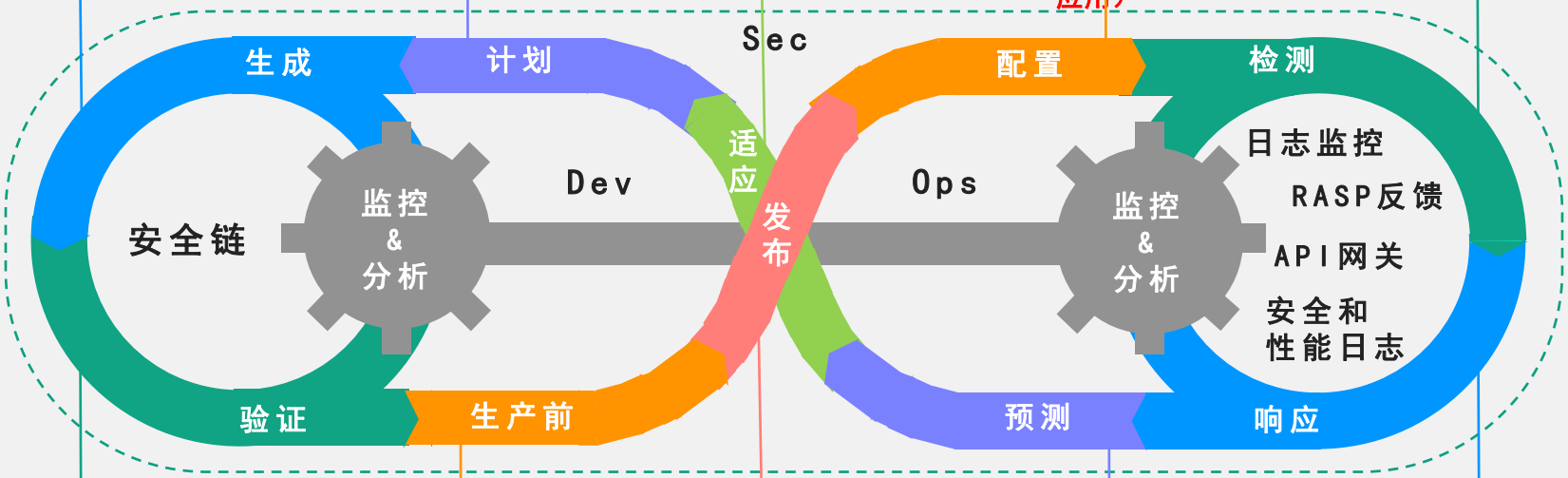
- IDE安全插件
- 代码仓库实时监控扫描（雳鉴SAST）

- 安全培训服务
- 安全编码规范
- 安全测试规范
- 威胁建模服务
- 安全需求&设计方案

- 安全方案评估
- 工具策略优化
- 应急响应优化

- 签名验证
- 完整性验证
- 纵深防御措施部署（主机+网络+应用）

- RASP，UEBA
- 流量监控
- 渗透测试



- 雳鉴SAST：SAST+SCA能力
- 雳鉴IAST：IAST+DAST+SCA能力
- Docker安全检测服务

- 主机安全测试
- 安全基线核查
- 集成测试（人工渗透）
- 混沌工程
- Fuzz测试

- 软件签名

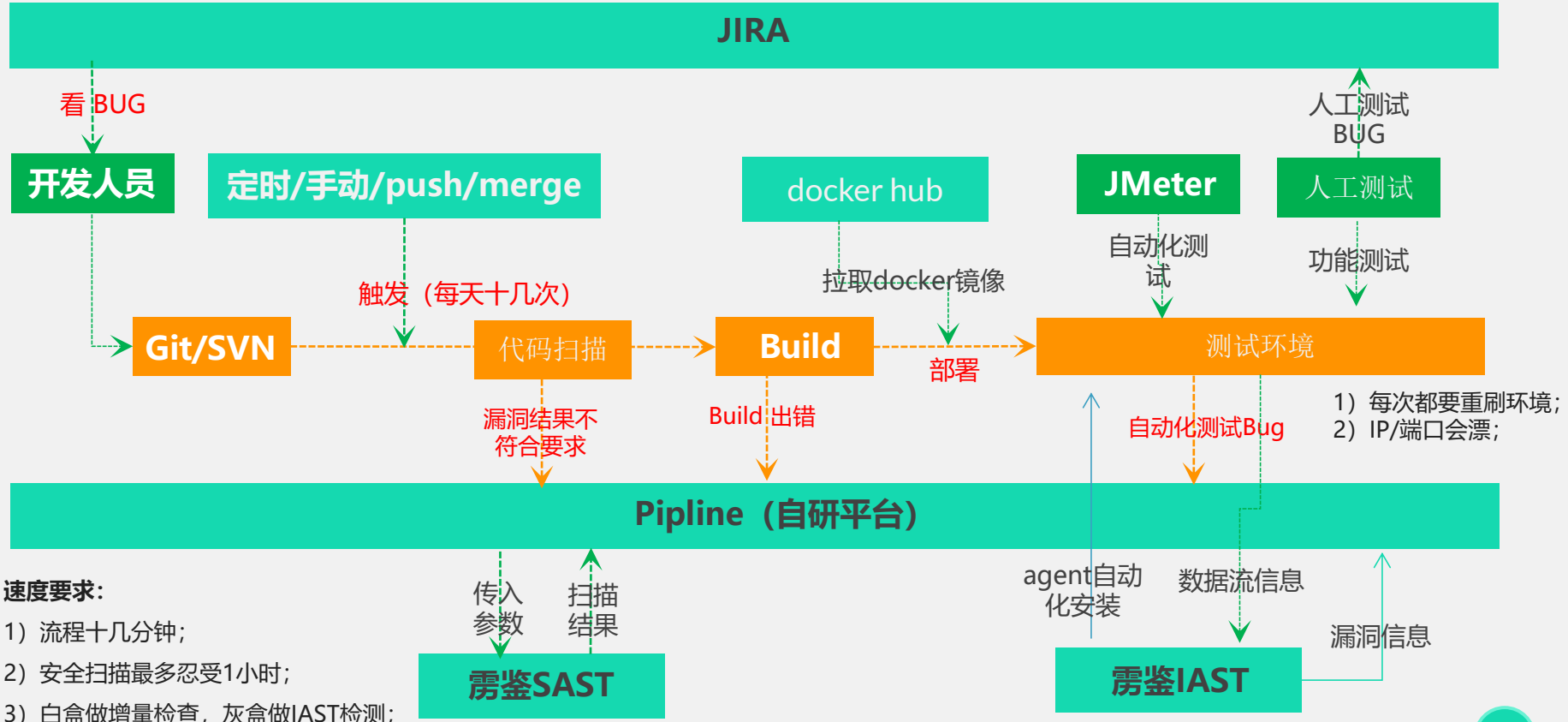
- 漏洞情报（应急漏扫插件，服务）
- 威胁情报（TTP）

- RASP、WAF
- 安全编排
- 应急响应

默安科技
企业信赖的安全伙伴

霁鉴软件开发安全解决方案

1 某能源集团：DevSecOps流程落地



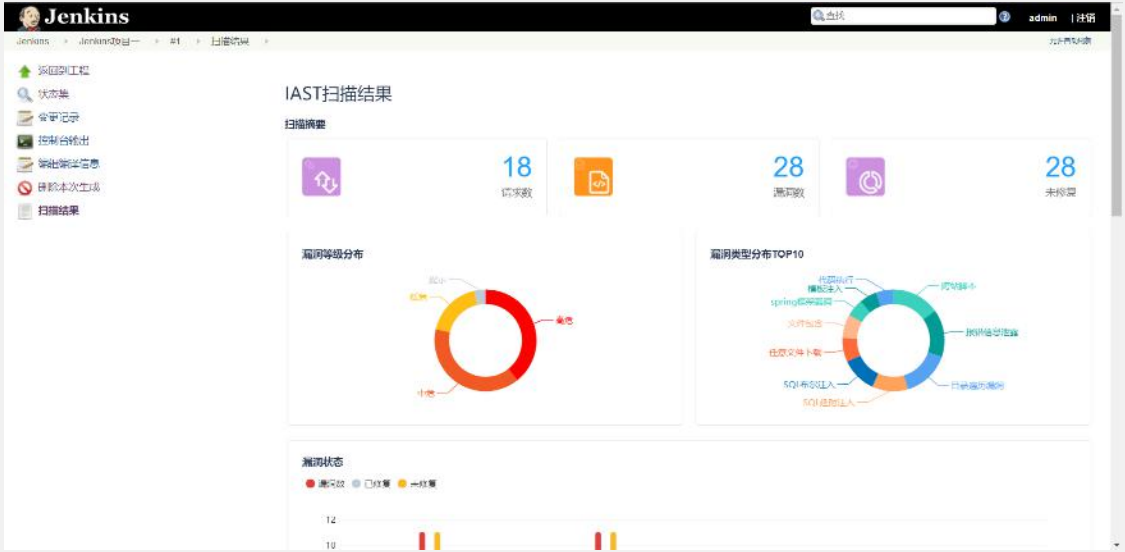
速度要求：

1）流程十几分钟；

2）安全扫描最多忍受1小时；

3）白盒做增量检查，灰盒做IAST检测；

2 DevSecOps集成-jenkins对接集成



1.Jenkins插件：

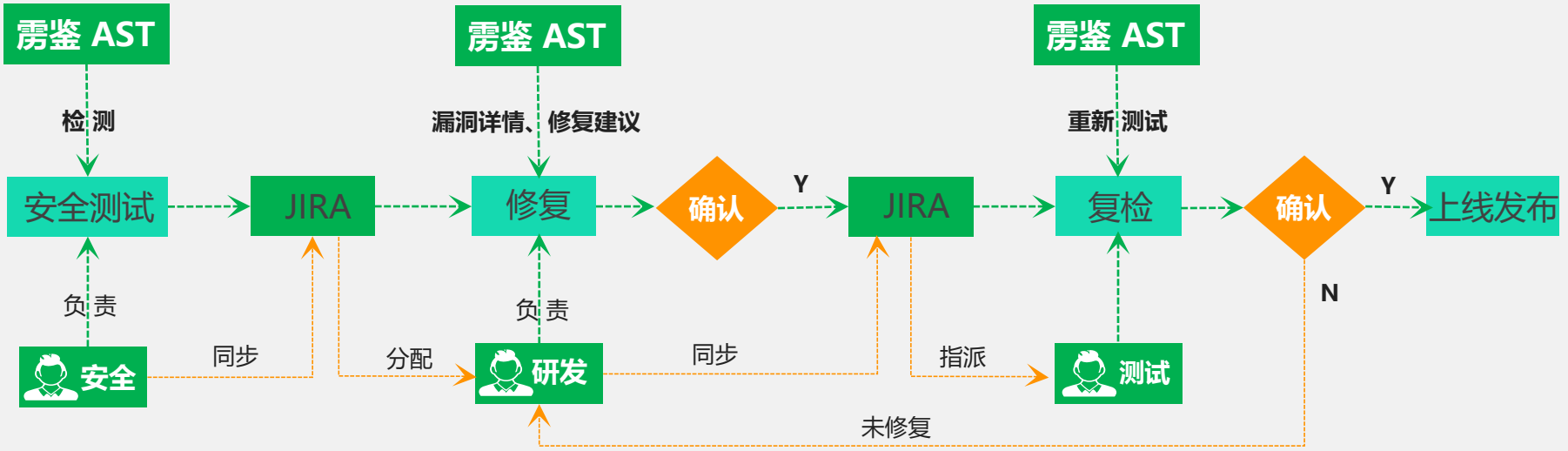
（1）用于自由风格和流水线模式
（2）将扫描结果展示到jenkins平台
（3）设置代码安全质量阈值，决定jenkins流程的是否中断

2.Jenkins pipeline辅助组件

（1）根据用户参数协助生成pipeline脚本
（2）提供二进制程序，一条命令创建项目发起扫描

```
stage('sec_test'){
 steps{
     LJ_pipe_agent create 'token' 'proj_name'
   }
}
```

3 DevSecOps集成-JIRA对接



1）使用到的工具： 雳鉴IAST（Y） 、雳鉴SAST（Y）

2）JIRA推动流程，如果研发不修复，流程停滞，会影响下一步上线发布

3）半自动化解决方案

默安科技
企业信赖的安全伙伴

霁鉴软件开发安全解决方案

01 DevSecOps最佳实践探索

02 默安DevSecOps体系

03 落地实践案例

04 DevSecOps领域的新方向

1 DevSecOps领域的一些新方向

01 安全需求与威胁建模平台

基于业务场景，对业务场景自动化进行威胁建模，分析业务的安全设计与实现的安全合理性。

02 漏洞自动化修复

漏洞最佳修复点识别，结合安全组件，推荐自动化修复方案，实现一键修复

03 AVC漏洞关联分析

将各个阶段漏洞集成，统一进行关联分析，定义漏洞合理的优先级，降低误报

04 ASTO安全测试编排

综合SAST/SCA/IAST/DAST各个安全检测能力，完善与开发工具链集成与自动化能力，提供安全能力编排方案，用户自定义编排安全检测手段，工具与其他安全产品的自动化集成响应

05 流程平台持续运营

通过**雳鉴SDPP**平台将各个阶段的安全活动与进度可视化展示，提取有价值的风险与项目开发信息，促进安全开发过程不断优化

THANK YOU