



默安DevSecOps落地实践

How to integrate security with DevOpS

默安科技产品部 2020-03







02 默安DevSecOps体系

雳鉴软件开发安全 解决方案

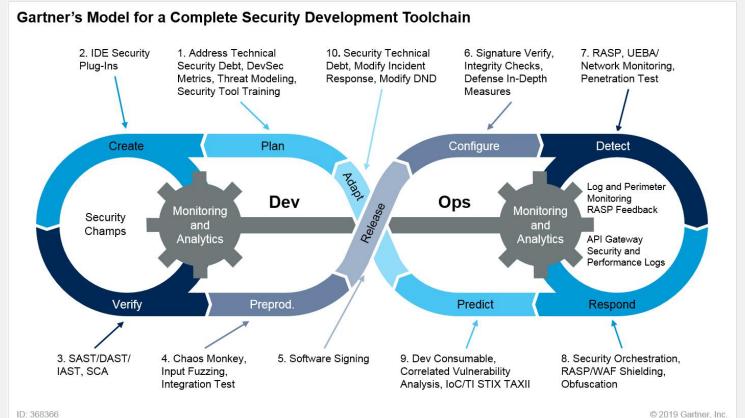


03 落地实践案例



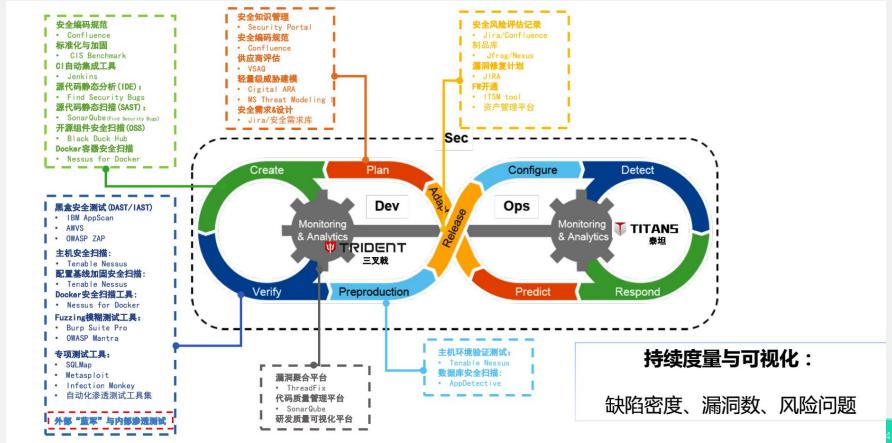


1-1 Gartner DevSecOps安全开发工具链模型





1-2 华泰证券DevSecOps落地实践









02 默安DevSec0ps体系

雳鉴软件开发安全 解决方案

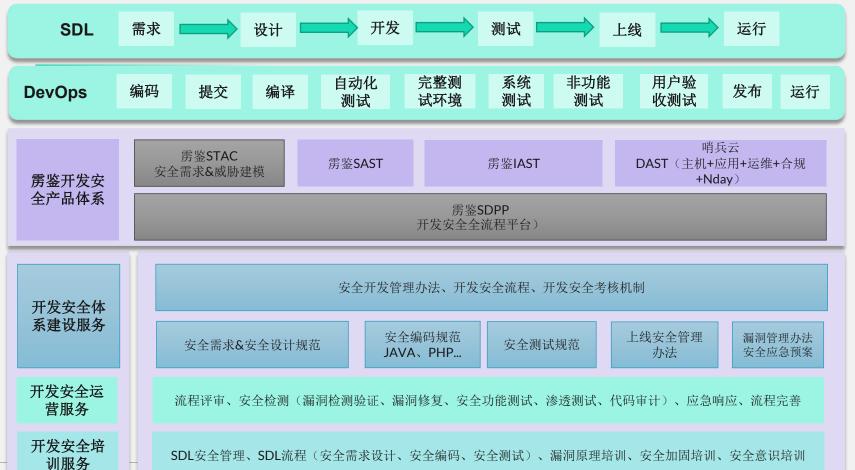


03 落地实践案例



2.1 默安DevSecOps产品与服务体系





2-2 默安DevSecOps工具链集成模型

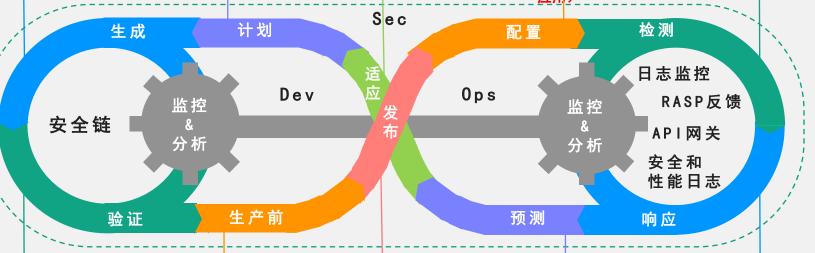


- · IDE安全插件
- · 代码仓库实时监控 扫描(雳鉴SAST)
- 安全培训服务
- 安全编码规范
- 威胁建模服务
- 安全需求&设计方案

- 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 カ
- · 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

领先的第三方云计算安全服务商







02 默安DevSecOps体系

雳鉴软件开发安全 解决方案

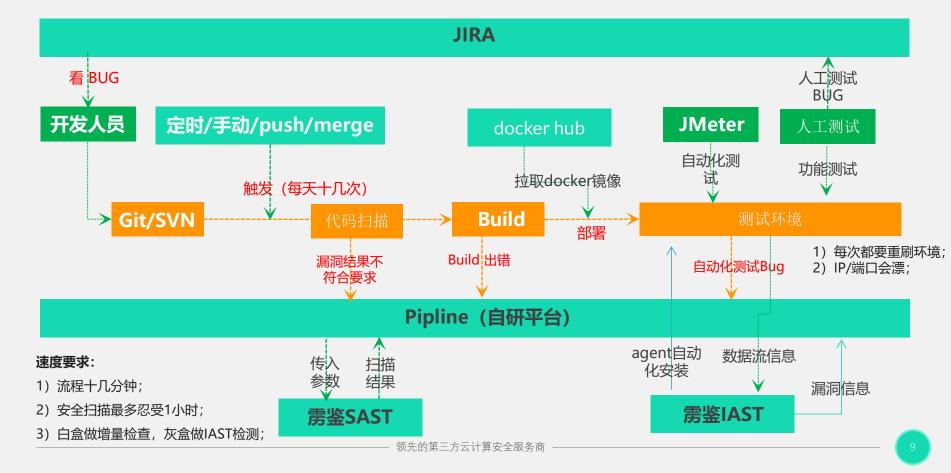


03 落地实践案例



1 某能源集团: DevSecOps流程落地





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

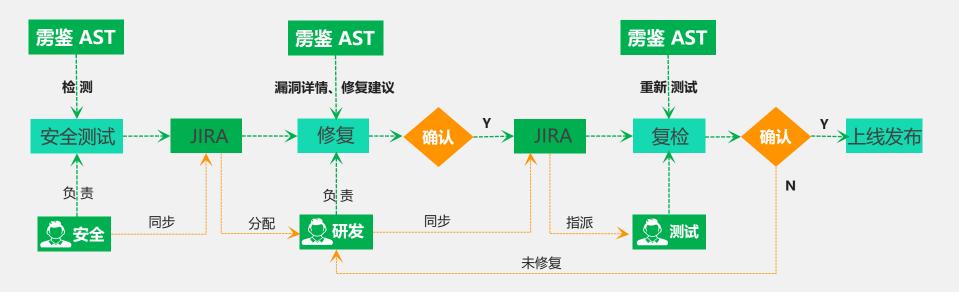
2.Jenkins pipeline辅助组件

- (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







02 默安DevSecOps体系

雳鉴软件开发安全 解决方案



03 落地实践案例



1 DevSecOps领域的一些新方向



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

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。



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



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

领先的第三方云计算安全服务商

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



THANK YOU