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

SDL与安全能力服务化

爱奇艺- 王超

SDL 1.0 瀑布流

Microsoft Security Development Lifecycle

http://www.microsoft.com/security/sdl/discover/default.aspx

产品抱怨

- 慢 – 时间太紧
- 重 – 环节太多
- 忙 – 人手不够

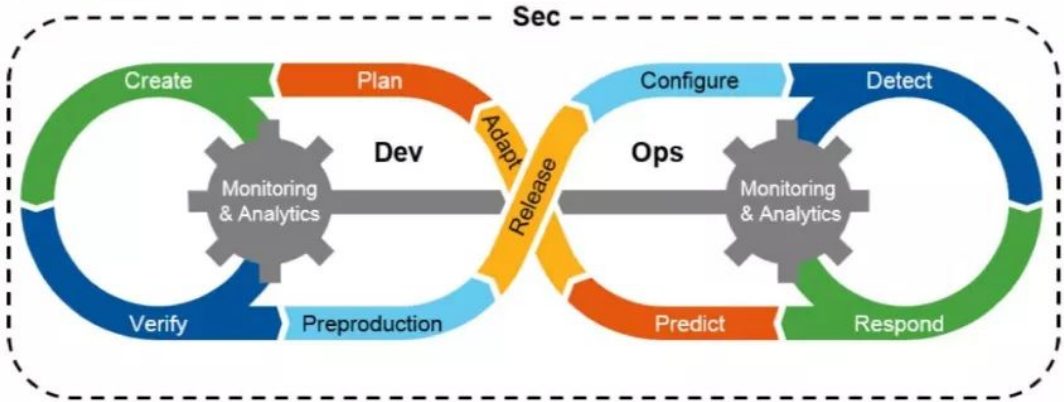
安全抱怨

- 开会，开会，开会
- 文档，文档
- 对方不懂安全

结果 累死

US $1,000,000

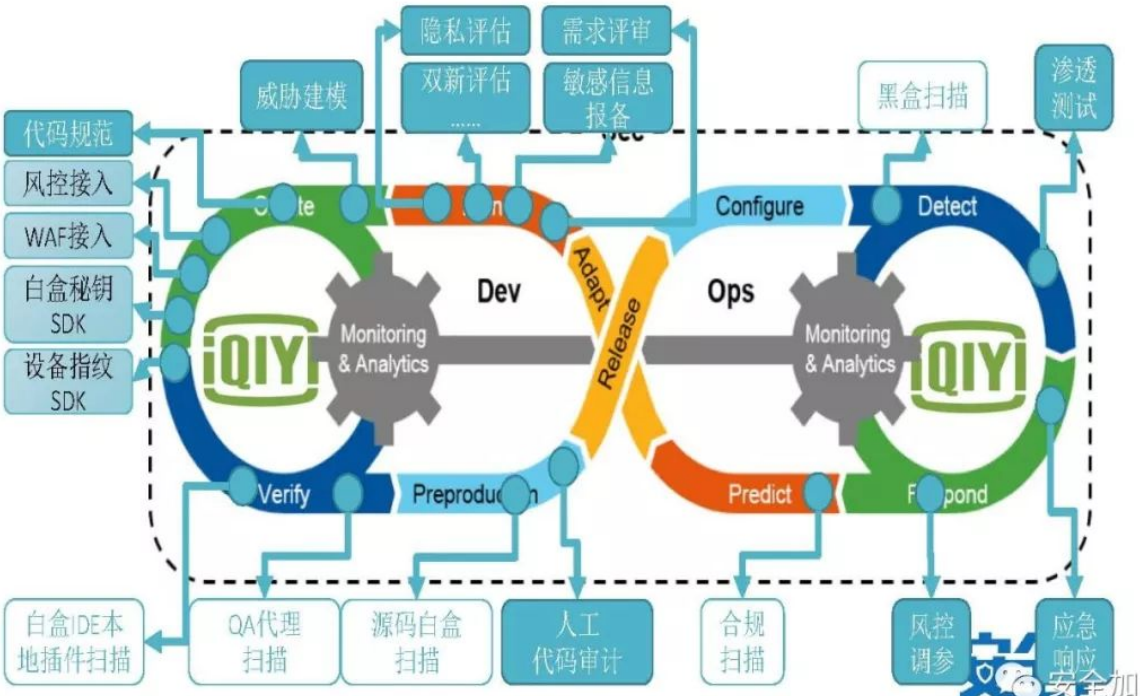
SDL 2.0


Sec
Create
Plan
Configure
Detect
Dev
Adapt
Release
Ops
Monitoring & Analytics
Monitoring & Analytics
Verify
Preproduction
Predict
Respond

$4700 → $360

✓自动化
✓效率

爱奇艺基于DevSecOps的SDL流程



安全能力服务化

效率 → 体验 → 数据运营

效率优先

✓人工流程标准化

效率优先

✓一次接入，永久收集

代码扫描

代码地址： 可输入关键字 搜索

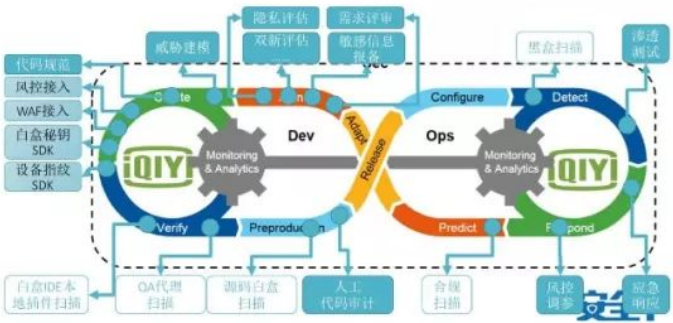
接入状态： 全部 已接入 未接入

代码地址	代码类型	接入状态	编译命令	url地址	操作
ssh://git@[redacted]_front_web.git	java	已接入	mvn clean package		接入 取消 配置
ssh://git@[redacted]-flink-job.git	java	已接入	mvn clean package		接入 取消 配置
ssh://git@[redacted]n_hids.git	java	已接入			接入 取消 配置
ssh://git@[redacted]-flink.git	java	已接入	mvn clean package		接入 取消 配置
ssh://git@[redacted]		未接入			接入 取消 配置

方便用户

✓灵活可选

✓不必面面俱到



可选服务

- [x] 需求评审安全加固服务
- [ ] 敏感信息流程
- [ ] 双新评估流程
- [x] 隐私评估流程
- [x] 代码检测(白盒扫描)
- [ ] 人工代码审计
- [ ] 安全扫描服务
- [x] 渗透测试服务
- [ ] WAF服务
- [x] 堡垒机服务
- [x] 风控系统

方便用户

- ✓白屏UI－方便小白
- ✓后台容器化－标准配置，减少兼容性bug
- ✓加固选项SDK接口化服务，降低沟通成本

数据化运营 – 三种能力指标

数据化运营

✓SDL 打通各流程

✓数据埋点：Who、When、How、MTTR

检查项	完成状态	处理人	评估结果	评估时间点	修复结果	修复时间点	项目得分
敏感信息流程	未开始	填写域账号	有0条评估意见	评估时间点	已完成0条	修复时间点	0
隐私评估流程	未开始	填写域账号	有0条评估意见	评估时间点	已完成0条	修复时间点	0
代码检测(白盒扫描)	进行中	填写域账号	应修复6个高危，130个中危，29个低危漏洞	2018-11-12 0(	已修复3个高危，81个中危，29个低危漏洞	2018-11-21 1(	6
安全扫描服务	未开始	填写域账号	应修复0个高危，0个中危，0个低危漏洞	评估时间点	已修复0个高危，0个中危，0个低危漏洞	修复时间点	0
渗透测试服务	进行中	填写域账号	应修复1个高危，8个中危，3个低危漏洞	2018-11-07 1(	已修复1个高危，2个中危，3个低危漏洞	2018-11-14 1(	8
WAF服务	已完成	填写域账号	需要接入	2018-11-20 1(	已完成	2018-11-21	10

SDL 2.0 解决问题了吗？

- 单个报告输出，解决单个项目问题
- 多项目间没法统一比较
- 无法跟踪同一项目的风险趋势

SDL 3.0

面对的威胁

会员

撞库盗号
帐号分享
批量注册
垃圾注册

视频

搜索爬虫
盗播盗看
广告屏蔽
推荐作弊
广告作弊
评论作弊
弹幕作弊
有效观看作弊
页面浏览作弊

活动

薅羊毛
抽奖作弊
投票作弊
拉新作弊
任务作弊

直播

挂站人气
恶意图文
抢红包

电商

恶意下单
订单欺诈
黄牛
虚拟商品套现

支付/金融

盗号盗卡
洗钱
恶意提现
恶意借款
代理中介
信息伪造
征信修饰

其他

钓鱼邮件
恶意爆破
短信轰炸
垃圾信息
渠道防刷

SDL 3.0

✓业务视角

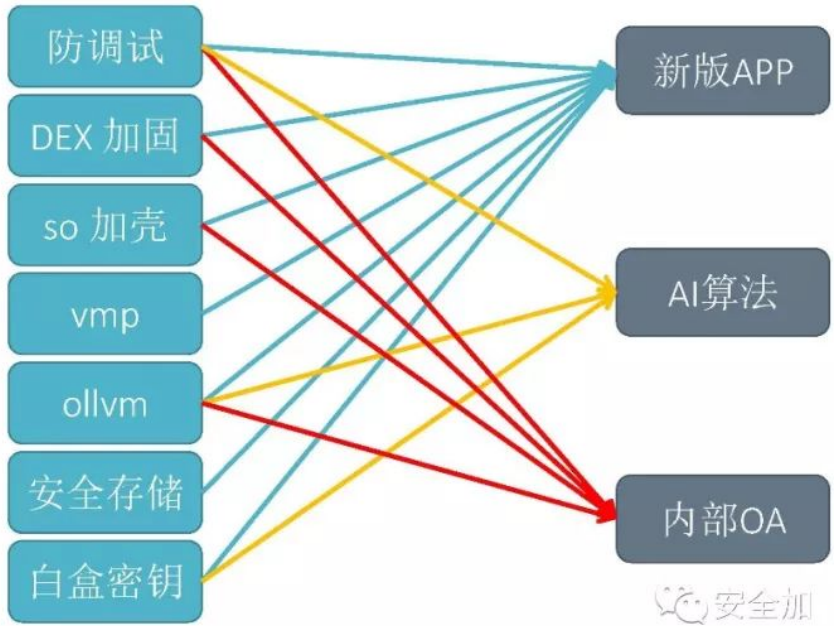
- 安全等级
- 评估关注点
  - 隐私，数据，手机端，风控。。。
- 业务线不同

✓乙方思路

- $$
- 人
- 沟通成本

SDL 3.0

✓按需求赋能



SDL 3.0

✓按业务线聚合

项目数量：近4次SDL项目（默认）　项目名称：爱奇艺

爱奇艺 项目积分

	SDL20180930095754815	SDL20181017100305584	SDL20181031145635509	SDL20181115160403604	Counts
需求评审加固	✓	✓	✓	✓	4
敏感信息报备流程	✓				1
双新评估流程	✓				1
隐私评估流程	✓	✓			2
白盒扫描服务	✓	✓	✓	✓	4
人工代码审计	✓	✓	✓	✓	4
安全扫描服务	✓	✓	✓	✓	4
渗透测试服务	✓	✓	✓	✓	4
WAF服务		✓			1
堡垒机服务	✓				1
风控系统	✓				1
CA证书	✓		✓		2
白盒密钥SDK				✓	1
设备指纹SDK		✓			1
Total Score	56	51	78	23	208

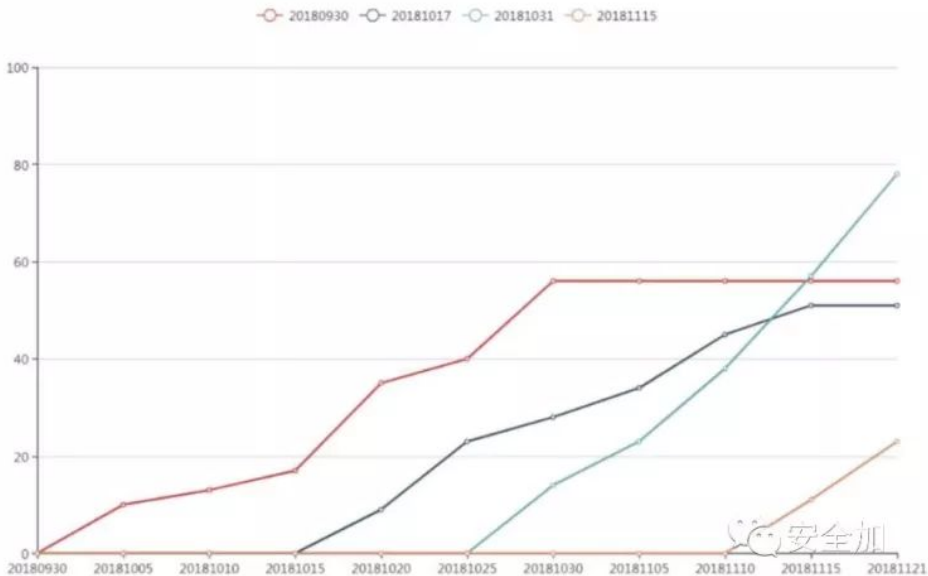
SDL 3.0

✓按权重打分

```
case "penetrationTestService":
    if (toDoHighNum8 != 0) {
        if (toDoHighNum8 <= 3) {
            score += ((doneHighNum8 / toDoHighNum8) * 7 + 3.0) * 0.6;
        } else {
            score += ((doneHighNum8 / toDoHighNum8) * 7 + (3.0 / (toDoHighNum8 - 2))) * 0.6;
        }
    } else {
        score += 3.0 * 0.6;
    }
    if (toDoMediumNum8 != 0) {
        if (toDoMediumNum8 <= 5) {
            score += ((doneMediumNum8 / toDoMediumNum8) * 7 + 3.0) * 0.3;
        } else {
            score += ((doneMediumNum8 / toDoMediumNum8) * 7 + (3.0 / (toDoMediumNum8 - 4))) * 0.3;
        }
    } else {
        score += 3.0 * 0.3;
    }
    if (toDoLowNum8 != 0) {
        if (toDoLowNum8 <= 8) {
            score += ((doneLowNum8 / toDoLowNum8) * 7 + 3.0) * 0.1;
        } else {
            score += ((doneLowNum8 / toDoLowNum8) * 7 + (3.0 / (toDoLowNum8 - 7))) * 0.1;
        }
    } else {
        score += 3.0 * 0.1;
    }
      score = score * 0.9;
```

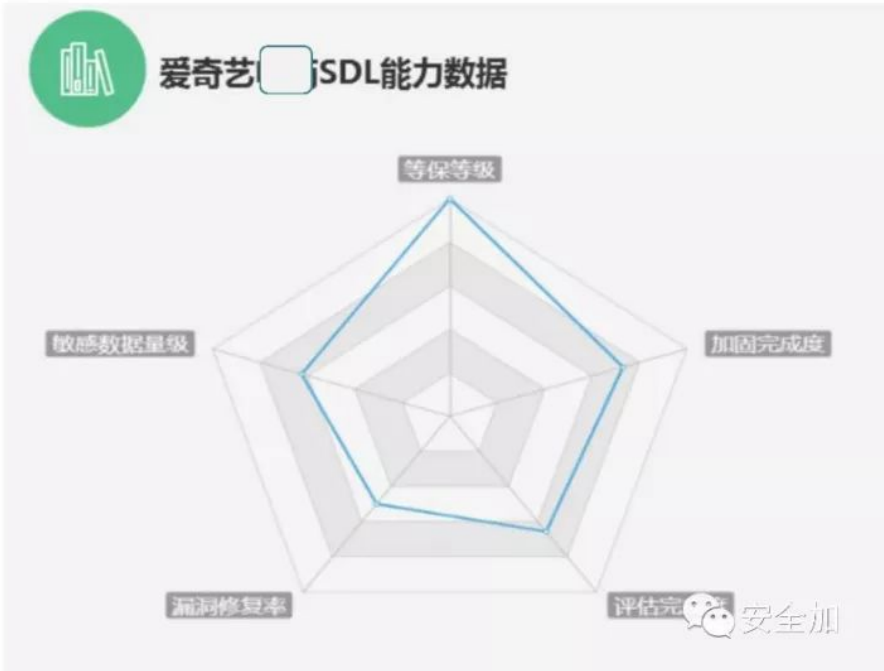
SDL 3.0

✓按时序呈现


20180930
20181017
20181031
20181115
100
80
60
40
20
0
20180930
20181005
20181010
20181015
20181020
20181025
20181030
20181105
20181110
20181115
20181121

SDL 3.0

✓按雷达图对比



谢谢