# 应用安全

## 理解

应用安全对象是应用，围绕着应用生命周期进行。理念有SDL/DevSecOps。

应用类型有APP，WEB系统，小程序，PC客户端，服务器应用。

落地应用安全理念，安全介入应用开发的各阶段，在应用生命周期的各阶段对其进行安全检查与保护。

体系建设完成后，需要对实际运行效果负责。可以从漏洞检出率、安全培训效果、安全开发实现效果、新功能漏洞数量、代码审计漏洞检出率、渗透测试检出率、漏洞修复效率、安全流程CICD自动化程度等指标判断薄弱环节。

应用安全包含管理体系，技术体系，运营体系。

## 人选要求

因为应用的更新性，应用与业务的绑定性，业务变化性等，应用安全对能力要求较高，对经验要求不高。因为每个公司的情况不一样，没法照搬。

所以招聘的时候，有相同行业背景，且有经验的是第一匹配。因为可以照搬。

有能力，无经验，有行业背景是第二匹配。

有能力，无行业背景是第三匹配。

有经验，无背景是第四匹配。

提出问题的能力，比解决问题的能力重要。想明白需要什么，为什么需要，提出功能需求的能力，比实现功能需求能力重要。

有实际的SDL/DevSecOps落地经验，有从零搭建落地的能力，越全面越好。

有体系运作经验，能够从体系中发现关键安全指标、参数、结果，从一堆运营数据中找到关键数据，以此为基础，持续改进SDL，为结果负责。

从当前现实中，快速准确的找到关键点。要有设计架构经验，能够完成相关设计架构工作。

## 落地

一般是先进行纯技术体系的落地，然后是运营体系，然后是管理体系。

### 技术体系

渗透测试，纯技术内容，时间短，见效快，而且位于应急范畴。

威胁建模，同安全设计一同实现。

代码审计，可构建pipeline，集成到CICD中，审计每次提交，实现自动化审计。也可周期性审计整个项目代码。

依赖检查，可随代码审计一同进行。

静态动态审计，可集成到CICD中。

异常行为审计，可借助日志，搭建审计系统，SEIM，按业务/用户/应用创建不同的审计规则，发现异常行为。

安全加固，在不同阶段有不同的加固技术，有混淆、加密、加壳、完整性检查、waf、网关、身份认证等。

应急响应，很普通，没啥说的。

持续安全感知，针对不同资产，有多方面的不同感知技术，如DLP、EDR、HIDS、流量检测、蜜罐、cpu内存监控等。

持续扫描及监控，针对不同资产，有不同技术，如代码的GitHub监控，服务器的端口监控，对域名的扫描等，很普通，没啥说的。

持续安全运营，真正发挥安全体系的价值，持续发现并处理安全问题。进一步有，通过数据发现应用开发中的突出问题，薄弱点。再进一步有，实现运营的自动化。比如waf发现某IP在扫描某个域名，可利用接口实现自动化拉黑24小时。比如业务日志发现，爬虫在爬取数据，可将爬虫IP拉黑或用户拉黑24小时。

### 安全运营初步建设

安全培训，持续运营，自动化，处理漏洞及问题。积累数据，根据数据持续优化。

### 管理体系

安全培训、安全需求、安全设计、应用发布、安全风险管理，是属于管理体系，要构建应用安全的工作流，保证产品、开发、测试及运维与安全的沟通同步。

威胁建模、静态动态审计、代码审计、依赖检查、渗透测试、异常行为审计、安全加固（waf，容器安全，镜像安全等）、应急响应、持续安全感知（运行时安全）、持续安全扫描及监控、持续安全运营处理，是属于技术体系建设。

培训部分可录成视频，周期性季度性培训，也可在新员工入职、项目立项后、项目测试等节点进行培训，对应有相关安全考试题进行培训效果检查。

安全需求（合规，安全架构，CIA，审计）可在项目立项会议上，随产品需求一同提出。

安全设计评估，可与开发架构师在架构阶段一同实现。

应用发布，应当借助系统进行发布，任何人都不应该有应用商城的账号。应当借助审批流，实现应用发布，经产品经理、开发测试、安全等环节审批后，实现自动发布到所选商城。

安全风险管理，可借助系统实现安全风险的跟进处理。如内部漏洞管理系统。

## 细节见excel文档