SDL体系落地实践与系统实现

重庆八戒网络股份有限公司

VSRC成都沙龙站

目　录

CONTENTS

谷计划

VSRC成都沙龙站

01

什么是SDL

SDL概念

SDL即Security Development Lifecycle (SDL)

是微软提出的从安全角度指导软件开发过程的管理模式。SDL不是一个空想的理论模型。它是微软为了面对现实世界中安全挑战，在实践中的一步步发展起来的模式。

SDL的核心理念

将软件安全的考虑集成在软件开发的每一个阶段 需求分析、设计、编码、测试和维护。

猪八戒对SDL的理解是将安全相关工作集成到项目研发的每一个阶段，以减少漏洞的数量并将安全缺陷降低到最小程度。大致可以分为：立项阶段、开发阶段、测试阶段、上线维护阶段、应急响应与运营阶段。

02

SDL困难三重奏

一重奏

安全团队常常是独立存在的部门，业务团队只有在需要安全策略支持时才通知安全团队介入，安全团队通常是在发生了安全事件或外部白帽子提交了漏洞才知道业务/资产的存在，造成对业务后知后觉的被动局面。

二重奏

。敏捷开发概念的引入，使得业务系统需要频繁快速的迭代开发，而安全人员在没有系统或工具的辅助下，常常需要频繁沟通、高频测试，使得上线流程效率低下。

三重奏

业务技术架构、开发语言不统一；上线流程不规范或不统一；公司资产未进行集中归口管理。

03

猪八戒网SDL流程实践

VSRC成都沙龙站

SDL落地前期准备

01 统一上线流程

使用开源流程控制系统或jira等，统一管理上线流程

02 统一域名资产

回收所使用的根域名的解析权限，由运维统一解析，只有统一管理的域名才能解析到公司服务器上

03 统一框架，提供安全组件

统一公司的开发语言和框架并协调相应部门开发必要的基础组件。

04 统一代码存储仓库

使用统一的代码管理仓库，git或svn

05 统一发布流水线

使用开源或自研的devops流水线管控系统

推行SDL

01 先知先觉

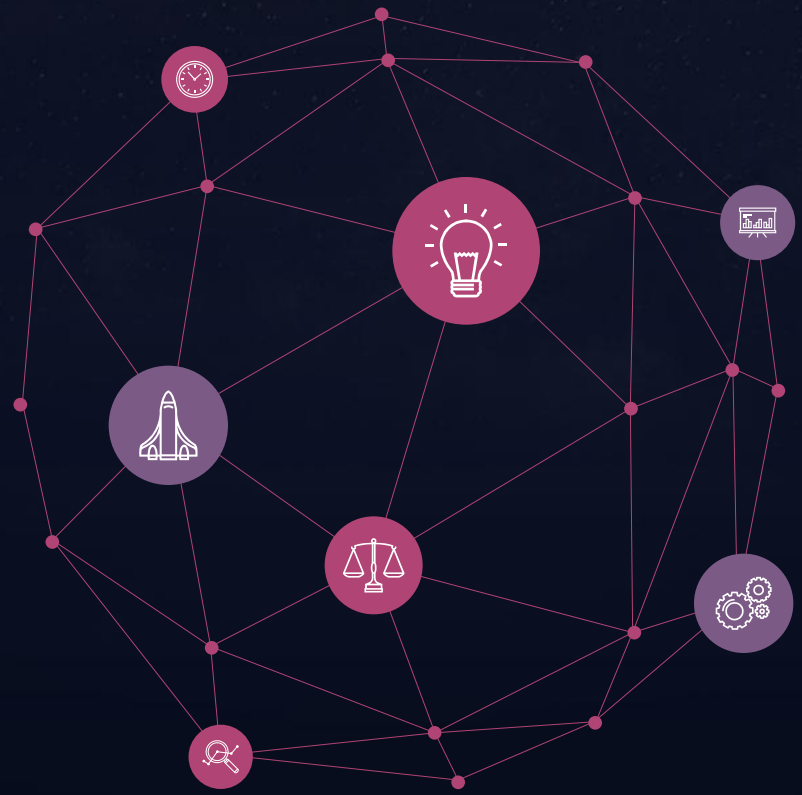
统一收集域名、项目名资产，有项目需要新增域名、修改域名，通知相应业务方进行安全评审

02 在线监控

通过统一的域名解析接口，维护域名与IP关系对应表，定时扫描web路径、端口

03 效率提升

接入统一的代码推送流水线，推送环境扫描安全组件和有问题的组件版本，收集每个项目所使用的组件以及版本信息



04 提升测试准确率

记录每次最终上线的hash值，当下次推送时，与上一次上线hash进行比较，扫描出差异信息。

05 运营管理

发现安全问题进行积分扣除，进行分值排行，与绩效挂钩，定期培训。

06 流程优化

安全测试进行排号，平均随机分配安全测试人员，过号重排队，重点关注安全开发能力低的人员，考核测试效率，漏测率。

SDL落地

立项阶段

1、安全评审
2、安全开发建议

开发完成阶段

1、自动化组件扫描

测试阶段

1、安全测试排期
2、灰盒测试
3、漏洞对应开发进行扣分处理

上线后阶段

1、黑盒测试
2、监控扫描

运营阶段

1、安全积分考核
2、安全意识&技能提升培训
3、安全测试人员考核
4、态势感知与风险预警

04 未来SDL规划

未来SDL规划

THANK YOU

谷计划

VSRC成都沙龙站