# 宜信SDL的深入探究与实践

宜信安全部

**序言**

作为一种根本性的应用安全解决方案，SDL（Secure Development Lifecycle）自从2004年微软发布以来，迅速得到了各大IT机构的认同和跟进，其所倡导的安全赋能、安全早期介入（细节请参考微软SDL社区）等理念在业界影响深远，是降低应用系统安全风险与安全成本的不二法宝。受益于SDL的影响力，业内其他应用安全相关解决方案也受到重视并得到广泛应用，比如BSIMM、OWASP SAMM体系、SSE-CMM、等标准体系，不仅为业界提供了丰富的方法指南，还提供的SDL能力成熟度衡量方法，为各个机构SDL演进指明路线。

近些年宜信为解决应用安全问题也是不遗余力的推进SDL，过程中参考各类SDL标准和各机构SDL推进总结文案，与很多同行一样，遇到过很多困惑，也进行一系列尝试。

本文将主要描述宜信SDL方案、推进思路，以及对相关问题解决过程与思考，为业内同行新增一个参考案例，在此欢迎同行拍砖。

**一、SDL问题与阻碍**

宜信SDL早前遭遇过的问题如下，跟很多同行遇到的问题基本相同：

**过度依赖于渗透测试**，无法有效作用于SDL前期阶段。应用安全团队成员多为渗透测试背景。

**渗透测试效果有限**，新产品上线或重大版本上线需要在上线前进行渗透，由于渗透测试资源有限，无法对所有上线版本进行覆盖。

**渗透测试流程或环节设置不合理**，渗透测试通常是上线前的最后一个环节，交付期限已经逼近，安全整改与延期导致产品线交付压力，造成安全部门与业务团队间某种程度对立情绪，这种情绪容易形成负循环，反过来影响安全部门各项工作的开展。（合并及缩略）

**SDL支撑的各种工具平台不充分，相关工作的沟通与执行效率不理想。**

这些问题同时引入了应用安全团队建设难题：

**应用安全团队建设难度大**，由于系统众多（粗略统计超过400个web系统），渗透测试工作压力大，简单而重复，没有时间增长新的技能。

由于外部团队存在一定程度的不合作情绪，安全工作存在一定困难，团队成员工作缺乏认可度和成就感。

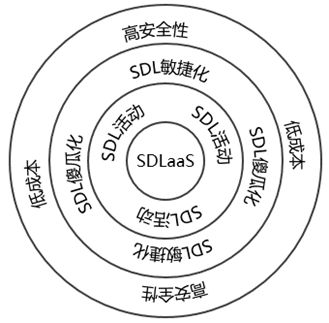
透过这些现象看背后的原因，个人觉得可能的**原因如下**：

**SDL缺乏整体性解决思路和方案，手段单一；**

**SDL核心理念需要升级。**SDL工作开展需要的不仅仅是技术，是管理，更需要一种服务理念。安全常规理念是管控，对话语权的依赖性比较大，这样的情景中安全部制订规矩，明确目标、流程路径与考核标准，设置各种卡管环节，想方设法将安全部门转变为管理者和考核者。安全部门为了工作便利，更是积极赢取和扩大这种优势地位，业务部门为了改变被动局面，走向了消极应对或对抗之路。这种管控理念容易形成安全部门的懒惰趋势，可以通过压迫轻轻松松完成任务，谁还愿意累死累活服务业务部门，部门间对立成为必然。

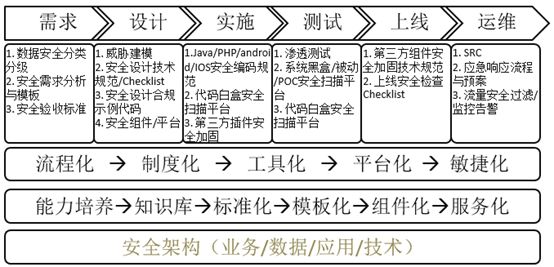
**二、宜信SDL解决方案**

结合上述问题与原因分析，宜信采取了系统化的SDL解决方案，落地过程中贯穿了服务理念，虽然目前仍在全面积推广中，但从已覆盖部门的反馈来看，获得了不错的馈。下面将会对宜信SDL解决思路与方案做一些说明。



上图为宜信安全部建设SDL的指导性思路，最核心的SDLaaS是指**将SDL作为体系化的安全服务提供给各个研发产品线，将服务理念贯穿到SDL各项活动中，使SDL能够敏捷化、傻瓜化。**SDL敏捷化是指SDL不拖研发进度的后腿，SDL傻瓜化是指SDL不给研发设置能力门槛，通过各种手段降低SDL的执行难度，最终能够达到高安全低成本的理想效果。

宜信SDL整体解决方案如下图所示：



宜信SDL整体解决方案参照微软模型做了一些调整，对于SDL活动项、SDL敏捷化和傻瓜化的实现路径进行调整和补充。

方案主要安全活动包括：

|  |  |  |
| --- | --- | --- |
| No | SDL活动名称 | SDL活动介绍 |
| 1 | **安全需求分析** | 明确数据安全目标和合规目标，产品经理是主要责任人，安全部提供赋能培训、演练与试点辅导等服务。同时安全部提供一系列的安全服务，协助产品经理实现安全闭环。 |
| 2 | **威胁建模** | 明确系统在实际运行环境和访问网络环境中主要安全风险，安全部提供威胁建模赋能培训，威胁模型风险基线确立、安全问题整改与跟踪、年度威胁模型更新与维护等服务。 |
| 3 | **安全设计规范** | 为主要场景下的安全措施设计提供一致的文本参考标准和检查标准，安全部提供推广培训、简易CheckList和合规审核等服务。 |
| 4 | **安全组件与平台** | 为安全设计规范合规提供标准化的技术实现，降低安全措施的设计与实施的门槛。安全部负责安全组件与平台的需求收集、设计与推广服务，协助其他部门开发。安全部提供桥梁服务，将个别产品线的优秀安全组件或服务推广到其他产品线。 |
| 5 | **安全编码规范** | 为安全编码提供一致性文本参考，包括安全编码流程、漏洞特征以及典型解决方案，安全部提供规范日常维护、宣贯、人工审计协助等服务。 |
| 6 | **白盒扫描平台** | 为安全编码提供自动化审计平台，安全部提供平台日常升级、规则维护、扫描报告培训与解析等服务。 |
| 7 | **黑盒扫描平台** | 提供黑盒安全扫描工具，供测试团队日常测试使用。安全部提供赋能培训、工具平台的日常升级维护和规则维护和报告解析服务 |
| 8 | **渗透测试** | 为即将上线产品提供安全测试服务，安全部提供测试、漏洞整改方案建议与跟踪等服务。 |

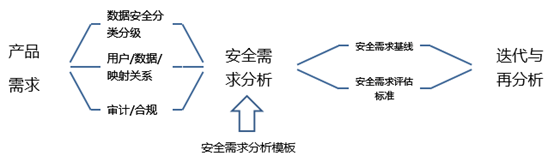
下面针对目前宜信已经开展，并取得一定经验的SDL活动进行简要介绍。

**1、安全需求分析**

这一项活动主要是从业务角度提出业务安全需求，包括数据安全需求与合规需求。数据安全需求主要从目标系统所包含的数据、用户出发，保障数据安全性和用户数据间的安全访问关系。合规需求主要是宜信内外部的合规要求进行罗列，是应用安全的底线。

每次安全需求分析都会形成新的基线，后续新的产品需求是否会触动已有基线，安全部给产品经理提供了一个简单明了的安全需求评估标准，帮助产品经理进行判断，**目前宜信安全部的做法是产品经理、开发经理和安全专家共同判断，产品经理主要负责判断哪些需求一定要做安全评估，安全专家主要负责判断那些需求不需要做安全评估，开发经理帮助缩小安全评估的范围。**

需求分析推广过程中，先培训、示例与演练、再产品试点，然后推广。产品经理更新安全需求时可以随时找安全专家帮助进行确认或评审。



**2、威胁建模**

实际上是针对目标环境中的目标系统设计的安全风险评估，宜信安全部目前采取微软STRIDE威胁分析模型。**威胁建模的重点在于发现了多少风险**，而不是建议了多少控制措施。威胁总是来自于特定运行环境与访问网络，威胁建模发现的往往是特定环境中的理论风险，一些风险甚至无法用简易的渗透测试进行验证，比如口令加盐哈希算法选择上MD5算法到底比SHA256算法弱多少，存在什么样的风险。虽然存在一些难题，但威胁建模的目标是发现所有可能的重大安全风险，最终形成一个理论上较为完美的安全设计方案，将安全风险降到可接受程度。

3、安全设计技术规范与CheckList

主要是为研发团队在具体安全措施设计时提供参考和自查手段，形成安全措施基线，使安全措施趋于标准化，安全措施标准化后，问题发现与整改的难度和成本都会有所降低。宜信已经初步形成用户管理/权限管理、身份认证、访问控制、加解密、日志审计、弱口令检测、web安全、移动安全等相关安全技术规范。

**宜信安全技术规范是在这几年累积的2000+的漏洞库上分析归纳总结而来，其中结合业内最佳安全措施实践要求和宜信自身的设计实践，过程中进行了多次试点部门的访谈、讨论和修订**，从目前的反馈来看，具有较强的适用性，得到了试点部门的好评。

**4、安全组件/平台**

为了降低安全技术规范的合规门槛，安全部尽最大努力将安全技术规范中的技术要求用安全组件或平台进行标准化实现，提供给各个研发部门使用。将安全措施的实现逻辑进行封装，形成可以继承的安全组件与服务，进一步降低安全设计与实现的难度，合规检查变得简单，只需要查看系统集成的安全组件版本号及其配置参数，对于集成了安全平台相关服务的系统，其合规更是简单，只需要检查安全平台相关安全配置参数即可，其与各个业务线的代码逻辑实现了完全解耦。

安全措施出现漏洞后，修补更方便快捷，进一步降低了成本和安全风险。安全组件化、服务化是安全专业化的体现，由于安全部的深度参与，安全组件与平台的设计开发更加专业，更为可靠。

**目前宜信安全部联合其他业务线提供了多种安全组件或平台，比如身份认证平台、SSO平台，多种场景的加解密组件、多种形式的图形验证码、弱口令检测组件与服务等。**

**5、安全编码规范**

通常规范是日常学习的材料，也是合规检查的依据，安全编码规范需要告诉研发工程师安全编码流程、代码安全审计方法、重大安全编码漏洞的典型解决方案等内容。安全编码规范不能简单等同于安全编码知识库，了解到的一些单位，其安全编码规范通常是从网络、兄弟单位或标准化机构借用过来的常见漏洞的解决方案，缺乏针对性，我们建议针对一个轮次中（比如一年）代码人工审计和工具扫描的结果进行统计排序，排名靠前并且风险重大的安全编码漏洞及其解决方案建议写入安全编码规范，并且在新一轮年度工作中作为安全编码检查重点，重点消除这些安全编码漏洞。

安**全编码规范条目不宜过多，我们的经验是10条左右，条目过多容易分散学习者和审计者的精力，难以达到预期的效果**。编码规范实施一个轮次后（如一年）如果统计排序发生了变化，则调整安全编码规范，开始新一轮的推广培训和督促检查工作。

**6、代码白盒安全扫描平台**

宜信安全部在开源平台的基础上通过二次开发形成了自己的白盒代码扫描平台，该平台功能不仅是代码安全扫描，而且嵌入了代码白盒扫描的相关服务流程，可以通过配置，自动连接代码仓库，自动发送报告到邮箱，还可以在DevOps平台中自动执行上线前的代码审计扫描，扫描报告发送到安全团队邮箱进行报告复核。

**安全部针对扫描平台进行了使用培训，报告分析方法培训，也随时提供报告解析服务。**为了方便研发部门自主代码扫描，安全部还计划给每个研发部门部署一套平台，安全部负责各个平台的日常升级与规则维护，让研发部门更简单更轻松的执行代码扫描工作。

**7、渗透测试**

对于宜信而言，系统多，上线频繁，渗透测试面临的最大问题是效率问题。作为黑盒测试，其覆盖的深度与广度不好拿捏，渗透测试的有效性难以保证，为了扭转这种局面，**宜信安全部努力推动渗透测试人员与产品经理、开发经理合作，获取并理解需求，获取代码更新比对信息，在持续迭代过程中，渗透测试资源倾斜到那些新增或变更数据、功能和接口上，将资源聚焦，避免重复测试，将渗透测试由黑盒转变为白盒**。

另外渗透测试的时机需要做一些调整，以前的渗透测试作为上线前的最后一个环节，给研发团队和渗透测试团队很大的时间压力，重大渗透发现，容易造成交付延期，也容易催生安全与业务的对立情绪。安全部给产品经理制定了简单明了的判断标准，符合标准的新需求无需渗透测试。

**8、系统黑盒/被动/PoC扫描平台**

为了响应研发团队自主安全测试需求，进一步细化安全部和各研发团队的安全分工，安全部为各个研发团队提供了公共的黑盒/被动/PoC扫描平台，针对个别研发团队的高负荷扫描需求，安全部为这些部门部署了独立的扫描平台，**安全部对这些平台进行统一培训和规则维护。**

**扫描平台负责执行常规的安全扫描检测工作，扫描报告通过平台供安全部参考，安全部将后来主要负责非常规和较高专业技能的安全测试。**

三、宜信SDL核心目标

宜信安全开发建设在未来需要达成的如下两大效果：

1. **敏捷化**

宜信安全部希望**通过流程化→制度化→工具化→平台化**等逐步进阶方式，使研发部门和安全部能够快速发送请求、快速共享各种SDL过程信息，快速沟通，最终能够使得SDL各项工作敏捷执行，坚决不拖研发与运维的后腿，抹除安全反敏捷的呆板印象。

**宜信SDL的终极目标是希望通过平台化的服务，连接所有产品线和安全部所有人员，准确触发各项工作流程，快速获取或提交各项过程信息，并快速交付各项工作成果。**这里的工具平台主要是指各类需求管理系统、源代码管理系统、各种流程管理系统，CI/CD相关系统，DevOps相关系统，将SDL相关服务嵌入到开发交付流程中。目前宜信SDL敏捷化程度无法确定达到了哪一个阶段，目前多个阶段的特征并存，需要持续建设和整合，使得SDL工作平台化成为主流。

1. **傻瓜化**

SDL工作对于研发部门而言是一项有门槛的工作。工作过程通常是人员能力和问题难度的博弈过程，让安全工作变得不是问题，有两种方法可以选择。

**第一种方法是人员能力没有变化的情况下，安全工作难度降低**，比如提供安全技术规范、安全组件、安全服务以及相关集成示例代码，将安全逻辑标准化、复用化可以降低安全设计难度和开发难度；将安全措施的设计开发与应用系统业务逻辑剥离开，使之专业化，比如各种认证服务、加解密组件与服务等，不仅可以减少开发量和开发难度，还可以提升安全措施的安全程度和稳定性；

**另外一种方法是提升研发人员安全能力**，在有能力的高手面前，再难的安全技术问题也是浮云。目前宜信安全部两种方法并举，一方面大力推广各类安全培训，提供工具、漏洞靶机和练习环境，提升研发团队安全意识与能力，逐步形成宜信的SDL能力课程体系；收集业内最佳SDL实践，总结归纳研发过程中发生的各类安全问题，形成安全知识库，供大家日常学习。另一方面大力推动安全设计的标准化、模板化、组件化与服务化，让研发团队从安全设计与安全措施实现的困境中解脱出来，降低安全能力门槛。目前宜信安全部会在日常工作中收集各产品线需求，投入资源研发安全组件与服务，而且还会收集各产品线的优秀安全组件成果，充当桥梁作用，再将这些优秀安全组件扩散到其他产品线。

**四、关于安全架构与SDL**

安全架构是SDL一个很重要的输入，也是SDL发展到高级阶段的产物。SDL通常关注单系统的安全性，即使是复杂系统，也通常被拆分为若干个小系统进行安全分析，这一点在威胁建模的时候表现尤为充分，无法像安全架构那般安全整体布局、整体架构，注重系统拆分、既有全系统安全目标，也有子系统安全目标拆分，互有配合，相得益彰，而SDL着眼点很难兼顾系统全貌，在定义子系统安全需求或目标时，容易扩大化，忽视周边环境与周边系统的安全配合。

**安全部希望未来在SDL建设的过程中，对宜信所有系统的安全设计进行归纳总结，配合系统分层、微服务改造，以及业务、技术和数据中台等概念的落地推进，逐步形成宜信自己的安全架构体系，弥补SDL缺陷的同时，降低应用安全建设成本，提升SDL工作的效率**

**五、SDL工作的其他感悟**

学习和推进SDL已有近10年，越来越感觉到SDL是一项软技巧水平要求比较高的工作。

**安全即服务**

SDL既然可以作为一项服务，**就应该做到以人为本**，尽可能的为研发团队着想，为研发团队安全赋能，降低其安全实施门槛，能够轻轻松松的应付各种安全问题，只要能走进研发团队心里，得到研发团队的认可，实现高效配合，取得较好的服务效果是水到渠成的事情。正所谓，送佛送到西天，扶上马再送一程，说的就是这个道理。

**融洽的安全服务关系**

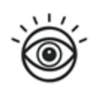
**安全部的领导有责任在组织机构内营造出一种融洽的安全服务关系**，在安全专家输出各项安全服务的同时，消除各种额外的游说劝服或客服畏难情绪的成本，后者往往是安全服务专家的短板，笔者见到过一些技术超强的安全专家，工作中缺乏这种融洽的服务氛围，也无能力创造这种氛围，空有一身本领，却无法为业务有效输出价值。实践中，安全骨干可以在管理层之间首先营造出这种服务氛围，后续通过在部门内部反复讲解、亲身示范、日常强调等手段，一定会将这种氛围逐渐荡漾到执行层中去，安全服务氛围就会随之形成。

**安全敏捷与DevSecOps**

从SDL各种分析报告来看，SDL的核心思想是安全在应用生命周期早期阶段介入，越早解决问题，越能降低安全风险，但从我的个人经验来看，这个核心思想还需要附加新的内涵，为了控制安全风险，“团结一切可以团结的力量”，作为SDL根本性指导思想会更贴切些，研发团队和安全团队一样，都是SDL建设的主要力量，**安全和研发越是深度合作，安全工作开展的形式、效率与效果提升就越是有无限可能**，就拿前方说过的渗透测试，深度合作，就可以将渗透由黑盒转换为白盒，由普遍撒网转换为精准打击，甚至安全团队可以将一些基本的安全任务，如黑盒深度扫描可以交由研发团队完成，可以让安全团队集中精力检测和解决一些安全深层次问题。

工作过程中曾遇到一些乙方公司推介类似于云WAF的产品，针对访问流量进行深度检测，再加上大数据分析、海量攻击样本训练与机器学习，有一些产品还辅以在线专家人工分析，给人印象这是应用安全的一站式解决方案，安全部门终于找到了与研发团队无关的应用安全解决方案，但经过试用或测试后，理性回归，还得回到与研发团队紧密合作的老路上来。

**因此安全敏捷与DevSecOps的核心是安全与产品、研发和运维能够无间合作，消除各种合作过程中的部门壁垒，快速有效的输出安全价值，取得良好的安全效果。**



写在最后：

SDL作为安全服务并不排斥安全绩效考核，如果SDL团队既有考核的话语权，同时又能放下身段，具有安全服务的理念和能力，一定可以将SDL工作开展的更顺畅更有效果。

SDL没有固定形态，一切SDL活动的执行都需要因地制宜， 但核心的SDLaaS的理念需要长期支持，贯穿到SDL团队日常的每一项活动中去，终有一天，**安全团队与各业务团队面临安全问题时，携手前行，相互支持，荣辱与共，最终为业务搏出一个安全而又明亮的前程，我想这是我们所有SDL工作者的共同愿望。**

原文链接：

搜狗微信搜索： 宜信SDL的深入探究与实践