SYNOPSYS®

如何制定坚如磐石的软件安全计划

（以及您需要此类计划的10个理由）

目录

您有软件安全策略吗?

今年,您测试了46个Web应用、19个移动应用和20个客户端-服务器应用。您购买了一款新的应用安全测试工具,发现了112个漏洞。您感觉相当不错。

但还不能高兴得太早!首先问问自己:是否明显降低了风险?是否存在未处理的严重漏洞?公司董事会是否理解您所开展的这些工作的重要性和影响?

如果无法确定这些问题的答案,说明您可能拥有软件安全测试计划,但还没有软件安全策略。

如果您在应用安全测试方面进行了投资,说明您在朝着降低风险的方向努力。然而,您现在应该进入下一个阶段:制定软件安全计划(SSI),将公司的应用安全活动从成本中心转变为竞争优势。

本指南的适用对象

如果您曾经有过如下经历，则应该阅读本指南：

- 完全凭直觉来决定安全预算投资于何处
- 在安全问题的轻重缓急和修复方面与开发团队意见不合
- 难以与公司高管或其他部门沟通安全要求和结果
- 在同一团队中屡次发现相同的安全缺陷
- 急匆匆寻求资源来解决容量问题、应对开发进度或监管政策的不断变化
- 在最后一分钟被要求测试出那些可能导致产品延迟发布的应用漏洞
- 每当听到有关数据泄露事件的新闻报道时（例如Twitter、Uber、Twilio和DoorDash），都不禁会想："这种情况会发生在我的公司吗？"
- 因糟糕的安全规划而备受煎熬
- 因没有安全的软件开发生命周期（SDLC）或者不知道哪些供应商采用了好的软件安全实践而被客户要求让步，导致交易延迟
- 有可能受到联邦贸易委员会或其他监管机构的审查
- 请如实回答。我们不会记录您的答案。如果您对这些情况似曾相识，请继续阅读本指南，了解制定和演进SSI的行之有效的步骤，通过这些操作，您可将当前的安全活动转变为结构化、战略性、坚如磐石的计划。

但我已经开展了应用安全测试，这还不够吗？

一句话，不够。

在案例研究和白皮书中，我们经常看到企业将应用安全测试视为事实上的软件安全技术，这是企业用来表明他们重视安全的灵丹妙药。

应用安全测试是所有安全计划的关键且必要的组成部分。然而，仅渗透和补丁应用测试根本不是安全策略。应用安全性测试只是起点，而不是终点。

主动安全可以节省时间和金钱，但这还不够。您需要实施安全计划才能全面降低风险。

—Tyler Shields，Forrester Research, Inc.
高级分析师

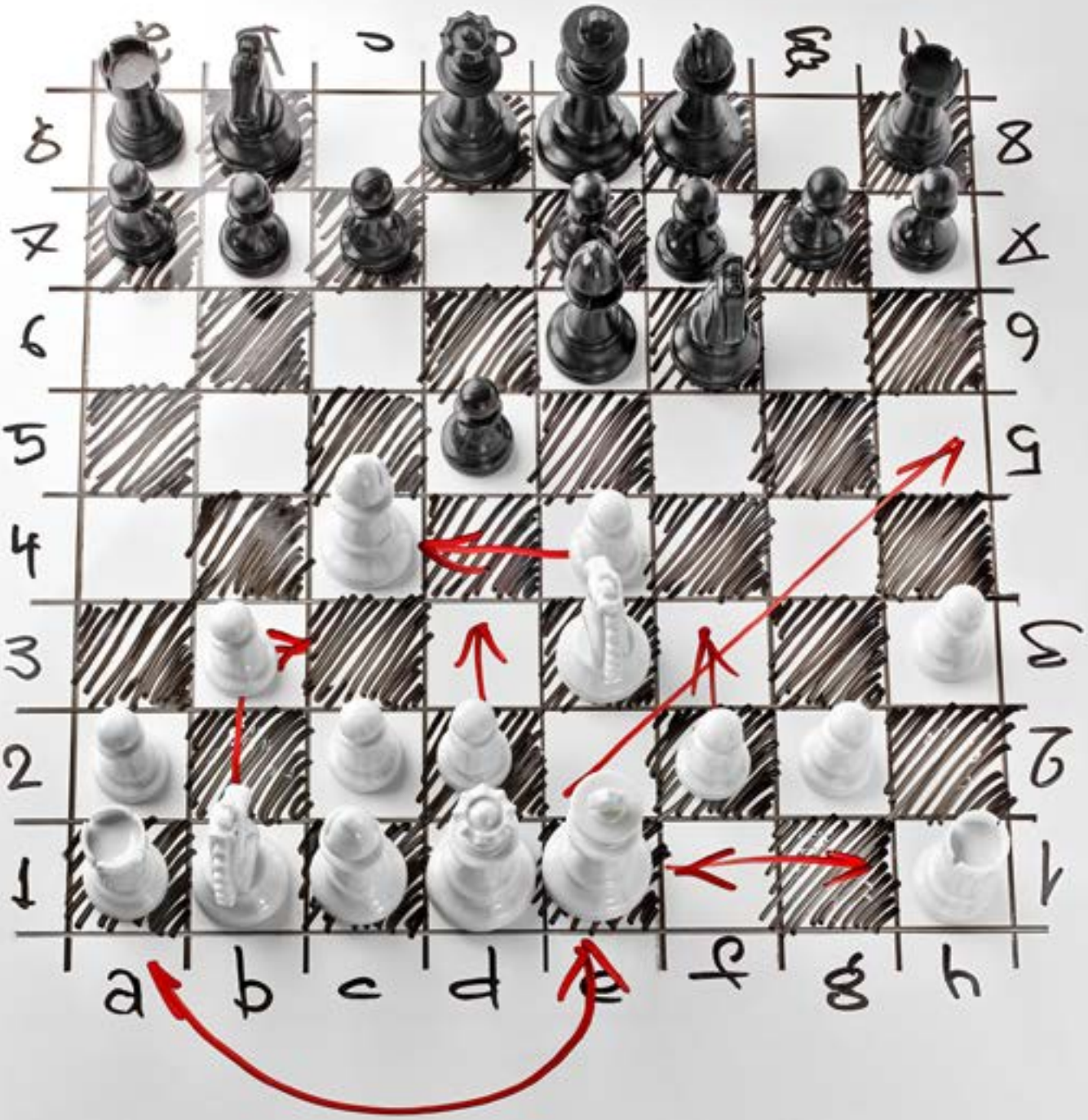
您需要软件安全计划的10个主要原因

制定SSI好处多多，包括：

1. 确保优先处理不可接受的风险
2. 为开发人员提供一条以最小干扰来创建安全软件的途径，从而提高生产力
3. 指定专人或小组负责降低软件安全风险，确保这项艰苦的工作能够真正完成
4. 在安全和开发团队之间搭建正式的桥梁，以便他们就优先事项达成一致，共同承担责任，享受共同的奖励机制，从而减少混乱局面，使每一个人都能更高效地参与协作
5. 记录并协调产品经理、架构师、开发人员、测试人员和所有其他利益相关者的软件安全需求，以实现整个组织的一致性
6. 对软件供应链中的每一个人（包括内部团队和外部供应商）应用统一标准，这样您就可以相信软件是安全构建的，无论其来自何处
7. 为所有软件安全需求（策略、标准、工具和专家等）提供卓越中心，以便所有利益相关者都有地方寻找答案并提高技能
8. 使您能够评估成功与否，并与客户、合作伙伴和董事会沟通
9. 确保以一致的方式与软件开发链中的每个利益相关者交流，提供一致的培训，以强化安全第一的文化
10. 在管理风险的同时满足开发团队不断变化的需求

为坚如磐石的软件安全计划绘制蓝图

最有效的SSI是专门针对企业需求进行微调，并能够围绕着员工、流程和软件组合进行扩展的SSI。它允许您通过清晰易懂的方法来降低风险，并解释投资决策的理由，从而帮助您展示工作成果。



我们认为，为SSI奠定坚实基础（或重新唤醒陈旧的SSI）的最佳方法是一种五步法。

构建　　评估　　验证　　改进　　管理

构建

为SSI奠定适当的基础需要满足一些前提：一些用于设置优先级的关键信息，治理结构，以及将安全性融入开发周期中的培训和工具。我们逐一进行详细讨论。

每位安全主管都应该知道的5件事

在开始为应用安全活动设置优先级之前，您需要了解您所面临的全部挑战。您需要回答下面这些问题：

- 您正在进行哪些开发项目?截止日期是哪天?
- 哪些团队正在接触哪些应用?
- 哪些代码是内部开发的?哪些软件是现成的商业软件或第三方软件?
- 您最大的技术风险在哪里?
- 您的应用目录中都有哪些应用?哪些应用对您的业务影响最大?

去寻找答案吧。如果您不能马上找到所有这些问题的答案，也没关系。SANS Institute近期的一项研究表明，超过四分之一的受访者不知道他们公司到底使用或管理着多少个应用。

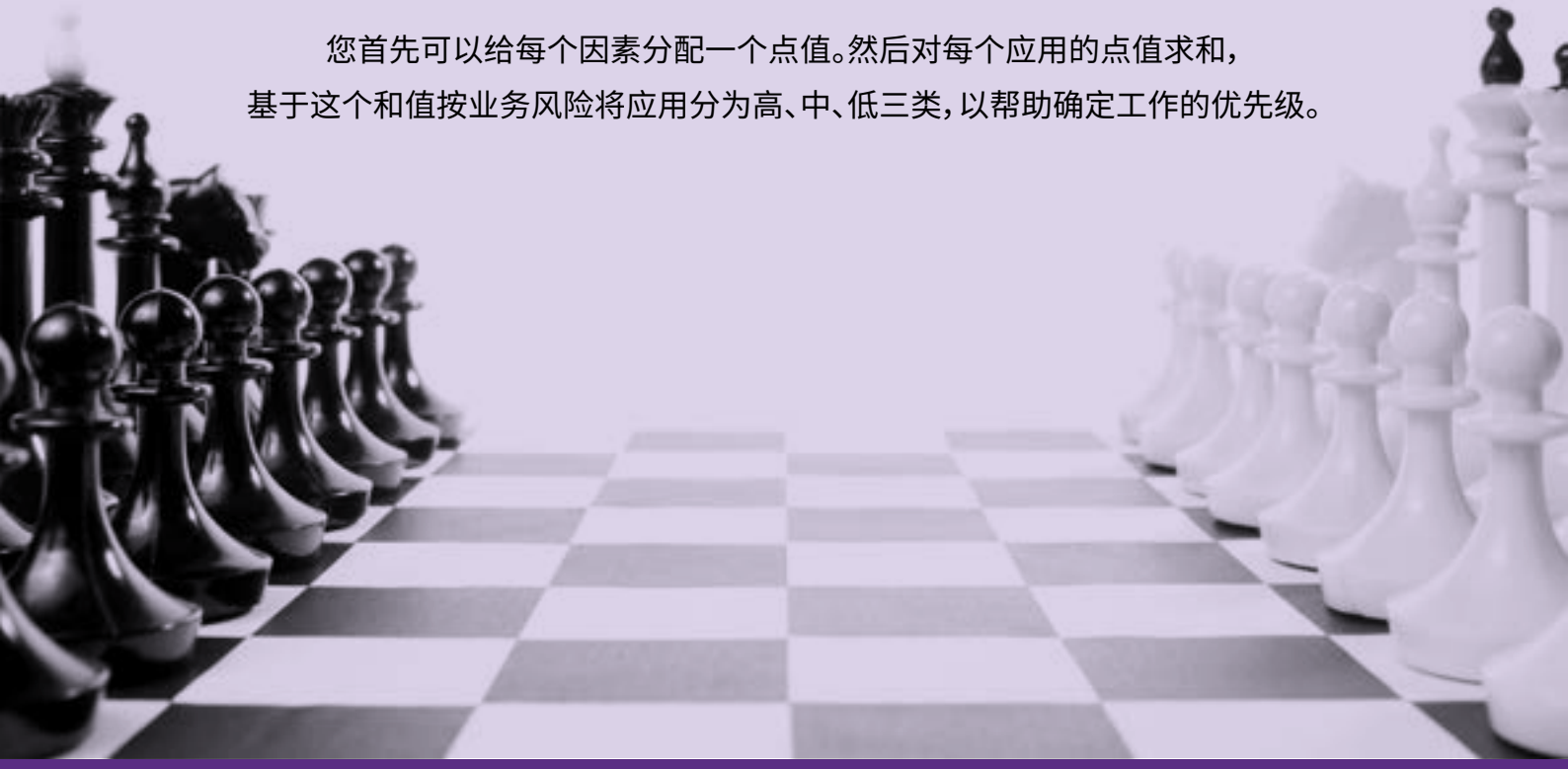
您应该先弄清楚自己知道什么，然后再继续积累知识，寻找答案。

风险 = 发生概率 x 影响

左右应用的业务影响的因素包括：

- 与收入的关系
- 对业务连续性的影响
- 合规或监管要求
- 所服务的受众
- 存储或访问了多少敏感数据
- 访问方法
- 与其他系统的连接/集成
- 人身安全
- 国家安全

您首先可以给每个因素分配一个点值。然后对每个应用的点值求和，基于这个和值按业务风险将应用分为高、中、低三类，以帮助确定工作的优先级。



坚如磐石的SSI有何秘诀

SSI成功的秘诀在于治理。因为治理可以为安全活动确定责任，为行为人确定要求，因此，它是为可持续的SSI奠定或调整基础的必要步骤。

治理本身并没什么区别 — 无论是由中央安全团队通过正式的策略、明确的标准和一些系统化流程而建立，还是由scrum管理员通过针对几个应用团队的技术和编码标准而建立— 但关键是必须有人负责，并且必须明确软件安全相关要求。否则，您就不可能拥有安全的SDLC。

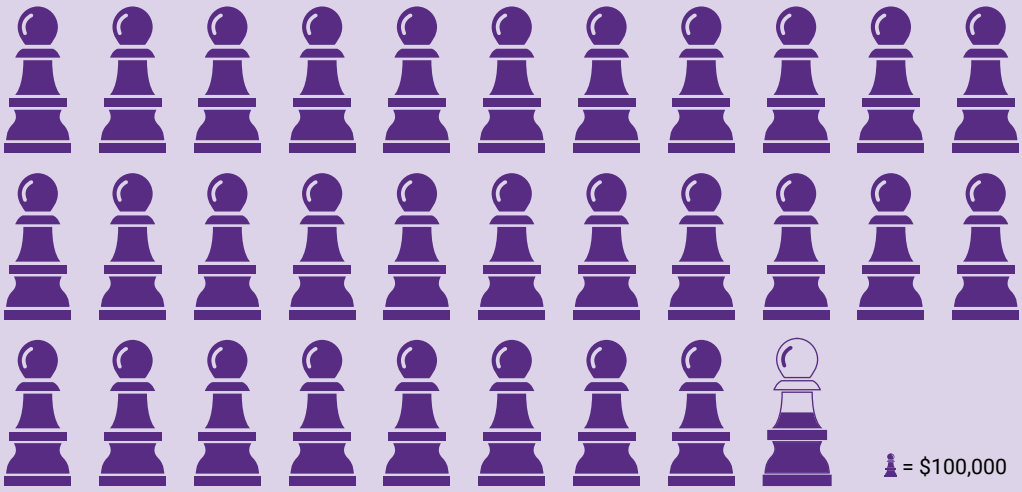
提醒一句：不要在真空中制定安全策略。虽然安全主管可能是最终负责人，但他/她必须与公司的其他领导全面讨论应用安全问题，并在整个企业中进行宣传。最重要的是，尽早让开发团队参与进来，并确保他们也对策略的制定和执行负有责任。

大多数公司都没有安全的SDLC

这是因为尽管大多数公司都声称他们为了保证安全水平而对其应用组合实施了软件安全治理或系统化控制，但实际情况正好相反。

不要成为他们中的一员。因为客户不喜欢，保险公司不喜欢，监管机构不喜欢，很快便会波及到全公司，惹得高管和董事会也不喜欢。下面，我们以类比的方式来看看缺乏安全策略所产生的影响。

部署安全自动化技术可将漏洞的生命周期缩短74天



全面部署安全自动化技术可将平均成本节省305万美元

5个关键安全策略

1.软件安全。传达公司对软件安全的总体期望，并将安全性融入产品需求、实施、采购、部署和运维中。至少要涉及以下主题：

- **安全的SDLC。**这是不容选择的强制性要求。
- **应用风险排名。**就确定哪些应用对业务最重要提供明确的指导。
- **应用设计。**要求将安全控制内置在系统设计中。
- **应用开发。**需要特定的技术栈和强制性编码标准。为开发人员提供明确的指导和预构建的安全设计模块。
- **应用测试。**确定哪些应用必须接受测试及其合格标准。制定测试时间表。
- **软件项目影响度排名。**定义软件项目的影响度排名标准。概述排名如何推动相关的保障工作。
- **缺陷的严重程度和补救措施。**为确定漏洞和缺陷的严重程度制定规则，并为修复编码漏洞和设计缺陷制定时间表。

2. 网络安全。确定有助于应用安全的协议和授权级别。

3.数据安全。识别宝贵的IP和敏感客户数据并进行分类，以帮助开发人员应用适当的安全功能。

4.物理安全。制定访问控制措施并保护您的物理基础设施。

5.灾难恢复。确定发生攻击时需要采取的措施，包括如何报告、记录和处理应用攻击。

确保软件安全策略与其他策略的一致性。

创建持续培训计划的诀窍

参与软件开发生命周期的每一个人都必须知道如何履行与其角色相关的软件安全职责：高层管理人员、中层管理人员、产品负责人、测试人员、系统架构师、开发人员和所有其他人。

为何选择开发人员？

开放式Web应用安全项目 (OWASP) 每三年发布一次10大Web应用安全漏洞列表，以提高安全意识。众所周知的安全漏洞每年都会出现在列表上，如SQL注入和跨站脚本攻击。然而，如今的软件开发人员仍将这些漏洞编码到应用中。

有效的SSI必须确保在编写代码时将应用安全放在核心位置。在构建应用时，越早清除漏洞和缺陷，QA阶段所需的修复时间越短，成本越低，而且推出安全的应用的速度就越快，甚至可能成为一种竞争优势。

您必须在SSI计划中建立激励机制，以激励开发人员除了交付代码外，还要提高创建安全代码的能力。您可以通过提供面对面和在线培训来支持开发人员。但是，如果您希望开发人员认真对待这些事情，并将其作为职业道路的一部分给予重视，则必须将激励机制纳入到绩效评估和薪酬中。

借助适当的工具将安全性纳入开发工作中

动态分析和渗透测试等安全测试技术有助于安全团队以一致的方式识别各种漏洞。但是，这些技术都只作用于生产或预生产状态的应用，导致漏洞修复既昂贵又耗时。

您应寻找有助于在安全SDLC中左移的工具。越早进行安全测试和修复，成本效益和生产力就越高。

> 由于能够及早预防缺陷，我们的生产率提高了15%。
>
> —Jim Routh，Aetna首席信息安全官

您可将安全工具直接集成到开发人员的现有工作流和技术中（如集成开发环境），帮助他们从一开始就创建安全代码。如果新工具要求开发人员改变工作流程，或者放弃他们熟悉的系统，那么，让他们接受新工具将是一场艰苦的斗争。

评估

许多人都认为软件安全性是无法评估的。软件安全的目的是防止攻击取得成功，您如何评估没有发生的事情呢？

但是，您不知道安全漏洞的存在，并不意味着它们真的不存在。现在不存在，并不意味着将来也不会存在。

即使您不能证明成功阻断了黑客入侵，也可以通过其他方式来演示SSI的效果。

内部指标可以帮助您朝着业务目标不断改进。在为SSI设定目标时，要将其与基本业务目标挂钩。这样，当您分享成果时，便能够展示SSI如何从根本上改变了企业的运营方式。

通过向董事会展示您不仅改进了运营流程，而且还将软件加速推向市场并节省了资金，您将能够把安全计划从纸上谈兵转变为重要的业务能力。

没有证据来证明成效，并不能构成没有成效的证据。

如何从高管角度阐述问题

如果您专注于高层领导理解和重视的衡量指标，则更有可能获得他们对SSI的持续支持，或者能够争取到更多资源。

外部指标允许您将内部SSI与大量的SSI进行比较。除了展示内部改进外，您还可以将内部SSI与其他公司的SSI进行比较，让公司高管从更广阔的视角来审视您所取得的进步。我们应该直面现实：让公司领导层看到别人的做法可以成为激励他们重视安全的强大动力。

了解有关BSIMM的更多信息

用于评估和规划SSI的行业领先模型是软件安全构建成熟度模型（BSIMM）。BSIMM可对所有企业采用的软件安全实践进行基准测试，是可以增强软件安全性的公认模型。它可将您的项目与有数据支撑的安全行业标准进行比较。

您应考虑开展BSIMM评估并加入BSIMM社区。开展BSIMM评估使您能够了解自己的表现，加入BSIMM社区则允许您不断接触SSI的既有群体。随着您的计划不断演进，您可以借鉴他们的经验教训。

10个重要的SSI指标

以下是可以证明软件安全性得到持续改进的10个指标(和一个额外指标):

1. 软件资产现状,包括每个软件的健壮性和风险数据
2. 经测试的应用所占百分比,包括按需测试或定期测试
3. 接受了所有类别和级别的风险测试的应用数量,从零级、到轻量级、再到深度级
4. 由于未满足软件安全策略或合规要求而需要进行调整的应用数量
5. 修复各种类型的安全缺陷所需的时间
6. 直到进入生产阶段才被发现的安全漏洞和设计缺陷的数量
7. 做到安全SDLC各项指标达标的软件项目(无论是开发还是采购的软件项目)的百分比
8. 开发人员在漏洞修复活动上花费的时间
9. 从需求挖掘到生产阶段,由于软件安全问题而导致延迟的次数
10. 满足或超过合规要求的应用数量
11. 具有相应岗位技能水平的软件安全利益相关者的数量

验证

一旦您制定了策略和评估计划，便可以设置检查点来验证工作团队是否正在执行SSI中的活动并满足SSI要求，以产生预期影响。

您可以这样想象“验证”步骤：您的汽车通常一两年进行一次安全检查，但如果看到发动机故障指示灯亮了，您便会提前开到修理厂进行检测，看看到底是什么情况。

缺陷发现就像汽车上的发动机故障指示灯。当您需要尽快解决系统问题时，它会向您发出警告。

您可以在开发过程中开展简单测试，不必等到开发周期结束才进行复杂的安全测试。换句话说，您可以将测试理念从“让我们看看该软件是否因为太糟糕而不能发布”改为“让我们来验证一下该软件，看是否一切按部就班。”

对于采用瀑布式开发方法的企业来说，这意味着将测试添加到需求挖掘、架构设计、程序编码和质量保证阶段。对于采用敏捷开发方法的企业来说，这意味着将安全性融入用户体验中，确保开发人员能够无缝发现和解决问题。

这将能够大大缩短产品发布之前的安全测试周期，让您及时知道SSI是否有效。您将不会再遇到令您措手不及、推迟产品发布、并让每个人都感到心痛的大量的安全问题。

外部视角的价值

如果您是在内部开展评估和补救工作，最好能够经常从外部视角来审视工作。外部测试合作伙伴可以为您提供专家意见，跟踪您的测试结果是否准确，以及您的底层系统能否抵御攻击。

外部应用测试供应商拥有必要的工具和手动测试策略来捕捉内部工具可能遗漏的漏洞。他们可将测试结果结合起来进行评估，以确认疑点并消除误报。最重要的是，他们可以解释测试结果，以帮助您的团队补救其发现的任何问题。

警告：不要止步于此！如果缺陷发现是SSI的唯一作用，您将永远不会取得进步。

改进

制定SSI就像1-2-3一样简单

制定SSI不是一劳永逸的活动。当您在真实的日常工作环境中执行最初的SSI结构时，会不断发现需要改进的地方。请切记，随着可供您使用的工具和技术不断改进，攻击者也在不断演进。

1. **留意模式。**如果在验证过程中不断发现相同的安全问题，您可能需要调整标准、增加培训，或者为开发人员提供更有效的工具。如果您发现漏洞是基本设计缺陷造成的，则必须追溯到设计团队来更改架构。
2. **做好构建弹性能力的准备。**您的SSI必须是富有生命力的计划，能够响应应用组合中数量和类型的变化、组织变化、合规要求变化和新出现的攻击向量。有时候，应用测试的需求会不可避免地超过您的内部能力。找到合适的测试合作伙伴可以帮助您减轻内部团队的负担，并始终对所有的应用实施一致的测试和风险控制。
3. **绘制未来发展路线图。**理想情况下，您的SSI应在所有的软件安全功能领域都具有专业能力，例如：
    - 风险与合规
    - 开源管理
    - 供应商管理
    - 安全架构设计审查
    - 应用安全测试
    - 安全代码审查
    - 缺陷管理

您无需同时培养每一项专业能力。但您需要确保一直稳步前进，并为SSI作为业务优先事项继续发展设定目标。

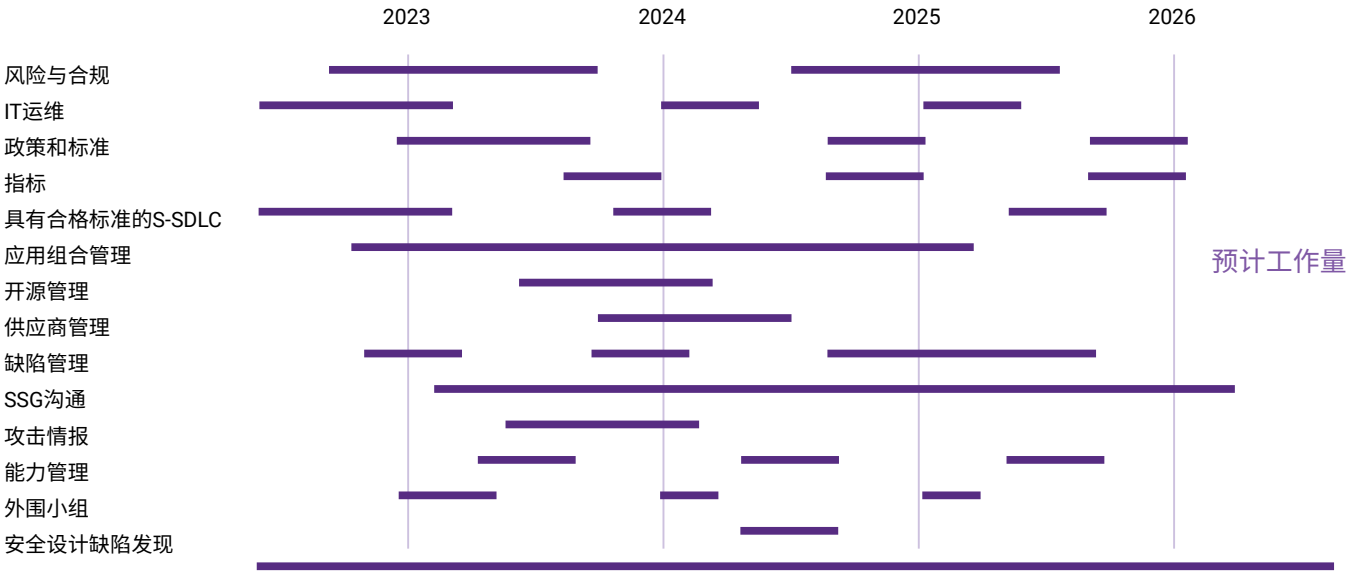
制定SSI不是一劳永逸的活动。

您必须不断地寻求模式并调整您的做法。

- 您是否需要加强培训?
- 您是否需要新的编码标准?
- 您的执行方案是否可以更有效?
- 您是否应该调整现有测试方案?

路线图示例

现在，我们来到了成功SSI的下一步，也就是最后一步：管理。



管理

读到这里，您应该已经知道有效的SSI包含很多活动，涉及很多人员和部门。作为掌舵人，您必须要把握好方向，这样你们才能始终在正确的航道上行进。

为了维护稳定的结构并深入了解每一项安全活动，您需要建立有助于实现安全目标的强大项目管理系统。

该系统应使您能够将安全活动与开发生命周期中的安全标准以及软件发布和升级时间表轻松匹配。与一般的项目管理工具相比，专用安全工具将能够为您节省时间，并确保您不会错过SSI中管理的任何关键元素。

合适的系统将使您能够跨越时间、应用类型、业务部门和特定项目来轻松比较SSI。您可以一目了然地追踪进展情况，了解可能落后于目标的地方，并确定需要额外关注的领域。

此外，您将获得及时、可操作的数据来向向公司领导层汇报。

专用安全工具能够为您节省时间，
并确保您不会错过SSI中管理的任何关键元素。

结论

每个SSI都能体现出其母公司的结构和文化。有些公司选择集中管理，有些则实行联合管理。有些公司依赖外包提供商，有些则选择雇佣新员工。有些公司依赖托管服务，有些则选择培养自己的技术团队。

这个五步流程将推动您走上成功之路：在开发周期中更好地协调所有利益相关者，展示SSI对业务目标的影响，拥有坚如磐石的长远计划。

SSI备忘单

1. 构建

- 收集有关应用组合、监管达标以及技术和业务风险领域的相关信息。
- 建立治理结构，包括得到领导层支持的责任制和政策。
- 与内部团队和第三方供应商全面沟通。
- 引入适当的内外部资源来执行SSI中定义的评估和补救活动。
- 为员工提供提升安全技能的机会，并激励他们利用这些机会。

2. 评估

- 确定与基本业务目标相关的指标，并展示持续进展。
- 将您的安全实践与软件安全构建成熟度模型 (BSIMM) 进行比较，并加入该社区。

3. 验证

- 跨越整个开发流程建立缺陷发现检查点，而不仅仅是在最后阶段。
- 将内部分析结果与外部分析结果进行比较，以确保准确性并减少误报。

4. 改进

- 确定需要额外资源、培训和持续投资的模式和领域。
- 为增强软件安全专业能力制定路线图。

5. 管理

- 设置专用的安全项目管理工具，帮助您管理和掌控SSI。
- 分析并比较团队和各类应用的表现。
- 与高级管理层和整个企业的所有利益相关者分享项目进展。

SYNOPSYS®

新思科技与众不同

新思科技提供的集成解决方案可以改变您构建和交付软件的方式，在应对业务风险的同时加速创新。与新思科技同行，您的开发人员可以在编写代码的时候快速兼顾安全。您的开发和DevSecOps团队可以在不影响速度的情况下在开发管道中自动进行安全测试。您的安全团队可以主动管理风险并将修复工作聚焦在对贵组织最重要的事情上。我们无与伦比的专业知识可以帮助您规划和执行所需安全计划。只有新思科技能够满足您构建可信软件的一切需求。

了解更多信息，请访问：www.synopsys.com/software.