SYNOPSYS®

了解您的代码组成：保护软件供应链安全

概述

数字化转型正在重塑组织机构的运作方式。无论您是销售软件的数千家公司之一，还是使用软件来运营业务的数百万家公司之一，您的创新能力以及为客户提供价值的能力都需要安全可靠的软件来驱动。这也正是为何说每家企业都是软件企业的原因。

为确保您的业务能够在当今充满挑战的市场中蓬勃发展，保证软件的质量和安全至关重要。但是，了解代码组成并不像听起来那么简单。现代应用程序的结构很复杂，涉及专有和开源代码、API和用户界面、以及应用程序行为和部署流程等元素。软件供应链的每一点都包含可能使您和您的客户面临风险的安全问题。

正如近期的《开源安全与风险分析》(OSSRA)报告所示，84%的被测代码库至少包含一个开源漏洞，74%的代码库至少包含一个高风险漏洞 — 比前一年增长了54%。此外，软件供应链攻击也变得越来越复杂，目前已经出现了将恶意软件和恶意包注入软件开发生命周期(SDLC)的攻击，这些攻击可将风险一路传递到最终用户。

有效地识别、跟踪和管理第三方代码是软件安全计划取得成功的关键，也是加强软件供应链安全的关键。然而，大多数企业购买、使用和开发的代码数量之多使得这些任务的执行难度越来越大。

企业还需将许可证合规作为软件供应链安全计划的一部分加以考虑。开源代码可能不需要任何前期成本，但却需要履行很难识别和解释的许可义务。许可证合规风险带来了其自身形式的安全漏洞。2024年的OSSRA报告指出，超过一半的代码库包含存在许可证冲突的开源代码，给那些使用开源软件但未能满足许可证要求的企业带来了诉讼。

新思科技提供全方位的软件供应链安全解决方案，用于检测、跟踪和管理源代码、容器和工件中的开源项。此外，新思科技的工具还可以帮助您评估所依赖项（软件运行所依赖的代码）是否存在安全漏洞、IP冲突、健康和质量状况欠佳以及恶意行为。

新思科技软件组成分析(SCA)解决方案使您能够导入第三方软件物料清单(SBOM)并评估其组件风险，并基于CI/CD工具集成和API以行业标准格式自动构建您的SBOM。借助这些功能，您的团队可以建立完整的软件供应链可视性，识别和降低风险，并与客户和行业要求保持一致。

以下是一些开始确保您的软件供应链和代码库安全的方法。

构建安全的代码

首先是构建安全的代码，但这比看起来更棘手。内部开发可能存在漏洞。今年的第20版OWASP Top 10列表对最常见的漏洞进行了详细介绍。例如，跨站脚本和SQL注入漏洞会对软件完整性构成巨大风险，并且几乎出现在每一年的OWASP Top 10列表中，但却因为过于复杂而无法通过手动代码检查来发现。

考虑到商用软件开发者需要对其分发给客户的软件负责，因此，安全编码实践对他们来说尤其重要。这些开发人员还必须知晓开源代码和第三方代码中的安全漏洞。

构建安全代码的几个关键点包括：

- 尽早提醒开发人员注意脆弱或不安全的编码实践，并使他们能够在未来工作中编写更安全的代码
- 在整个SDLC的各个阶段，识别软件开发项目涉及的开源和第三方组件中的已知漏洞
- 使用自动测试以及集成安全门禁和策略来加快修补速度，避免将问题推向下游
- 持续监控影响已测项目的新发布漏洞
- 检测可能已经通过受损的开源项目或SDLC引入到应用程序的恶意文件和包

防护恶意软件

攻击者越来越老练，不再满足于被动的漏洞利用攻击，而是开始主动在PyPI、GitHub和npm等常见的存储库中植入恶意软件，以进行有意的、有针对性的、巧妙的攻击。近期的ReversingLabs报告指出，2020到2023年间，通过开源软件包存储库传播的威胁增长了1300%。其中，仅2023年在PyPI平台上发现的威胁就增长了400%。备受瞩目的供应链攻击，如近期的xz Utils恶意软件事件，表明了这些威胁越来越复杂。

显然，恶意软件攻击者试图对开发团队使用的代码实施“井里投毒”。通过这种方式，他们不必等待新的漏洞出现，而是开始感染常用的代码源，使大批的组织受到影响。最常见的受害者通常是软件的最终用户。

例如，2020年的SolarWinds黑客事件便是典型的恶意软件攻击。攻击者将恶意软件注入到SolarWinds IT性能监控系统“Orion”的更新中。当客户更新其系统时，便会在不知不觉中安装后门，以便黑客通过这个后门访问用户的账户和系统文件。该问题直到波及成千上万的SolarWinds客户才被发现，给SolarWinds造成了4,000万美元的损失。

以下是保护代码库免受恶意软件攻击的几种方法。

- 在每个阶段通过集成安全测试来保护SDLC和CI管道，提供关键的安全网来检测紧急问题和恶意软件。
- 执行构建后分析，以检测恶意软件的存在，例如可疑文件，可能的多余应用和异常文件结构。
- 持续监控您生成的SBOM和您导入的SBOM，以发现机密信息泄露、恶意软件和恶意软件包。

为代码中使用AI做好准备

生成式人工智能(GenAI) 使用由大量已有代码组成的深度学习大语言模型(LLM)来创建新代码。开发人员以多种方式使用AI编码工具：有些人使用AI在键入代码时自动填充和完成代码，另一些则将代码注释作为提示语，使用AI构建完整的方法或功能。

随着GenAI的兴起，人们越来越期望它生成的代码不会出现许可证问题、漏洞和错误。但事实正好相反。因为用于训练GenAI的代码是不完美的，因此它生成的代码也是不完美的。如前所述，OSSRA报告显示84%的代码库存在漏洞，53%的代码库存在许可证冲突。此外，AI工具通常缺乏整个程序的重要背景信息，这也可能引入安全漏洞。

GenAI代码面临的潜在挑战包括：

- 因缺乏相关许可信息而无意中采用受许可保护的代码，从而引发知识产权冲突
- 引入镜像人类开发人员典型安全漏洞的代码

源代码安全问题，如WASP Top 10列表中的问题，可能很复杂，很难通过手动审查发现。这也正是为什么大多数开发团队都使用静态分析测试工具的原因，因为这些工具可以作用于整个应用程序，收集信息流的上下文，并发现可能导致漏洞的缺陷。您应该像对待其他代码一样，对AI生成的源代码进行安全漏洞检查。

尽管您有理由对GenAI代码的使用保持谨慎，但没有理由因为恐惧这些风险而拒绝采用AI生成的代码。新思科技提供几种方法，可以帮助您在管理风险的同时获得AI生成代码的好处。

- Black Duck® SCA代码片段分析：GenAI工具可能会引入缺乏许可证信息或未包含在清单文件中的开源代码片段、或其他受许可证保护的代码片段，Black Duck® SCA代码片段分析解决方案可以帮助开发和测试团队找到这些代码片段。
- 新思科技静态分析：可以帮助工作团队发现并修复由开发人员和AI助手编写的源代码中的安全和质量缺陷。
- 新思科技的其他应用安全测试解决方案：可以帮助工作团队确保他们构建和交付给客户和用户的软件是安全、可信的。

新思科技如何提供帮助

新思科技是唯一一家拥有全面产品组合的供应商，提供对软件供应链的完整可视性，使您能够据此采取行动，并通过轻松生成SBOM而使您能够永久性采取行动。因此，您可以向客户证明您所构建的应用程序是安全的，并在尽职尽责地管理和识别软件供应链风险，从而赢得客户的信任。

进一步了解新思科技如何能够帮助您的团队跨越整个SDLC来有效管理供应链安全。

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补救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。

如想了解有关Synopsys Software Integrity Group的更多信息，请访问：www.synopsys.com/software.

SYNOPSYS®

了解您的代码组成：保护软件供应链安全

概述

数字化转型正在重塑组织机构的运作方式。无论您是销售软件的数千家公司之一，还是使用软件来运营业务的数百万家公司之一，您的创新能力以及为客户提供价值的能力都需要安全可靠的软件来驱动。这也正是为何说每家企业都是软件企业的原因。

为确保您的业务能够在当今充满挑战的市场中蓬勃发展，保证软件的质量和安全至关重要。但是，了解代码组成并不像听起来那么简单。现代应用程序的结构很复杂，涉及专有和开源代码、API和用户界面、以及应用程序行为和部署流程等元素。软件供应链的每一点都包含可能使您和您的客户面临风险的安全问题。

正如近期的《开源安全与风险分析》(OSSRA)报告所示，84%的被测代码库至少包含一个开源漏洞，74%的代码库至少包含一个高风险漏洞 — 比前一年增长了54%。此外，软件供应链攻击也变得越来越复杂，目前已经出现了将恶意软件和恶意包注入软件开发生命周期(SDLC)的攻击，这些攻击可将风险一路传递到最终用户。

有效地识别、跟踪和管理第三方代码是软件安全计划取得成功的关键，也是加强软件供应链安全的关键。然而，大多数企业购买、使用和开发的代码数量之多使得这些任务的执行难度越来越大。

企业还需将许可证合规作为软件供应链安全计划的一部分加以考虑。开源代码可能不需要任何前期成本，但却需要履行很难识别和解释的许可义务。许可证合规风险带来了其自身形式的安全漏洞。2024年的OSSRA报告指出，超过一半的代码库包含存在许可证冲突的开源代码，给那些使用开源软件但未能满足许可证要求的企业带来了诉讼。

新思科技提供全方位的软件供应链安全解决方案，用于检测、跟踪和管理源代码、容器和工件中的开源项。此外，新思科技的工具还可以帮助您评估所依赖项（软件运行所依赖的代码）是否存在安全漏洞、IP冲突、健康和质量状况欠佳以及恶意行为。

新思科技软件组成分析(SCA)解决方案使您能够导入第三方软件物料清单(SBOM)并评估其组件风险，并基于CI/CD工具集成和API以行业标准格式自动构建您的SBOM。借助这些功能，您的团队可以建立完整的软件供应链可视性，识别和降低风险，并与客户和行业要求保持一致。

以下是一些开始确保您的软件供应链和代码库安全的方法。

构建安全的代码

首先是构建安全的代码，但这比看起来更棘手。内部开发可能存在漏洞。今年的第20版OWASP Top 10列表对最常见的漏洞进行了详细介绍。例如，跨站脚本和SQL注入漏洞会对软件完整性构成巨大风险，并且几乎出现在每一年的OWASP Top 10列表中，但却因为过于复杂而无法通过手动代码检查来发现。

考虑到商用软件开发者需要对其分发给客户的软件负责，因此，安全编码实践对他们来说尤其重要。这些开发人员还必须知晓开源代码和第三方代码中的安全漏洞。

构建安全代码的几个关键点包括：

- 尽早提醒开发人员注意脆弱或不安全的编码实践，并使他们能够在未来工作中编写更安全的代码
- 在整个SDLC的各个阶段，识别软件开发项目涉及的开源和第三方组件中的已知漏洞
- 使用自动测试以及集成安全门禁和策略来加快修补速度，避免将问题推向下游
- 持续监控影响已测项目的新发布漏洞
- 检测可能已经通过受损的开源项目或SDLC引入到应用程序的恶意文件和包

防护恶意软件

攻击者越来越老练，不再满足于被动的漏洞利用攻击，而是开始主动在PyPI、GitHub和npm等常见的存储库中植入恶意软件，以进行有意的、有针对性的、巧妙的攻击。近期的ReversingLabs报告指出，2020到2023年间，通过开源软件包存储库传播的威胁增长了1300%。其中，仅2023年在PyPI平台上发现的威胁就增长了400%。备受瞩目的供应链攻击，如近期的xz Utils恶意软件事件，表明了这些威胁越来越复杂。

显然，恶意软件攻击者试图对开发团队使用的代码实施“井里投毒”。通过这种方式，他们不必等待新的漏洞出现，而是开始感染常用的代码源，使大批的组织受到影响。最常见的受害者通常是软件的最终用户。

例如，2020年的SolarWinds黑客事件便是典型的恶意软件攻击。攻击者将恶意软件注入到SolarWinds IT性能监控系统“Orion”的更新中。当客户更新其系统时，便会在不知不觉中安装后门，以便黑客通过这个后门访问用户的账户和系统文件。该问题直到波及成千上万的SolarWinds客户才被发现，给SolarWinds造成了4,000万美元的损失。

以下是保护代码库免受恶意软件攻击的几种方法。

- 在每个阶段通过集成安全测试来保护SDLC和CI管道，提供关键的安全网来检测紧急问题和恶意软件。
- 执行构建后分析，以检测恶意软件的存在，例如可疑文件，可能的多余应用和异常文件结构。
- 持续监控您生成的SBOM和您导入的SBOM，以发现机密信息泄露、恶意软件和恶意软件包。

为代码中使用AI做好准备

生成式人工智能(GenAI) 使用由大量已有代码组成的深度学习大语言模型(LLM)来创建新代码。开发人员以多种方式使用AI编码工具：有些人使用AI在键入代码时自动填充和完成代码，另一些则将代码注释作为提示语，使用AI构建完整的方法或功能。

随着GenAI的兴起，人们越来越期望它生成的代码不会出现许可证问题、漏洞和错误。但事实正好相反。因为用于训练GenAI的代码是不完美的，因此它生成的代码也是不完美的。如前所述，OSSRA报告显示84%的代码库存在漏洞，53%的代码库存在许可证冲突。此外，AI工具通常缺乏整个程序的重要背景信息，这也可能引入安全漏洞。

GenAI代码面临的潜在挑战包括：

- 因缺乏相关许可信息而无意中采用受许可保护的代码，从而引发知识产权冲突
- 引入镜像人类开发人员典型安全漏洞的代码

源代码安全问题，如WASP Top 10列表中的问题，可能很复杂，很难通过手动审查发现。这也正是为什么大多数开发团队都使用静态分析测试工具的原因，因为这些工具可以作用于整个应用程序，收集信息流的上下文，并发现可能导致漏洞的缺陷。您应该像对待其他代码一样，对AI生成的源代码进行安全漏洞检查。

尽管您有理由对GenAI代码的使用保持谨慎，但没有理由因为恐惧这些风险而拒绝采用AI生成的代码。新思科技提供几种方法，可以帮助您在管理风险的同时获得AI生成代码的好处。

- Black Duck® SCA代码片段分析：GenAI工具可能会引入缺乏许可证信息或未包含在清单文件中的开源代码片段、或其他受许可证保护的代码片段，Black Duck® SCA代码片段分析解决方案可以帮助开发和测试团队找到这些代码片段。
- 新思科技静态分析：可以帮助工作团队发现并修复由开发人员和AI助手编写的源代码中的安全和质量缺陷。
- 新思科技的其他应用安全测试解决方案：可以帮助工作团队确保他们构建和交付给客户和用户的软件是安全、可信的。

新思科技如何提供帮助

新思科技是唯一一家拥有全面产品组合的供应商，提供对软件供应链的完整可视性，使您能够据此采取行动，并通过轻松生成SBOM而使您能够永久性采取行动。因此，您可以向客户证明您所构建的应用程序是安全的，并在尽职尽责地管理和识别软件供应链风险，从而赢得客户的信任。

进一步了解新思科技如何能够帮助您的团队跨越整个SDLC来有效管理供应链安全。

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补救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。

如想了解有关Synopsys Software Integrity Group的更多信息，请访问：www.synopsys.com/software.