BLACKDUCK®

在CISA的六类SBOM中，哪一类最适合您？

软件物料清单(SBOM)远非表面看起来那么简单

虽然业界对SBOM内容的最低要求早已达成一致，但网络安全和基础设施安全局(CISA)还是将SBOM分成了具体的六种类型。大部分情况下，每类SBOM都是在软件开发生命周期(SLDC)的某个阶段创建的，反映了软件在那一时刻的构成状态。

究其根本，SBOM就是一个列出软件所包含的各种成分的清单。CISA定义这些SBOM类型的原因之一是为组织机构提供更多信息，使他们能够了解软件在这些不同时刻的构成情况。但这也意味着组织机构必须弄清楚在哪种情况下应该构建哪种SBOM，以及构建SBOM的目的是什么。

在本指南中，“软件”一词应理解为一个功能齐全的应用，而SDLC则是用于讨论CISA定义的这六类SBOM的框架。

六种类型SBOM的定义

下面简要介绍不同类型的SBOM及其各自的优缺点。我们以SDLC作为组织原则，但要记住，有些SBOM类型可能适用于生命周期的多个阶段，而有些则只适用于某一阶段。此外，任何 SBOM 类型中显示的数据可能会有所不同，具体取决于软件的生命周期阶段和所属的行业。

设计型SBOM (Design SBOM)

- “设计型SBOM”是描述预期和计划的软件项目或产品的清单，它包含了用于创建新的软件构件的各种组件— 其中有些组件可能还没有实现。这些信息通常来自设计规范、招标书或初始概念，需要人工编制。
- 这种类型的SBOM通常没有最终应用中会包含的许多依赖项。但它可以帮助工作团队提前发现和解决可能出现的问题，从而规划好工作流程。

源码型SBOM (Source SBOM)

- “源码型SBOM”是基于开发环境中的源文件和依赖项直接创建的清单，用于描述构建产品构件所需的软件成分。通常，它由软件组成分析(SCA)工具自动生成，但也需要人工进行一些说明和补充。
- 这种类型的SBOM是在无法查看完整构建或运行态程序的情况下创建的，因此可能缺少生命周期后期的依赖项，甚至包含不相关的依赖项。

构建型SBOM (Build SBOM)

- “构建型SBOM”是在构建过程中生成的，它包含了构建产品构件所需的数据，如源文件、依赖项、构建组件和临时构建过程数据等。这类SBOM是在构建阶段完全自动创建的，遵循常规的配置操作。这类SBOM中包含了所有可用的元素，包括第三方SBOM、源文件、代码和构建组件，而且还集成了中间的“构建型SBOM”和“源码型SBOM”。
- 因为这种类型的SBOM中包含源代码之外的依赖项，因此能够准确反映已部署的项目的构成。在这个阶段创建的SBOM包括其他SBOM，因此可以集成中间的“构建型SBOM”和“源码型SBOM”，形成最终发布的构件SBOM。工作团队还可以选择在这个阶段签署SBOM，以实现安全的交付。
- 但是，这类SBOM需要大量的配置工作才能与构建工具集成。为此，一些团队可能需要调整其构建过程。

分析型SBOM (Analyzed SBOM)

- “分析型SBOM”是在构建软件后，通过对软件中的各种构件（例如可执行文件、包、容器和虚拟机镜像）进行分析而生成的。这种分析通常需要用到多种启发式方法。某些情况下，“分析型SBOM”也可以称为“第三方SBOM”，因为对软件构件的分析是使用第三方工具完成的。
- 这种类型的SBOM需要一个二进制分析工具，自动或手动工具都可以。这种工具不需要访问源代码或构建系统。创建这类SBOM是为了建立对内部开发的软件的可视性，或者验证供应商或者软件制作商提供的SBOM。它还可以发现其他SBOM生成工具在不同阶段无法检测到的依赖项。因为“分析型SBOM”依赖启发式方法和上下文，因此比较容易出现版本号不准确或遗漏的情况。

部署型SBOM (Deployed SBOM)

- “部署型SBOM”提供运行在已部署的系统上的软件清单。它可能由其他SBOM组合而成，例如，它可以在（模拟）或真实部署环境中对配置选项和执行行为进行分析。
- 这种类型的SBOM是通过手动检查系统上安装和运行的软件而编制的。这需要手动操作，因此，工作团队必须考虑SBOM提供的信息和构件的配置信息，然后必须执行应用的行为。这可以由软件提供商在模拟环境中完成，也可以由操作人员在真实或模拟环境中完成。
- “部署型SBOM”中可以包括软件实际运行的环境，但是，准确、完整地获取这些信息可能有困难，并且很多依赖项可能存在于无法访问的代码中。

运行时SBOM (Runtime SBOM)

- “运行时SBOM”是通过对运行软件的系统进行检测而生成的，检测目的是捕捉系统中存在的组件以及外部调用或动态加载的组件。某些情况下，“运行时SBOM”也可以称为“检测型SBOM”或“动态型SBOM”，因为它通常是使用动态分析工具对运行中的应用执行“黑盒”测试而生成的。
- 这种类型的SBOM可以剔除无关信息，并找出哪些依赖项应该优先评估。对运行中的应用进行此类分析需要大量开销，并且可能需要很长时间和很多测试用例才能呈现应用的所有功能。要使这类SBOM可靠和准确，您必须探索应用的每一个深层、隐秘的角落，这在没有应用架构知识的情况下可能很难做到。

如何确定哪类SBOM最适合您

一般来说，“构建型SBOM”或“分析型SBOM”可以帮助工作团队实现准确性和效率的平衡。SBOM的目的是揭示软件的组成，以帮助识别应用依赖项中的风险，因此，准确性对于软件构建者和使用者都至关重要。

“构建型SBOM”通常是软件构建者的首选。它们可以让SBOM的生成与SDLC直接集成，以自动生成SBOM，从而在每个工件版本的整个生命周期中都能构建精确的SBOM。

“分析型SBOM”可由构建者生成，以便更深入、更具体地了解其向消费者提供的软件的情况。使用者也可以自己生成“分析型SBOM”，以获得有关应用组成的可靠信息，而无需访问源代码或构建细节。这意味着“分析型SBOM”的结果可以让构建者和使用者进行协作和沟通，例如在必要时讨论差异。

“构建型SBOM”或“分析型SBOM”还有助于满足大多数行业的要求。当结合在一起时，这些SBOM中包括开源码依赖项、专有代码、基础镜像、固件、操作系统和应用可能需要的任何第三方库。由于这些类型的SBOM需要工具和自动生成，因此，您可以自定义它们的生成方式和时间，并指定SBOM需要包含的字段、生成格式和生成时间。

此外，“构建型SBOM”或“分析型SBOM”还使您能够满足国家电信和信息管理局(NTIA)的最低SBOM要求，该要求现已成为SBOM的事实标准，即使在公共部门之外也是如此。这意味着如果您是软件制作者，则可以满足客户需求。如果您是软件使用者，则可以开始明确定义您对供应商的要求，并开始控制自己的软件供应链。

如何开始管理SBOM

了解了SBOM的类型之后，问题来了：如何管理所有这些SBOM呢？

必不可少的工具

这离不开优秀的SCA工具。组织机构对SBOM的生成和使用有许多要求，确定如何对它们进行优先级排序可能是一个挑战。由于SBOM提供了对软件供应链的可视性来帮助识别和管理应用的风险，因此，使用SCA工具可以帮助您建立可视性，并将其与风险相映射。

最全面的SCA工具可以发现应用、源代码、文件、构建构件、容器镜像、库和固件等对象中的依赖项。虽然SCA主要用于检测开源依赖项，但有些工具也允许工作团队开发和识别专有或商业依赖项。这种分析可以生成一个完整的SBOM。

SCA工具还提供数据源，使工作团队能够将依赖项与风险相关联，从而可以根据三个主要的风险考虑因素对其进行评估。

- 安全性
  - 是否超过了漏洞严重性的阈值？
  - 是否符合OWASP/SANS标准？
  - 漏洞的可利用性、可修复性和可达性如何？
- 合规性
  - 每个许可证有哪些义务？
  - 是否有任何许可证与最终应用的许可方式相冲突？
  - 是否有任何许可证在批准或禁止列表上？
- 构件健康度
  - 构件是否有活跃的贡献者？
  - 构件的安全信誉如何？
  - 这是不是构件的最新版本？

建立流程

许多软件使用者都为他们自己的客户制作软件，并且有义务提供SBOM。虽然这可以手动完成，但最佳做法是将SBOM生成集成到构建系统中，并使用API自动检索每次修改或新构建时更新的SBOM。这样就可以生成机器可读的SBOM，从而能够将SBOM导入到SCA工具中，以便您能够及时、持续地评估依赖项在安全性、许可证和质量方面的风险。

最后，您应将SBOM创建视为一个过程，而不仅仅是一个文档。任何一个SBOM都会列出应用的组成，但是将SBOM创建看作是一种方法，可以实现动态的供应链可视性和上游风险管理。

将SBOM视为一个过程意味着您应该：

- 关注SBOM中需要包括哪些内容，多久生成一次SBOM，以及使用哪些技术来管理SBOM。
- 学习如何导入SBOM。它们可以导入到应用安全态势管理工具、SCA工具，甚至数据库中 — 以及任何能够让您汇总多个SBOM并最终将依赖关系与产品组合中所有应用的风险相关联的任何工具。
- 需要SBOM具有可操作性。许多组织机构都要求软件供应商提供SBOM，但却不能评估或使用它们来降低风险。
- 为SBOM建立您自己的托管链。托管链是一种证明机制，可用作产品生命周期和过程的可验证的记录。
- 与重要的利益相关者安全地共享SBOM，并在整条托管链中保护其完整性。
- 启用SBOM搜索和查询功能，以便您能够在下一个轰动性的漏洞被曝光时，了解您的暴露情况。

Black Duck如何提供帮助

在SBOM的生成和管理方面，并没有万能的方法或解决方案。不同团队有不同资源和风险偏好，这决定了他们需要或能够生成的SBOM的类型。这可能让团队感到迷茫，不知道如何入手。如果工作团队能够关注本文所述的SBOM管理方法的核心要素，便可以朝着正确的方向前进，根据自己的情况制定一个完善、个性化的策略。

Black Duck提供一系列满足SBOM管理基本需求的工具和服务，可以帮助工作团队快速开始管理SBOM。我们的SCA工具能够识别应用的依赖项，生成第一方SBOM，导入第三方SBOM，发现依赖风险，并指导修复，且所有这些都提供了统一的用户体验。这使得软件构建者和使用者都能建立供应链可视性，并采取措施识别和减轻风险。

Black Duck也认识到，工具只是解决方案的一部分。为了帮助客户将SBOM从一个文档转变为一个高效的流程，我们利用专业知识和咨询服务来了解客户的特殊情况，并帮助制定完整的SBOM管理策略。

Black Duck与众不同

Black Duck® 提供业界最全面、最强大、最值得信赖的应用安全解决方案组合。我们拥有无与伦比的专业知识和经验，来帮助世界各地的组织机构快速保护其软件，在其开发环境中高效集成安全性以及使用新技术进行安全创新。作为软件安全领域公认的领导者、专家和创新者，Black Duck拥有您构建可信软件所需的一切。如预了解更多信息，请访问www.blackduck.com。