SYNOPSYS®

在CISA 的六類SBOM中，哪一類最適合您？

軟體物料清單(SBOM) 遠非表面看起來那麼簡單

雖然業界對SBOM內容的最低要求早已達成一致，但網路安全與基礎建設安全局 (CISA) 還是將 SBOM 分成了具體的六個類型。大部分情況下，每類SBOM都是在軟體開發生命週期 (SLDC) 的某個階段建立的，反映了軟體在那一時刻的構成狀態。

究其根本，SBOM 就是一個列出軟體所包含的各種成分的清單。CISA 定義這些 SBOM 類型的原因之一是為組織機構提供更多訊息，使他們能夠了解軟體在這些不同時刻的構成狀況。但這也意味著組織機構必須弄清楚在哪種情況下應該建構哪種SBOM ，以及建構 SBOM 的目的是什麼。

在本指南中，"軟體"一詞應理解為一个功能齊全的應用，而SDLC 則是用於討論CISA定義的這六類SBOM的框架。

六種類型SBOM的定義

下面簡要介紹不同類型的SBOM及其各自的優缺點。我們以SDLC作為組織原則，但要記住有些 SBOM類型可能適用於生命週期的多個階段。而有些則只適用於某一階段。此外，任何SBOM類型中顯示的數據可能會有所不同，具體取決於軟體的生命週期階段和所屬的行業。

設計型SBOM (Design SBOM)

- "設計型SBOM"是描述預期和計劃的軟體項目或產品的清單，它包含了用於建構新的軟體元件的各種組件 -- 其中有些組件可能還沒有實現。這些訊息通常來自設計規範、招標書或初始概念，需要人工編制。
- 這種類型的SBOM通常沒有最終應用中會包含的許多依賴項。但它可以幫助工作團隊提前發現和解決可能出現的問題，從而規劃好工作流程。

源碼型SBOM (Source SBOM)

- "源碼型SBOM"是基於開發環境中的源文件和依賴項直接建立的清單，用於描述建構產品元件所需的軟體成分。通常，它由軟體組成分析(SCA) 工具自動生成，但也需要人工進行一些說明與補充。
- 這種類型的SBOM是在無法查看完整建立或運行態程序的情況下建立的，因此可能缺少生命週期後期的依賴項，甚至包含不相關的依賴項。

建構型SBOM (Build SBOM)

- “建構型SBOM”是在建構過程中產生的，它包含了建構產品元件所需的資料，如源文件、依賴項、建構組件和臨時建構過程資料等。這類SBOM是在建構階段完全自動建立的，遵循常規的配置操作。這類SBOM中包含了所有可用的元素，包括第三方SBOM、源文件、代碼和建構組件，而且還整合了中間的“建構型SBOM”和”源碼型SBOM “。
- 因為這種類型的SBOM中包含源代碼之外的依賴項，因此能準確反映已部署的項目的構成。在這個階段建立的SBOM包括其他SBOM，因此可以整合中間的“建構型SBOM”和”源碼型SBOM “，形成最終發布的元件SBOM。工作團隊還可以選擇在這個階段簽署SBOM，以實現安全的交付。
- 但是，這類SBOM需要大量的配置工作才能與建構工具整合。為此，一些團隊可能需要調整其建構過程。

分析型SBOM (Analyzed SBOM)

- “分析型SBOM”是在建構軟體後，通過軟體中的各種元件(例如可執行文件、套件包、容器和虛擬機鏡像)進行分析而產生的。這種分析通常需要用到多種啟發式方法。某些情況下，“分析型SBOM”也可以稱為“第三方SBOM，因為對軟體元件的分析是使用第三方工具完成的。
- 這種類型的SBOM需要一个二進制分析工具，自動或手動工具都可以。這種工具不需要使用原始碼或建構系統。建構這類SBOM是是為了建立對內部開發的軟體的可視性，或者驗證供應商或者軟體製作商提供的SBOM。它還可以發現其他SBOM產生工具在不同階段無法檢測到的依賴項。因為“分析型SBOM”依賴啟發式方法和上下文，因此比較容易出現版本號碼不準確或遺漏的情況。

部署型SBOM (Deployed SBOM)

- “部署型SBOM”提供運行在已部署的系統上的軟體清單。它可能由其他SBOM組合而成，例如它可以在(模擬)或真實部署環境中對配置選項和執行行為進行分析。
- 這種類型的SBOM是透過手動檢查系統上安裝和運行的軟體而編制的。 這需要手動操作，因此工作團隊必須考慮SBOM提供的訊息和元件的配置訊息
- “部署型SBOM”中可以包括軟體實際運行的環境，但是準確、完整地獲取這些訊息可能有困難，並且很多依賴項可能存在於無法訪問的代碼中。

運行時SBOM (Runtime SBOM)

- “運行時SBOM”是透過對運行軟體的系統進行檢測而產生的，檢測目的是捕捉系統中存在的組件以及外部呼叫或動態加載的組件。某些情況下，“運行時SBOM”也可以稱為“檢測型SBOM”或“動態型SBOM”，因為它通常使用動態分析工具對運行中的應用執行“黑盒”測試而產生的。
- 這種類型的SBOM可以剔除無關訊息，並找出哪些依賴項應該優先評估。對運行中的應用進行此類分析需要大量開銷，並且可能需要很長時間和很多測試案例才能呈現應用的所有功能。要使這類SBOM可靠和準確，您必須探索應用的每一個深層、隱密的角落，這在沒有應用架構知識的情況下可能很難做到。

如何確定哪類SBOM最適合您

一般來說 “建構型SBOM”或“分析型SBOM”可以幫助工作團隊實現準確性和效率的平衡。 SBOM的目的是揭示軟體的組成，以幫助識別應用依賴項中的風險，因此，準確性對於軟體建構者和使用者都至關重要。

“建構型SBOM”通常是軟體建構者的首選。 它們可以讓SBOM的產生與SDLC 直接整合，以自動產生 SBOM。從而在每個工作版本的整個生命週期中都能建構精確的SBOM。

“分析型SBOM”可由建構者產生，以便更深入、更具體地了解其向消費者提供的軟體情況。使用者也可以自己產生 “分析型SBOM” ，以獲得有關應用組成的可靠訊息，而無需使用原始碼或建構細節。這意味著分析型SBOM” 的結果可以讓建構者和使用者進行協作和溝通，例如在必要時討論差異。

“建構型SBOM”或“分析型SBOM”還有助於滿足大多數行業的要求。當結合在一起時，這些SBOM中包括開源碼依賴項、專有代碼、基礎鏡像、韌體、操作系統和應用可能需要的任何第三方庫。由於這些類型的SBOM需要工具和自動產生，因此您可以自定義它們的產生方式和時間，並指定SBOM需要包含的字段、產生格式和產生時間。

此外，“建構型SBOM”或“分析型SBOM”還使您能夠滿足國家電信和訊息管理局(NTIA)的最低SBOM要求，該要求現已成為 SBOM的事實標準，即使在公共部門之外也是如此。這意味著如果您是軟體製造者，則可滿足客戶需求。如果您是軟體使用者，則可以開始明確定義您對供應商的要求，並開始控制自己的軟體供應鏈。

如何開始管理SBOM

了解了SBOM的類型之後，問題來了：如何管理所有這些SBOM 呢？

必不可少的工具

這離不開優秀的SCA工具。組織機構對SBOM的產生和使用有許多要求，確定如何對它們進行優先級排序可能是一個挑戰。由於SBOM提供了對軟體供應鏈的可視性來幫助識別和管理應用的風險，因此SCA工具可以幫助您建立可視性，並將其與風險相對應。

最全面的SCA 工具可以發現應用、原始碼、文件、建構元件、容器鏡像、元件庫和韌體等對象中的依賴項。雖然SCA主要用於檢測開源依賴項，但有些工具也允許工作團隊開發和識別專有或商業依賴項。這種分析可以生成一個完整的SBOM。

SCA工具還提供資料來源，使工作團隊能夠將依賴項與風險相關，從而可以根據三個主要的風險考慮因素對其進行評估。

- 安全性
  - —是否超過了漏洞嚴重性的閾值？
  - —是否符合OWASP/SANS 標準？
  - —漏洞的可利用性 、可修復性和可達性如何？
- 合規性
  - —每個授權型態有哪些義務？
  - —是否有任何授權型態與最終應用的許可方式相衝突？
  - —是否有任何授權型態在批准或禁止列表上？
- 開源元件健康度
  - —元件是否有活躍的貢獻者？
  - —元件的安全信譽如何？
  - —這是不是元件的最新版本？

建立流程

許多軟體使用者都為他們自己的客戶製作軟體，並且有義務提供 SBOM。雖然這可以手動完成，但最佳做法是將 SBOM 的產生整合到建構系統中，並使用 API 自動檢索每次修改或新建立時更新的 SBOM。這樣就可以產生機器可讀的SBOM，從而能夠將SBOM導入到SCA工具中，以便您能夠及時、持續地評估依賴項在安全性、授權合規和品質方面的風險。

最後，您應將SBOM建立視為一個過程，而不僅僅是一個檔案。任何一個 SBOM都會列出應用的組成。但是將 SBOM建立看作是一種方法，可以實現動態的供應鏈可視性和上游風險管理。

將SBOM視為一個過程意味著您應該：

- 關注SBOM中需要包括哪些內容，多久產生一次 SBOM，以及使用哪些技術來管理 SBOM。
- 學習如何導入SBOM。它們可以導入到應用安全態勢管理工具、SCA工具，甚至資料庫中---以及任何能夠讓您彙整多個SBOM並最終將依賴關係與產品組合中所有應用的風險相關連的任何工具。
- 需要SBOM具有可操作性。許多組織機構都要求軟體供應商提供SBOM，但卻不能評估或使用它們來降低風險。
- 為SBOM建立您自己的託管鏈。託管鏈是一種證明機制，可用作產品生命週期和過程的可驗證的紀錄。
- 與重要的利益相關者安全地共享SBOM，並在整條託管鏈中保護其完整性。
- 啟用SBOM搜尋和查詢功能，以便您能夠在下一個轟動性的漏洞被曝光時，了解您的暴露情況。

新思科技與達友科技如何提供幫助

在SBOM的生成和管理方面，並沒有萬能的方法或解決方案。不同團隊有不同資源和風險偏好，這決定了他們需要或能夠產生的SBOM的類型。這可能讓團隊感到迷茫，不知道如何入手。如果工作團隊能夠關注本文所述的SBOM管理方法的核心要素，便可以朝著正確的方向前進，根據自己的情況制定一個完善、個性化的策略。

達友科技提供一系列滿足SBOM管理基本需求的工具和服務，可以幫助工作團隊快速開始管理SBOM。我們的SCA工具能夠識別應用的依賴項，產生第一方SBOM，導入第三方SBOM，發現依賴風險，並指導修復，且所有這些都提供了統一的用戶體驗。這使得軟體建構者和使用者都能建立供應鏈可視性，並採取措施識別和減輕風險。

達友科技也很清楚工具只是解決方案的一部分。為了幫助客戶將SBOM從一個檔案轉變為一個高效的流程，我們利用專業知識和諮詢服務來了解客戶的特殊情況，並幫助制定完整的SBOM管理策略。

docutek 達友科技

Synopsys 台灣代理商：達友科技股份有限公司
聯絡電話：02-2658-8970
聯絡信箱：contact@docutek.com.tw

新思科技與眾不同

新思科技提供的整合解決方案可以改變您建構和交付軟體的方式，在應對業務風險的同時加速創新。與新思科技同行，您的開發人員可以在編寫代碼的時候快速兼顧安全。您的開發和DevSecOps團隊可以在不影響速度的情況下在開發管道中自動進行安全測試。您的安全團隊可以主動管理風險並將補救工作聚焦在對貴組織最重要的事情上。我們無與倫比的專業知識可以幫助您規劃和執行所需安全計劃。只有新思科技能夠滿足您建構可信賴軟體的一切需求。

如想了解有關 Synopsys Software Integrity Group 的更多訊息，請訪問：www.synopsys.com/software.