安全需求不一而足

支援軟體供應鏈安全所需的 10 大類安全工具

軟體供應鏈安全正在迅速發展，如果資安長只關注軟體供應鏈安全和軟體物料清單，那麼他們只能得到因應問題的部分解決方案。我們在此專為軟體供應鏈安全解決方案堆疊之規劃提供了一份入門檢查清單。

文／Ericka Chickowski　譯／酷魯

隨著安全領導者在建立軟體供應鏈安全計畫方面取得進展，他們在可用工具上面臨了好壞摻半的消息：相關技術正在朝向好或壞的面向迅速發展。

快速發展之軟體供應鏈安全技術的好消息是，創新的快速步伐提供了越來越多的機會，可以獲得對軟體組合中大量元件和程式碼的更高可視性和透明度。

然而壞消息是，實驗和創新同時朝著許多不同的方向發展，這使得整個可用工具的狀況就好比是一個令人困惑的混合體（由全新且不斷新增的首字母縮寫類別與利基產品混雜而成）。

其中一些是更傳統的應用程式安全工具，它們在朝向更開發人員友善的方向發展。還有一些是傳統的開發工具，它們增加了以安全為中心的控制機制和功能，以便能有效應對供應鏈風險的挑戰。還有一些工具來自開發安全營運（DevSecOps）領

域，其旨在促進這些社群之間的相互協作。

「人們對軟體供應鏈安全很難有一番清晰的認識，原因之一就在於供應鏈中有很多環節很可能出錯，」美國網路安全獨角獸公司 Tanium 產品顧問 Tom Goings 告訴我們。「你可能會將有安全漏洞的東西直接引進到軟體中，就像幾年前知名的 SolarWinds 供應鏈攻擊案例那樣、也可能是 Log4j 等充滿安全漏洞的共用函式庫，甚至可能是受劫持的憑證授權中心（CA）之類的安全漏洞。」

軟體供應鏈安全沒有絕對標準

雖然市場上已有一些軟體供應鏈安全產品堆疊和平台開始進行整合，但這些產品的功能組合卻依舊五花八門、天差地遠。

這些平台主要鎖定的核心工具類別偏向於軟體組成分析（Software Composition Analysis，SCA）以及專門生成軟體物料清單（Software Bills of Materials，SBOMs）的工具，亦即現代軟體所謂的「成分清單」（ingredient list）。雖然軟體組成分析和軟體物料清單往往是許多軟體供應鏈安全工具的骨幹支柱，但對於試圖構建路線圖以支持管理供應鏈風險之全面計畫的資安長來說，這真的只不過是冰山的一角。

「當人們關注供應鏈安全時，他們會將重點聚焦在使用軟體組成分析之類的工具上，他們並同時關注軟體物料清單，」Gartner 應用安全資深總監暨分析師 Dale Gardner 接受採訪時表示。「這些都是這方面解決方案中非常重要的部分。但它們實際上只是一種非常不全面的解決方案。」

事實較全面性的解決方案還涉及了許多其他的運作組件，包括機密管理、依存關係對應（dependency mapping）和管理、持續整合/持續交付管道安全性（CI/CD pipeline security）、有效的儲存庫管理等等。大多數專家都認為，安全團隊很難從一家供應商那裡找到他們所需要的一切。

諮詢顧問公司 Coalfire 應用安全資深經理 Michael Born 解釋說：「我認為，沒有一家供應商能夠以滿足所有組織需求的方式處理與軟體供應鏈安全相關的所有挑戰。」他進一步指出，缺乏整合並不一定是件壞事。「這可能會使組織陷入所謂「供應商鎖定」（vendor lock-in）相關的風險，並且意味著組織成熟或應變的速度比供應商能夠跟上的速度更快。」

軟體供應鏈 10 大類安全工具：

1. 軟體組成分析和軟體物料清單生成
2. 程式碼掃描和滲透測試
3. 軟體物料清單的豐富化和聚集
4. 機密管理
5. 依存關係管理和對應
6. 受信任的儲存庫和註冊表
7. 安全程式碼簽章
8. 持續整合 / 持續交付管道安全性
9. 第三方風險管理平台
10. 基礎設施即程式碼安全和雲端原生應用程式保護平台

這種解決方案的分散性不僅是來自多個不同技術觀點（以開發為導向的工具、以營運為導向的工具、以安全為導向的工具）的有機創新結果，而且還因為需要解決各種不同的使用案例與情況所致。

「我們必須非常具體地瞭解我們正在談論的風險或使用案例，以便能夠找到合適的軟體解決方案或整體解決方案堆疊來解決這些問題，」德勤（Deloitte）網路風險服務業務的網路風險安全供應鏈負責人 Sharon Chand 解釋道。「因為我所需要的解決方案類型將完全取決於我在軟體供應鏈安全場景中所處的位置而定。如果我是一個軟體的生產者，那麼我所需要的解決方案類型會和我是一個軟體消費者所需要的有很不大的差異。但通常情況下，在整個供應鏈生命週期的某些階段，每個人都會同時處於這兩種狀況下。」

組織如何將它們整合在一起將高度依賴於他們的使用案例、基礎設施，以及他們團隊技能和文化的組成。不幸的是，目前還沒有一勞永逸的萬能按鈕能夠一口氣構建這樣的整體解決方案堆疊。

十大類別

以下列表為資安長提供了一個很好的入門檢查清單，可用於規劃適合他們的軟體供應鏈安全解決方案堆疊。這份名單並不是百分之百的詳盡，而且可能很快會有所變動。但是它包含了安全負責人可能會在軟體供應鏈安全路線圖中考慮到的主要工具類別和功能。

‖ 1. 軟體組成分析和軟體物料清單生成

軟體組成分析工具目前最為人所知的是它們在軟體供應鏈安全中的角色與作用，但這一類別的起源故事卻是從更加平淡無奇的領域開始的。這些工具最初是為了幫助開發團隊追蹤其構建過程中開源元件的使用情況，以便掌握授權合規性。隨著供應鏈安全開始獲得更多關注，軟體組成分析工具內建了與追蹤元件相關的更深入漏洞及安全風險分析和管理，並成為企業組織生成軟體物料清單和管理其開放原始碼使用狀況的重要方法之一。開放原始碼管理平台Mend.io（前身是 WhiteSource）、依存關係分析工具 FOSSA 和軟體組成分析解決方案 Synopsys Black Duck 就是這種進化之路上的典型例子。

軟體組成分析並不是生成軟體物料清單的唯一選擇。其他一些軟體物料清單生成方法包括使用 CycloneDX CLI 和 SPDX Tool 之類的命令列介面（Command Line Interface，CLI）工具，像是 Rezilion 之類的執行期間分析（Runtime Analysis），抑或 ReversingLabs 之類的二進位分析等等。但是對於構建軟體供應鏈解決方案堆疊或生態系統的供應商來說，軟體組成分析往往是他們的籌碼。其中一些是軟體組成分析供應商，他們透過內部開發或收購已將觸角擴展到以下所描述的其他工具類別領域中。其他有些公司可能從一開始就抱持著以開發人員為中心的平台思維與心態，包括供應鏈工具組合中的軟體組成分析；開源軟體漏洞偵測工具商 Snyk 就是一個很好的例子。最近還出現了更多締造合作夥伴關係的案例，例如電子設計自動化公司新思科技（Synopsys）和惡意軟體分析解決方案商 ReversingLabs 宣佈，兩家將合作擴大供應鏈的安全能力，而不會將客戶鎖定在單一平台上。

‖ 2. 程式碼掃描和滲透測試

保護軟體供應鏈的核心是一個應用安全（Application Security，AppSec）問題，因此傳統的 AppSec 程式碼掃描工具將在這個解決方案堆疊中發揮作用。靜態應用程式安全測試（SAST）、動態應用程式安全測試（DAST）、互動式應用程式安全測試（IAST）和執行期間應用程式掃描防護（RASP）工具，以及明智地使用滲透測試（Penetration Testing，PT），可以幫助組織測試他們自己的內部程式碼，並提供對第三方程式碼的進一步檢查，以作為風險的安全備援措施，進而防止「使用常見軟體組成分析或軟體物料清單測試工具與技術所可能會忽略的可能風險，」Coalfire 的 Born 表示。

他說，透過全面的程式碼掃描來維持多層次的安全性是至關重要的，滲透測試的抽查也是如此。

他補充道：「軟體組成分析和軟體物料清單產品依賴於已知的、先前確認的漏洞，而全面性的應用程式滲透評估會在檢查第三方函式庫和框架時識別出有安全弱點的程式碼使用情況，而這些程式碼可能之前從未在其他地方被通報過。」

‖ 3. 軟體物料清單的豐富化和聚集

當企業組織建立他們自己的軟體物料清單並吸收來自供應商的軟體物料清單時，這些構件的聚合、豐富化和管理將成為構件被付諸實施過程中日益重要的一部分。例如，新增漏洞可利用性交換（Vulnerability Exploitability Exchange，VEX）資訊將成為「脈絡化」（contextualizing）軟體物料清單的一個日益重要的部分。同樣的，這些工具可以用來潛在強化軟體物料清單資訊的資料，包括了諸如開放原始碼安全基金會計分卡（OpenSSF

Scorecard）資料和來自美國網路安全暨基礎設施安全局（CISA）「已知遭駭漏洞」（Known Exploited Vulnerabilities，KEV）資料庫的漏洞遭駭預測評分系統（Exploit Prediction Scoring System，EPSS）分數等組件健康檢查數據。

此外，簡單地將橫跨軟體組合和主要業務範疇之間的軟體物料清單資訊聚集在一起，將成為安全負責人日益關注的重要問題。這仍然是一個新興的領域，還沒有真正形成行業分析師已確定的類別，因此資安長必須在 SCA+類型的工具、開放原始碼工具和新的平台中尋找這些功能，這些工具和平台正在開闢屬於他們自己定義之類別的大道。一些正在開闢這個新興領域的案例廠商與工具包括資安漏洞管理平台Cybellum、容器安全性檢測工具 Anchore 和自動化軟體供應鏈安全平台Rezilion，以及 Bomber 之類的新開放原始碼工具。

‖ 4. 機密管理

共享機密掃描和管理正迅速從一個獨立的工具類別轉變為一個被整合到各種軟體供應鏈安全工具中的功能。這是因為嵌入在原始程式碼、配置設定檔和基礎設施程式碼中的機密，在開發和實際環境中遭到外洩的問題依舊十分猖獗，因此迫切需要解決這樣的問題。

「諸如憑證檔、私密金鑰、密碼和 API 令牌等機密資訊不應提交給原始碼控制儲存庫，」Gartner 最近更新的一份報告建議。「請使用機密管理工具安全地儲存和加密機密資訊，實施存取控制，並管理機密（亦即建立、輪換和撤銷）。」

這是一個基本的工具組件，因為攻擊者可以利用共享機密或密鑰來全面破壞企業組織軟體供應鏈的完整性。

‖ 5. 依存關係管理和對應

依存關係管理和分析是另一個有點模糊的類別，其與軟體組成分析和軟體物料清單聚集之類的其他工具類別高度重疊。但這是值得呼籲的，因為它觸及到一些最複雜的軟體供應鏈安全問題的核心。

安全倡導者對當今軟體物料清單狀態的最大抱怨是，它們仍然難以交流與所枚舉軟體相關的可傳遞依存性（transitive dependencies）。

資安長和他們的團隊將需要更好的方法來規劃和管理隱藏在他們應用程式、API、持續整合/持續交付管道元件和 IaC 基礎設施即程式碼之間的依存關係網路。一些可用的工具包括依存關係對應工具，強調績效和彈性的利益關係人也依賴像是雲端監控平台 Datadog 和團隊協作軟體供應商 Atlassian 所提供的這類工具。此外，軟體組成分析和軟體物料清單管理工具經常將這些特性合併到它們的組合中。最近在這方面打入市場的一個值得注意的參與者是 Endor Labs，該公司於 2022 年 10 月脫去了過去一直保持低調的隱身模式外衣，開始力力宣稱自己是「依存關係生命週期管理」解決方案供應商。日前，該公司在 RSA 2023 大會的創新沙箱（Innovation Sandbox）大賽中成功闖進決賽。

‖ 6. 受信任的儲存庫和註冊表

雖然構件儲存庫和容器註冊表本身不是安全工具，但是搭配紀律嚴明的政策和流程一起使用的話，可以在管理供應鏈風險方面發揮重要的作用。建立可信賴的構件儲存庫和容器註冊表是為開發人員建立「安全防護機制」基礎設施的基本部分。提供經批准元件的集中化來源資訊是一種可以阻止問題發生的主動積極作法，並對導入到企業組織內軟體的內容打造健全的治理機制。

「這些儲存庫扮演了經批准和審查之構件和軟體組件的可信任來源角色，」Gartner 分析師寫道。「如此一來便能實現對軟體「成份」的集中治理、可視性、可稽核性和可追溯性。」

‖ 7. 安全程式碼簽章

隨著開發人員在程式碼與容器生命週期內提交和部署軟體，程式碼簽章正日益成為確保其完整性的最佳實踐。這個過程不僅對於建立強大的內部控制以防止篡改至關重要，而且對於建立將產品交付給外部客戶的顧客信任度也至關重要。當然，程式碼簽章憑證已成為軟體供應鏈攻擊者青睞的目標，

因此資安長和他們的團隊將需要確保他們選對了工具並建立良好的控制機制，以確保他們的程式碼簽章程序真的很安全。在此一類別中的一些重量級廠商包括 Garantir、Keyfactor、CircleCI 和 Venafi 等安全程式碼簽章系統商，以及軟體構件簽章工具商 Cosign。

8. 持續整合/持續交付管道安全性

持續整合/持續交付管道是軟體「工廠」的一部分，開發人員依靠它來生產程式碼，因此，它是整個供應鏈的內在組成部分。因此，加強這些環境的安全工具是健全供應鏈安全計畫中不可或缺的一部分。我們已經解決了機密管理問題，這是這個類別的一個重要方面。其他還包括了持續整合/持續交付政策和治理管理（就像雲端應用安全平台Apiiro 和軟體供應鏈安全方案商 Cycode 之類公司所生產的解決方案），以及實現良好的權限存取控制和強式身分認證。

9. 第三方風險管理平台

行文至此已描述的大多數工具多半著墨在內部開發軟體中使用的第三方組件。但是，對於一些組織無法從中獲得太多可視性的第三方商務軟體又該怎麼確保安全呢？別擔心！這就是第三方風險管理（Third-Party Risk Management，TPRM）工具和程序發揮作用的地方。即使在聯邦軟體物料清單的要求下，軟體供應商在未來幾年內競相推動提高透明度，但目前大多數組織仍然相當盲目。雖然像是資安風險監控平台SecurityScorecard 或第三方風險管理平台RiskRecon 等 TPRM 風險評分工具不能完全解決這類問題，但它們至少可以作為安全風險代理，協助企業組織確定自己的需求，並與特定供應商和軟體供應商合作，以深入探究他們的程式碼。

「我認為 TPRM 產品可以發揮作用的地方是，一旦存在風險，而我能夠識別風險，也許這就是我真正希望將全付精力集中在軟體組成分析和軟體組成理解的地方，」德勤的 Chand 表示。「它成為了一種風險緩解技術，而不是在所有我所生產或購買軟體中使用的奇特應急方案。」

她說，軟體供應鏈安全領域仍然缺乏應用安全風險和業務風險之間的可靠工具聯結，她認為下一個重大創新契機可能在於供應商和從業人員如何將 TPRM 平台和更廣泛的供應鏈風險管理流程與軟體物料清單和持續整合/持續交付管道的資料相互連結。

10. 基礎設施即程式碼安全和雲端原生應用程式保護平台

用於測試和部署程式碼的底層基礎設施本身也是程式碼，它是供應鏈的基本組成部分。因此，資安長最起碼應該考慮將「基礎設施即程式碼」掃描和安全工具作為其更廣泛的供應鏈安全計畫的一部分。這些工具傾向於跨越軟體供應鏈安全工具和雲端原生應用程式保護平台（Cloud-Native Application Protection Platform，CNAPP）之間的界限，這也顯示出他們開始跨入雲端安全和一般安全營運領域的跡象。但是 CNAPP 平台提供了很多其他的供應鏈安全支援，特別是在容器可視性和執行期間安全性方面為然。容器是軟體供應鏈中日益增長的攻擊目標，執行期間安全措施可以在工作負載衝擊生產環境後為其提供安全備援保障。