ソフトウェア・サプライチェーン・サービス

概要

ソフトウェア製作者に対して厳格なソフトウェア・セキュリティ・プラクティスの実践を義務付ける法律が世界中で可決されつつあります。これを受けて、組織はソフトウェア・セキュリティに対するアプローチ、従うべき業界標準、そしてソフトウェア開発チームにとってのベスト・プラクティスの見直しを迫られています。これらの法律は主に政府省庁や請負業者が調達するソフトウェアを対象にしたものですが、その直接的な影響はエンタープライズ・ソフトウェアやクラウド・サービス、さらにはコンシューマー・レベルの製品まで広範に及びます。このため、政府の調達はもはやこれまでのような単純な取引ではなく、重要インフラ・セクターおよび関連するテクノロジー・サプライヤーを幅広く巻き込んだ取引へと形を変えています。

こうした立法化の動きに共通する 1 つの要素として、「堅牢なソフトウェア部品表（SBOM）」および脆弱性開示プログラムへの参加という構想があります。ソフトウェア製作者は、自らのソフトウェアがどのように作成・テストされ、セキュリティ対策されているかについてより深く理解することがこれまで以上に求められています。具体的には、各ソフトウェア・コンポーネントの出所を記録した文書を常に最新の状態に維持すること、テストの結果およびテスト中に軽減されたリスクを証明すること、そしてソフトウェア・ライフサイクル全体を通じて信頼できるソフトウェア・サプライチェーンを維持するための自動化されたプロセスを採用することなどです。また、SBOM はアプリケーションの「成分」を文書化して伝達するための共通の枠組みとなるもので、これによって特にサードパーティのオープンソース・コンポーネントに関するコードの不透明性を軽減できます。

ソフトウェア・サプライチェーンを適切に管理するのは簡単ではありませんが、ブラック・ダックのソフトウェア・サプライチェーン・サービスにより、最新の規制や政府の要求への確実な適合が容易になります。

ソフトウェア・サプライチェーンのセキュリティ上の課題

新しいプロセス全般に言えることですが、ある特定のソフトウェアにおいてソフトウェア・サプライチェーンのセキュリティ対策をとることには多くの課題があります。これは、ソフトウェアを自前で作成したか、外部に作成を委託したか、ソフトウェア製作者から購入したかを問いません。例えば、コンポーネントの特定という問題があります。ソフトウェアには単一のソース（ベンダー）が存在するという前提に立ったシステムでは、オープンソース・コンポーネントを正しく特定できません。これは、オープンソース・ソフトウェアには単一のベンダーが存在せず、その代わりに多くの貢献者がいて、それぞれの出所から誰もがそのソフトウェアをダウンロードできるためです。これらの異なる出所をいかに正確に特定するかという問題は業界内で依然として未解決のままであり、今後は、どのように開発されたかにかかわらず、各コンポーネントに対して標準的な命名規則を適用することが必要となってきます。コンポーネントを特定できたら、アプリケーション内のサードパーティ・コード使用に伴うリスクを軽減するための標準、プロセス、教育、およびツールに関して開発コミュニティとエコシステムが共同で取り組む必要があります。

ソフトウェア・サプライチェーンのリスクについて調査する際に避けて通れないのが、SPDX（Software Package Data Exchange）と CycloneDX という 2 つの標準 SBOM フォーマットで、SBOM の要件を満たしていることが NTIA によって認められています。これらの規格は、アプリケーションにおけるサードパーティ・ソフトウェアの使用に関する情報を企業間で容易に交換できるようにするとともに、ソフトウェアがサプライチェーン全体でどのように作成、配布、利用されるかについての信頼性と透明性を確保することを目的としています。しかし SBOM 市場はまだ成熟の途上にあります。これらの標準によって企業間での情報交換は容易になりますが、SBOM 文書に含まれるデータの完全性と正確性の問題は解決しません。

サプライチェーンのセキュリティ対策を支援するブラック・ダックのサービス

SSDF 準備状況評価（SSDF Readiness Assessment）

米国国立標準技術研究所（NIST）からは、セキュア・ソフトウェア開発フレームワーク（SSDF）と呼ばれるガイダンスが発行されています。SSDF は、標準化された方法で安全にソフトウェアを開発する際にベースラインとなる一連のプラクティスと関連タスクをまとめたものです。米国政府が直接または間接に調達するソフトウェアのうち、2022 年 9 月以降に製作され、継続的にアップデートされるものについては、SSDF のサブセットへの適合を証明することが米国政府によって求められており、ソフトウェア・サプライヤーは SSDF への適合を自己証明する必要があります。

ブラック・ダックの SSDF 適合評価は、組織のソフトウェア開発プラクティスが SSDF のプラクティスとタスクに合致しているかどうかを判定し、ガイドラインに適合していない場合はどの対策が不足しているのかを評価します。この評価結果と関連する是正提案は、米国政府に対する証明に使用できます。

SBOM はビジネスの問題を技術面から解決するソリューションです。ソフトウェア・サプライチェーンに信頼性を持たせるには、ソフトウェアの組成（コンポジション）に透明性を確保し、NIST のセキュア・ソフトウェア開発フレームワーク（SSDF）など広く認められた標準に適合することが必要です。

SBOM 管理マチュリティ・アクション・プラン（MAP）

ソース・コードに対して SBOM 生成ツールを適用するだけで正確かつ完全な SBOM を作成できることはほとんどありません。ブラック・ダックの SBOM 管理マチュリティ・アクション・プラン（MAP）は、ソフトウェア・セキュリティのリーダーと実務担当者に対して顧客向けの SBOM を信頼できる方法で生成するための実用的なガイダンスを提供するとともに、サプライヤーから受け取った SBOM を利用する方法についてのガイダンスも提供します。また、組織内で SBOM の生成に携わる人、プロセス、テクノロジーを評価し、SPDX または CycloneDX 規格に準拠した正確な SBOM が生成されているかも確認します。

監査サービスとしての SBOM 生成

ソフトウェア製作者は今後、規制上または契約上の理由から SBOM の生成が必須となり、不正確または不完全な SBOM に対しては重大なペナルティが課される可能性があります。監査サービスとしての SBOM 生成は、定評ある Black Duck® 監査サービスのプロセスに基づいて Black Duck 監査サービス・チームがソフトウェアの完全なセキュリティ監査を実施し、目標とする SBOM の最小データ要件を満たす SBOM を生成します。このサービスは、アプリケーションに対してベースラインとなる実証済み SBOM を必要としながらも、SBOM の生成能力を持たない組織に特に大きな価値があります。

SBOM 監査 / 検証

規制上または契約上の理由から SBOM の生成が義務付けられ、自動化を利用して SBOM を生成しているソフトウェア製作者は、監査済み SBOM の提供を求められる場合があります。また、サプライヤーが生成した SBOM をソフトウェア利用者側で監査したいこともあります。いずれの場合も、ソフトウェア監査の分野で定評のある、信頼のおける第三者が必要です。Black Duck 監査サービスのソフトウェア・セキュリティ監査は、合併・買収（M&A）プロセスにおけるテクニカル・デューデリジェンスとして実施されるセキュリティ・レビューにおいて、業界で最も厚い信頼を得ています。これらの実績あるプロセスをベースにしたブラック・ダックの SBOM 監査 / 検証サービスは、ソフトウェアを監査して、クライアントが自動化によって生成した SBOM がサプライチェーンを正確に反映しているかどうかを確認します。

セキュア DevOps パイプライン評価

セキュアな DevOps パイプラインがなければ、パイプラインのアクションに基づいて証明を行っても、その証明自体が疑わしいものになります。ブラック・ダックのセキュア DevOps パイプライン評価は、DevOps パイプラインおよび関連するインフラストラクチャのセキュリティを検証するための一連のリファレンスを提供します。例としては、アクセス制御、ネットワーク・セキュリティ、暗号化、監査、継続的監視などが含まれます。

主な利点

ソフトウェア製作者は、顧客とユーザーのためにソフトウェア・サプライチェーンのセキュリティを保護する上で重要な役割を担っています。ブラック・ダックのソフトウェア・サプライチェーン・サービスなら、以下のことを達成できます。

- 組織のソフトウェア開発プロセスが SSDF に適合していることを自信を持って検証し、証明できる
- 貴重なセキュリティ・リソースを割り当てなくても、標準フォーマットの SBOM を生成して規制に適合できる
- ソフトウェア・サプライチェーンのセキュリティと SBOM についてどのようなストラテジー、能力、およびアクティビティを採用すべきかを見極めることができる
- 専門の第三者による妥当性確認とガイダンスにより、SBOM およびその生成ツールとプロセスが正確で完全であることを確認できる
- DevOps パイプラインで使用されるセキュリティ、構成、およびプロセスの妥当性を確認できる

これまで 20 年以上にわたりソフトウェア・セキュリティ・プログラムの実装を成功に導いてきたブラック・ダックの経験をご活用ください。ブラック・ダックは、ソフトウェア・サプライチェーンのセキュリティ・ストラテジー作成だけでなく、その実装に必要な賛同、リソース、および支援を得られるようにお手伝いします。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp