ブラック・ダック SSDF 準備状況評価

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ものへと形を変えています。

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 月以降に製作されたものについては、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 SSDF 準備状況評価は、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、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。

BSIMM で培った実績

ブラック・ダックのセキュア開発成熟度モデル（BSIMM）は、組織が自社のソフトウェア・セキュリティ・プログラムを分析し、さまざまな業種から参加した 100 以上の組織のスコアと照らし合わせてベンチマーク評価できる診断サービスです。データに基づいたこの客観的な分析を足がかりにして、リソース、時間、予算、優先順位を決定することで、セキュリティ態勢の改善を目指していくことができます。

ブラック・ダック SSDF 準備状況評価は、開発環境のセキュリティに加え、BSIMM で評価したガバナンス、文化、およびプロセスの測定結果も定量化します。BSIMM と SSDF の対応関係については、SSDF（SP 800-218 Version 1.1）の中で各 SSDF タスクの「References」欄に記載されています。

調達活動に関しては、SSDF に適合しながらソフトウェア・セキュリティを改善していくことが求められます。2022 年 9 月 14 日の翌日以降に製作されたソフトウェアを直接または間接的に米国政府に販売する場合、NIST SSDF の特定のタスクへの適合証明が必要です。以下の指令への適合でお困りの場合は、SSDF 準備状況評価のご利用をご検討ください。

- EO 14028
- NIST SP 800-218 Version 1.1
- OMB 覚書 M-22-18
- DHS CISA 自己証明
- IEC 62443

組織と製品の両方が対象

評価機能のコア部分は、SSDF タスクへの適合証明が求められているセキュリティ・チーム向けに設計されています。このような証明は、規制上または契約上の理由で外部の顧客から要求されることもあれば、買収後にソフトウェア開発の現状を評価し、セキュリティ・チームと製品チームのニーズに即した形で統合作業を進めるために必要となることもあります。

企業によっては、製品レベルで開発プラクティスを点検したいこともありますが、この場合もブラック・ダック SSDF 準備状況評価はうってつけです。製品レベルでの評価をいつ実施するかについては、(1) 製品が重要インフラと見なされる場合、(2) 契約上の要求事項、開発メソドロジ、セキュリティ目標に変更があった場合、(3) 全体的な製品ライフサイクルのステージごと、などが考えられます。

OMB/CISA の自己証明の要件に適合

米国行政管理予算局 (OMB) は、米国政府の調達サプライチェーンに属するソフトウェア・プロバイダーに対し、SSDF への適合証明を求める覚書を発行しました。この証明は、バイデン大統領のサイバーセキュリティに関する大統領令に関連するすべてのコンプライアンス・プログラムで重要な要素となります。2022 年 9 月 14 日の翌日以降に製作されたソフトウェア、または継続的アップデート / 継続的デリバリ・モデルによってデプロイされるソフトウェアは、この覚書の対象に含まれます。このため、クラウド・ベースまたは SaaS ソフトウェア・ソリューションはすべて対象に含まれることに注意が必要です。

OMB は、自己証明の要件のベースラインとして SSDF に直接言及しており、米国サイバーセキュリティ・社会基盤安全保障庁 (CISA) に対して具体的な要件の作成を指示しました。ブラック・ダック SSDF 準備状況評価は、必要な SSDF タスクが組織または製品ライン内で一貫して実施されていることを実証できるユニークなサービスです。デフォルトでは、各タスクの適合度スコアの平均値を使用して証明の各設問の適合度を算出します。より強いリスク回避が求められる組織では、最小値ベースのモデルに変更し、最もスコアの低いタスクの適合度を証明の設問の適合度とします。

平均値と最小値のどちらを使用した適合度であっても、ブラック・ダック SSDF 準備状況評価を実施することにより、どのタスクがスコア低下の要因となっているかを突き止めることができます。

修正または POAM が必要な領域を特定

ブラック・ダック SSDF 準備状況評価は、SSDF の 42 のタスクについて、それぞれの適合度を判定します。あるタスクの適合度が低い場合、そのタスクの実施に一貫性がなく、改善の余地があることを示しています。どの弱点を POA&M (Plan Of Action and Milestone) の対象とするかは、調達チームが定義した要件の性質に基づいて決めることができます。

成熟したソフトウェア・サプライチェーン・ストラテジーに不可欠な要素

ソフトウェア・サプライチェーンを適切に管理するには、種類の異なるアプローチを組み合わせることが必要です。最初は Black Duck® などのソフトウェア・コンポジション解析から始めますが、ソフトウェア部品表 (SBOM) やセキュア・ソフトウェア開発ライフサイクルなどのビジネス要件も盛り込む必要があります。ガバナンスの観点から、SSDF のタスクが組織全体、または事業部門や製品ライン内、あるいは個々の製品レベルで一貫して実施されていることを確認できるのがブラック・ダック SSDF 準備状況評価ならではの強みです。

SSDF への適合度スコア

組織の準備 (PO)

SSDF タスク	エンタープライズ	製品 1	製品 2	製品 3	製品 4	製品 5
PO.1.1	非常に高	非常に高	非常に高	非常に高	非常に高	非常に高
PO.1.2	非常に高	非常に高	非常に高	非常に高	非常に高	非常に高
PO.1.3	高	中	高	高	非常に高	非常に高
PO.2.1	非常に高	高	非常に高	非常に高	非常に高	非常に高
PO.2.2	非常に高	高	低	非常に高	非常に高	非常に高
PO.2.3	非常に高	低	非常に高	非常に高	非常に高	非常に高
PO.3.1	非常に高	中	非常に高	非常に高	非常に高	非常に高
PO.3.2	非常に高	非常に高	非常に高	非常に高	非常に高	非常に高
PO.3.3	非常に高	非常に高	非常に高	非常に高	非常に高	非常に高
PO.4.1	中	非常に高	非常に高	非常に高	非常に高	非常に高
PO.4.2	非常に高	非常に高	非常に高	非常に高	非常に高	非常に高
PO.5.1	非常に高	非常に高	非常に高	非常に高	非常に高	非常に高
PO.5.2	非常に高	非常に低	非常に高	非常に高	非常に高	非常に高

十分にセキュアなソフトウェアの作成 (PW)

SSDF タスク	エンタープライズ	製品 1	製品 2	製品 3	製品 4	製品 5
PW.1.1	低	中	高	高	低	高
PW.1.2	非常に低	高	高	高	高	非常に高
PW.1.3	非常に低	非常に高	非常に高	非常に高	中	非常に高
PW.2.1	低	非常に高	非常に高	非常に高	中	非常に高
PW.4.1	高	高	高	高	高	高
PW.4.2	非常に低	非常に高	非常に高	非常に高	中	非常に高
PW.4.4	中	中	中	中	中	中
PW.5.1	低	低	低	低	高	低
PW.6.1	低	非常に低	非常に低	低	低	低
PW.6.2	低	非常に低	非常に低	低	低	低
PW.7.1	中	非常に高	高	非常に高	非常に高	非常に高
PW.7.2	中	非常に高	非常に高	非常に高	非常に高	非常に高
PW.8.1	低	非常に高	高	非常に高	中	非常に高
PW.8.2	高	高	非常に高	高	高	非常に高
PW.9.1	非常に高	非常に低	非常に高	非常に高	非常に高	非常に高
PW.9.2	非常に高	非常に低	非常に高	非常に高	非常に高	非常に高

ソフトウェアの保護 (PS)

SSDF タスク	エンタープライズ	製品 1	製品 2	製品 3	製品 4	製品 5
PS.1.1	高	中	高	非常に高	非常に高	非常に高
PS.2.1	低	高	非常に低	非常に高	非常に高	非常に高
PS.3.1	非常に低	非常に高	非常に高	非常に高	非常に高	非常に高
PS.3.2	非常に高	非常に低	非常に高	非常に高	非常に高	非常に高

脆弱性への対処 (RV)

SSDF タスク	エンタープライズ	製品 1	製品 2	製品 3	製品 4	製品 5
RV.1.1	非常に高	中	非常に高	非常に高	非常に高	非常に高
RV.1.2	非常に低	非常に低	高	高	高	高
RV.1.3	非常に高	高	高	非常に高	非常に高	非常に高
RV.2.1	中	中	非常に高	非常に高	非常に高	非常に高
RV.2.2	中	中	中	非常に高	非常に高	非常に高
RV.3.1	非常に低	低	低	低	低	低
RV.3.2	中	高	高	高	高	高
RV.3.3	非常に低	非常に低	非常に低	非常に低	非常に低	非常に低
RV.3.4	中	高	高	高	高	高

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