マチュリティ・アクション・プラン（MAP）

**ソフトウェアに
セキュリティを組み込む
道筋をナビゲート**

概要

セキュリティ・チームと開発チームが協力して組織全体およびアプリケーション・ポートフォリオ全体でソフトウェア・セキュリティ態勢の強化に努める中、組織は達成可能なリスク緩和目標に優先順位を付けようとしています。また、現在の取り組みを改善する方法だけでなく、目標を達成するにはそれ以外に何をすべきなのかも見極めたいと考えています。資金提供の優先順位付け、リソースの合理化、ならびにソフトウェア脆弱性のリスクを低減するには、計画の作成が不可欠です。ブラック・ダックのマチュリティ・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および実務担当者に対し、既存のソフトウェア・セキュリティ・プログラム（SSP）の改善、または新規 SSP の設立についての実践的なガイダンスを提供します。MAP では、まず 7 要素分析、またはセキュア開発成熟度モデル（BSIMM）のフレームワークを使用して、現在のセキュリティ・プログラムを人、プロセス、テクノロジーの面から評価します。次に、ブラック・ダックがお客様の SSP リーダーと共同で、ROI を最大化しながら組織内のリスクを低減できるよう、組織に合った戦略を複数年計画として立案します。

エキスパートからの実践的なガイダンス

SSP MAP は、しばしば BSIMM 診断と組み合わせて実施され、セキュリティ・リーダーにとっての羅針盤となるもので、数ある製品、プロジェクト、人の中からどこに投資すべきかをナビゲートします。MAP のプロセスはシンプルで、ブラック・ダックには卓越した専門知識があります。

SSP の目標に対するコンセンサスを形成

ソフトウェア・セキュリティ・イニシアティブは、個々の組織に合わせて作成する必要があります。そのために、まずビジネスが直面するリスク・プロファイルを理解し、利害関係者の困難を理論的に説明し、プログラム憲章に対するコンセンサスを形成することから始めます。

ソフトウェア・セキュリティ・アクティビティの現状を把握する

このフェーズでは、ブラック・ダックのコンサルタントが業界標準の SSP 測定手法である BSIMM を使用して、組織の SSP やセキュア・ソフトウェア開発ライフ・サイクル（SDLC）など、エンタープライズ・ソフトウェア・セキュリティ・アクティビティの現状を測定します。正式な SSP を実施していない組織については、BSIMM 診断の代わりにペネトレーション・テストまたはセキュア・コード・レビューを推奨します。ここでは、SDLC のなるべく早い段階で不具合を発見し、コストが高くつくライフ・サイクル終盤での修正を防ぐことに重点が置かれます。

MAP の作成が完了したら、その実装に必要な賛同、リソース、および支援を得るために、組織全体への周知をお手伝いします。

工数の見積もり、主要なマイルストーンの定義、そして目標状態へ向かう初期段階で得られる成果の特定をコンサルタントがお手伝いします。

目標状態を定義する

SSP の目標を満たし、利害関係者の懸念を払拭するにはどのような変革が必要かを、ブラック・ダックのエキスパートが組織の SSP リーダーと共同で特定します。このフェーズでは、これまで多くの組織においてソフトウェアにセキュリティを組み込む活動を支援してきたブラック・ダックのコンサルタントの豊富な経験が活かされます。また、業界のベスト・プラクティス、コンプライアンスと規制上の義務、組織のリスク許容度も考慮します。

今後の道筋を定義する

ソフトウェア・セキュリティは旅であり、目的地ではありません。一度到達すれば終わりというものではなく、継続的に取り組むべきものです。しかし、その取り組みを成功させるには、ソフトウェア・セキュリティ・プログラムのビジョンを作成・維持することが不可欠です。このフェーズでは、目標状態へと向かう今後 12 ～ 24 カ月の変革の取り組みを定義し、優先順位を付けて合理的に説明できるようにエキスパートが支援します。

主な利点

- 組織で採用すべきソフトウェア・セキュリティ戦略、能力、およびアクティビティが明らかになります
- 経営陣に今後 2 年間にわたる SSP の成熟化に関する詳細なロードマップを提供できます
- 影響力の大きい取り組みの優先度を上げ、長期間を要する取り組みを実装フェーズの早期に開始することにより、予算をより効果的に配分できます

これまで 20 年以上にわたりソフトウェア・セキュリティ・イニシアティブ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。MAP の作成が完了したら、その実装に必要な賛同、リソース、および支援を得るために、組織全体への周知をお手伝いします。

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