ホワイトペーパー

Fortifyによるビジネス価値の継続的デリバリ

Mainstayカスタマーエビデンスリサーチ

MAINSTAY

アプリケーションの継続的デリバリは、あらゆる業界のソフトウェア開発を行う組織にとっての新たな常識になっています。ソフトウェア開発チームは、新規リリースやアップデートを目まぐるしい速さで提供することを求められており、これがソフトウェアセキュリティチームには大きな重圧になっています。このレポートでは、Fortifyのソフトウェアセキュリティソリューションを利用することで、アプリケーションスキャンの迅速化、適切なトリアージによる修復作業の効率化、およびソフトウェア開発環境全体へのセキュリティ保証の仕組みの統合を実現している主要企業の開発部門の取り組みについて詳しく説明しています。ボトルネックが解消されることで、セキュリティチームは短期間のリリーススケジュールに対応できるようになり、市場投入までの期間短縮が可能になります。また、開発者はソフトウェアの改善に注力できるようになります。

新時代のソフトウェアセキュリティ

デジタルトランスフォーメーションのセキュリティニーズへの対応

現在、あらゆるビジネスがソフトウェアビジネスになりつつあります。従来型の産業も、市場に対応して競争力を維持するために、ソフトウェアを活用した「デジタルトランスフォーメーション」の必要性に直面しています。たとえば、産業界の代表格であるGEは、既存の風力発電施設での発電量を少しでも増やそうと、風力タービン内のセンサーからのデータを利用するソフトウェアの開発を行っています。自動車メーカーは、「スマート化」や「コネクテッド化」が進む自動車製品に、何千万行ものコードを組み込んでいます[1]。

あらゆるビジネスでソフトウェアが重要な存在になり、さらにクラウドベースのソフトウェアサービスが急増するのに伴い、企業はこれまでにないペースでアプリケーションの開発とアップデートを行っています。継続的にソフトウェアデリバリを行う新しい時代に入っています。継続的デリバリでは、開発チームが新機能を搭載したソフトウェアをリリースするサイクルがますます短縮されます。1年または四半期に1回だったものが、毎月、毎週、または毎日のペースに短縮されることになります。

このアプローチは、Microsoft、Google、およびFacebookなどの先進企業のDevOps環境にはすでに組み込まれています。これらの企業のWebサイトでは、週1回のペースでメジャーソフトウェアリリースが行われ、それ以外の日にも毎日バグ修正が行われています。フォレスターリサーチは、2010年に年4回だったソフトウェアリリースが、2020年までにその30倍の年120回に増えると予想しています[2]。

セキュリティチームへの重圧

市場がアジャイルな継続的デリバリモデルに移行していく中で、組織内の開発チームとセキュリティチームは、膨大な数のアプリケーションとリリースへの対応に追われており、これがソフトウェアセキュリティ保証 (SSA) という開発ライフサイクルの重要な部分への重圧となっています。簡単に言うと、組織には、セキュリティテストや修復のためにソフトウェアデリバリのペースを緩める余裕がありません。

また、以下のようなトレンドが、この困難な状況をさらに複雑にしています。

- SaaSやモバイルデバイスが普及したことで、アプリケーションのセキュリティ上の欠陥を検出するための入念なテストが必要になっています。
- 多くの企業がレガシーアプリケーションとCOTSアプリケーション (commercial off-the-shelf; 商用オフザシェルフ、既製品で販売やリースが可能となっているソフトウェア製品) が混在するハイブリッド環境を利用し、さまざまなリリースサイクルに対応しているため、セキュリティプログラムの複雑化が進んでいます。
- 開発者がMavenやGitHubなどのオープンソースソフトウェア (OSS) リポジトリからダウンロードしたコードを利用することが増えており、その多くに脆弱性が存在することが確認されています。

ほとんどの組織で時代遅れになったセキュリティテストツールと手法が使用されていることもあり、この困難な状況への対応はあまり進んでいません。これらのツールには、短い時間で大量のコードと膨大な回数のスキャンへの対応を可能にする自動化機能がありません。多くの場合、これらのツールが対応しているのは、セキュリティテストプロセスの一部、一部の言語、または限られた展開オプションのみです。そのため、開発サイクルの中でいくつものツールを切り替えて使用する必要があり、効率的に作業を行うことができません[3]。

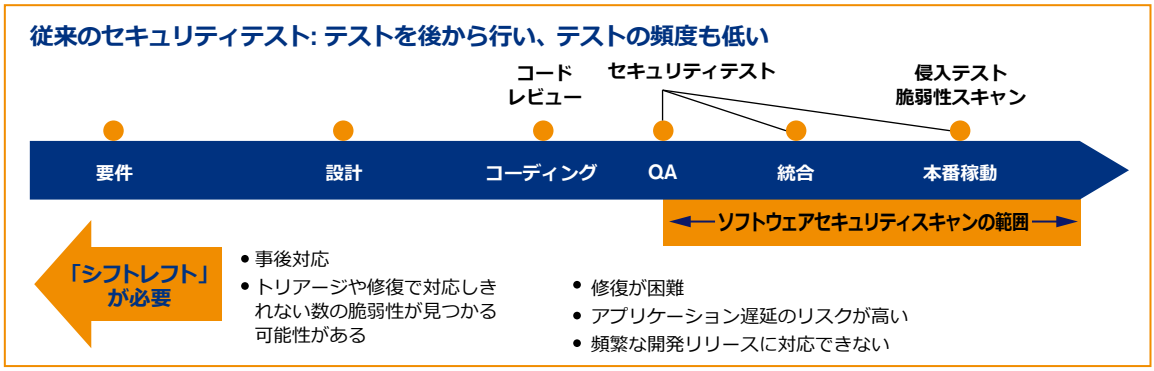
実際、業界アナリストの推計によると、90%の企業がアプリケーション開発を行っており、99%がエンタープライズセキュリティを強化することに賛同しているにも関わらず、エンタープライズセキュリティに関する何らかの対策を行っている企業は20%しか存在しません。ガートナーは、自社のDevOpsの取り組みに情報セキュリティを体系的に組み込んでいるエンタープライズセキュリティアーキテクトは20%に満たない状況で、Secure DevOpsと呼べるセキュリティ自動化レベルに到達している企業はさらに少ないと推定しています。

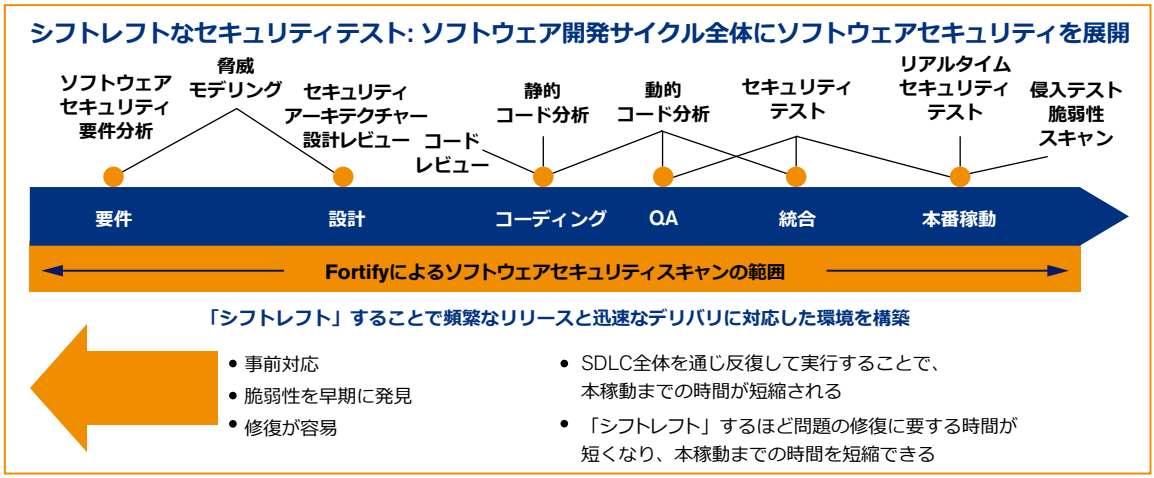
「シフトレフト」

最近になるまで、組織はセキュリティテストや修復の作業を、主にソフトウェア開発ライフサイクルの後半フェーズで行っていました。しかし、ソフトウェア開発の後半で修復を行うのは、非常にコスト高で、時間もかかります。また、製品開発スケジュールが厳しい場合は、修復のための時間を十分に取れないため、既知または未知の脆弱性が残ったままの状態でアプリケーションがリリースされる可能性が高くなります。また、現在のツールセットはスケーラビリティが十分でないため、アプリケーション数が増え、リリース回数が増大を続けるにつれてスキャン回数が相対的に少なくなり、生産性が損なわれます。

こうしたことはすべて事後対応型のセキュリティ保証につながり、結果としてプロジェクトに遅れが生じるリスクが増大します。また、アプリケーションセキュリティを十分に確保できず、継続的デリバリのニーズに合わせた拡張ができなくなります。対照的に、今回調査した先進企業では、よりアジャイルでプロアクティブなアプローチを用いています。これは、早い段階からフィードバックループに対応したテストを頻繁に行い、コードの脆弱性を徐々に取り除いていくことを重視したアプローチです。

つまり、下の図に示すように、これらの組織はセキュリティテスト業務を「シフトレフト」(テスト工程を前倒しすることによって開発全体の時間軸を左へシフト) することで、コーディング段階で持ち込まれる脆弱性の数を減らしています。最近の調査によると、こうした取り組みを行っている組織では、セキュリティ上の問題の修復に要する時間が55%短縮されています[5]。





ソフトウェアセキュリティ保証の進化

Mainstayは、2010年にFortifyのアプリケーションセキュリティソリューションの経済的効果に関する初めての調査を行いました。このときに、ITおよびアプリケーションセキュリティチームが抱えていた最大の課題は、単にソフトウェアの脆弱性を見つけることと、脆弱性を早期に見つけて修復を容易にすることでした[4]。2013年にMainstayが主要企業を再度調査したときには、以前と変わらずできるだけ多くの脆弱性を見つけて修復することに重点が置かれており、多くの企業がクラウドサービスを選択してセキュリティ対策をサードパーティの開発者に広げている状況でした。

当社の最新の調査では、これまで以上に短期間のリリースサイクルに対応できるスピードとスケーラビリティが求められる中で、ソフトウェアセキュリティソリューションの市場に変化が現れていました。組織は潜在的な脆弱性を漏れなく発見することに留まらず、適切にトリアージを行うことで、ビジネスに重大なリスクをもたらす欠陥をすばやく特定して修復することを求めるようになっています。

主要企業のソフトウェアセキュリティ業務に関する調査

主要企業が継続的ソフトウェアデリバリのニーズにどのように対処しているかを把握するため、MainstayはFortifyの製品やサービスを採用している幅広い企業のアプリケーションセキュリティ責任者を対象に詳細なインタビューを行いました。Mainstayはこれらのインタビューに加えてオンライン調査を行い、今日のテンポの速い環境でソフトウェア開発部門とセキュリティ部門が直面している課題を幅広い視点から明らかにしました。

ソフトウェアセキュリティ調査に参加した企業には、以下の企業が含まれています。

- 世界最大規模の金融サービス持ち株会社 (1社)
- 世界最大規模の多国籍石油ガス会社 (2社)
- グローバルなソーシャルレンディング (Peer-to-peer lending) およびオンライン取引プラットフォーム企業
- 機関投資家向けオンライン投資サービス事業者
- 50か国以上で事業を展開する世界最大規模の銀行 (1行)

この調査では、ソフトウェアセキュリティ保証プロセスを、以下の5つの重要な側面から分析し、Fortifyの導入が各要素にどのように作用したかを評価しました。

- **スキャンセットアップ:** スキャンのセットアップに要する手間と時間、セキュリティツールおよびセキュリティプロセスがどの程度適切に開発環境に統合されているか

- **スキャン性能:** スキャンの速度と検出された脆弱性の数

- **トリアージ:** 脆弱性の優先順位付けがどの程度効果的に行われたか、および誤検知の数、重要度で優先順位付けできるかどうか、FortifyのMTTT (平均トリアージ時間) への影響

- **修復:** 修復が必要な脆弱性の数、修復の効率とスピード、脆弱性の繰り返しの削減、FortifyのMTTR (平均修復時間) への影響

- **スケーラビリティ：** 当社の調査では、数量が大幅に増えたアプリケーションを短い時間でスキャンして修復するため、組織がどのようにFortifyを展開してセキュリティプロセスを柔軟に拡張するかについても確認しました。評価指標には、スキャンしたアプリケーションの数、実行したスキャンサイクル数、およびコーディング時にソース段階で回避した開発側の問題の数が含まれています。

以下の各セクションでは、調査の結果について検討します。

Fortifyを選ぶ理由

調査対象の企業の54%が、実際に導入を決める前から、Fortifyをアプリケーションセキュリティソフトウェアの第一候補として考えていたと答えています。Fortifyを選択した理由のトップ3は、次のとおりです。

- ソリューションの柔軟性
- 各種プログラミング言語およびサードパーティコードへの幅広い対応
- 優れた脆弱性の検出および修復機能

調査結果の要点: Fortifyによる迅速で効果的なソフトウェアセキュリティ保証の実現

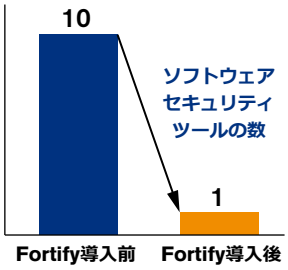
スキャンセットアップの迅速化

継続的デリバリ環境では、開発チームはセキュリティスキャンの計画と実行にすばやく取りかかる必要があります。しかし、現在の開発環境では、多様なプログラミング言語やコードコンポーネントが使用されているのが一般的で、この業務に必要かつ適切なセキュリティツールを用意し、さらに適切な要員と専門技術を揃えるのには時間がかかります。Fortifyへの移行前に、短期のリリースサイクル (毎週) の要件に対応できていたのは、今回の調査に参加した組織の半分以下でした。

Fortifyプラットフォームは、幅広い開発環境と言語に対応しているため、複数の個別ツールを使用して、ツールごとに専門の運用スタッフを確保する必要がなくなりました。平均して、1つのFortifyソリューションで10種類のツールを置き換えることができました。これにより、組織はソフトウェアセキュリティ環境を簡素化し、業務効率を改善することができました。お客様は、これがソフトウェアセキュリティのライセンスや保守に必要な全体コストの削減につながると考えていました。

必要なセキュリティツールの削減

お客様は、10種類の異なる個別ツールをFortifyに置き換えることで、統合やセットアップに要する手間を削減しています。



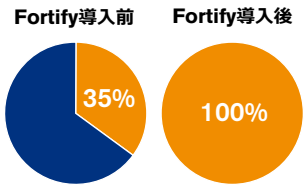
アジャイル環境の採用が増えるにつれて、開発ライフサイクル間でのプロセスの密接な連携が必要になっています。Fortify環境では、既存の開発環境との統合を容易にするためのツールやプラグインが利用できるため、Fortify環境に移行した組織は、コードのアップロード、スキャンの実行、および開発サイクルの各フェーズへのセキュリティチェックの組み込みに対応したプロセスの自動化を実現することができました。

実際、今回の調査では、リリースの頻度を改善 (1年または四半期に1回だったリリースを、毎月、毎週、または毎日のリリースに改善) できたお客様の割合が大幅に増加していました。Fortify導入前は、月1回または週1回のリリースが可能だと回答した企業は35%のみでしたが、Fortifyの高速ルールエンジン、テンプレート、およびトリアージテクノロジーの導入後は、ほぼすべての企業がリリーススケジュールの迅速化に対応できると回答しました。

セットアップの迅速化によるリリース頻度の向上

毎月または毎週のリリースサイクルのサポートが可能になる企業の割合

調査結果:
組織が同じ数量のリソースで毎週、毎月、または四半期ごとのリリースを行う能力が向上しています。



スキャン時間を短縮し、アプリケーションを改善する時間を確保

統合開発環境 (IDE) 内でスキャンを行うと、スキャンに数時間かかり、開発のオーバーヘッドが25%以上増えることがあります。このプロセスを高速化するため、あるFortifyのお客様は、開発者がコードをアップロードして数分でスキャンを実行できるHadoopリポジトリを作成しました。その結果、開発者は管理作業やセキュリティ作業に時間を取られなくなり、その時間をソフトウェアの改善に使えるようになりました。このお客様は、ソフトウェアがますます重要になる世界で、これが大きな競争上の優位性につながると考えています。

スキャンの効率化

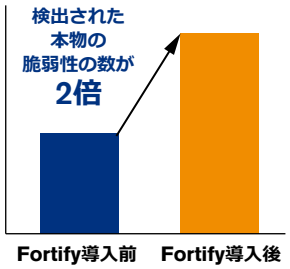
ほとんどの企業は、組織 (アプリケーションセキュリティ環境) に影響を与える、重大な上位10件の脆弱性への対処に重点を置いています。2017年に調査を行った企業では、これらにはクロスサイトスクリプティング (XSS)、SQLインジェクション、認証の不備、クロスサイト・リクエスト・フォージェリ、および不適切なセキュリティ設定などが含まれていました。

調査対象企業の半数以上が、比較的容易かつ安価に脆弱性を修復できる開発ライフサイクルの早い段階で、これらのリスクの高い脆弱性を見つけるのにFortifyが特に有効であると回答しました[6]。たとえば、Fortify Security Assistantなどのツールを使用することで、開発者はコーディング中にリアルタイムで脆弱性を識別できるようになりました。

全体として、Fortify Static Code Analyzerを使用した企業は、以前は識別できなかった数万の脆弱性を発見できるようになりました。さらに、調査対象企業はスキャンの実行に要する時間を (数日からわずか数時間または数分に) 大幅に短縮できたことで、開発者はスキャンを待機することなく、本来の業務である高品質なコードの作成に注力できるようになったと回答しています。

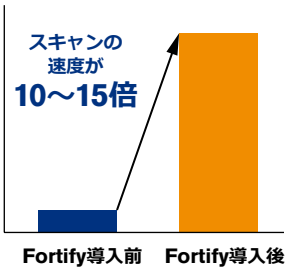
2倍の数の本物の脆弱性を検出...

お客様は、Fortifyで検出される本物の脆弱性の数が他のソフトウェアベンダーの製品の2倍であると報告しています。



さらにスキャンが大幅に高速化

お客様は、Fortifyによるスキャンが他のソフトウェアベンダー製品の10～15倍高速であると報告しています。



どのようなタイプの脆弱性が重要か?

当社の調査では、ほとんどの企業がクロスサイトスクリプティングやSQLインジェクションなどの一般的な脆弱性だけでなく、データセキュリティ侵害やそれによって起きる影響についても懸念しており、セキュリティ上の重要な懸念事項の1つと見なしていました。

適切なトリアージ、誤検出の削減

調査対象企業は、大量の脆弱性を検出し、関連性の深い脆弱性を識別し、誤検出やリスクの低い問題と重大な欠陥とをすばやく分離することで、MTTT (平均トリアージ時間) を大幅に短縮できるFortifyのユニークな機能に魅力を感じていました。

これらの企業の多くは、業界の最新のインテリジェンスとトレンドを考慮し、静的分析と動的分析を関連付けることで、トリアージルーチンの強化を図りました。いくつかの企業では、このようなトリアージ時間の短縮につながる手順を設計し実行するため、定期的にFortifyのエキスパートの力を借りていました。たとえば、ある主要なデータ分析企業では、日常的にコードをFortify on Demandにアップロードしてスキャンを行い、その後修復に着手する前にテクニカルアカウントマネージャーと、レビューおよびトリアージに関する合同セッションを行っています。

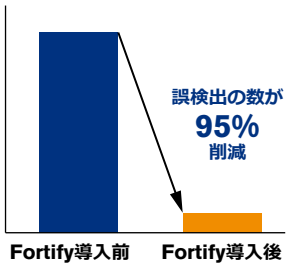
修復作業の改善

調査対象企業は、開発ライフサイクルの早い段階で脆弱性を見つけることの重要性を繰り返し強調し、ソフトウェアの本番稼動後に脆弱性が検出された場合、コーディング段階で脆弱性を検出するのに比べて、脆弱性を修復するのに100倍近い手間がかかることを指摘しています。品質保証テストで検出された脆弱性は、修復に要するコストは比較的少なくて済みますが、コーディング段階で検出した場合と比較すると、修復には約10倍の手間と時間が必要になります。

調査対象企業は、Fortifyを使用することで、トリアージ作業と修復作業を平均で約10倍速く (アプリケーションあたり20日かかったものがわずか1 ～ 2日で) 終了することができたと回答しています。こうして節約した時間は、ソフトウェアをエンドユーザーにとってより魅力的なものに改善する時間に充てることができます。

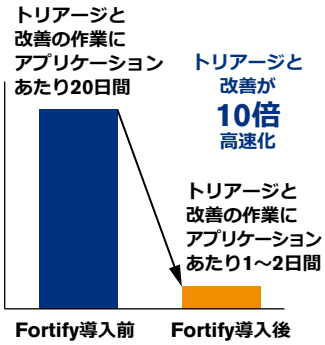
誤検出が少ない

お客様は、Fortify on Demandマネージドサービスにより誤検出の数が最大95%削減されたと報告しています。



迅速な修復

お客様は、Fortifyを使用するとトリアージと改善のプロセスを高速化できると報告しています。



誤検出が作業の遅れにつながる

ある大手金融機関は、大規模なアプリケーションでスキャンを行うと、50,000件もの脆弱性が検出されることがあり、このうちの60%は時間を浪費する誤検出、組織が重要とみなしていない欠陥、または分類を行うことでより効率的に修復できる脆弱性だと報告しています。この金融機関は、Fortifyのソフトウェアとマネージドサービスを使用して、誤検出を回避し、分析を通じてトリアージと修復の作業を改善することで、作業量を大幅に削減しました。あるITエグゼクティブは、「誤検出を解消しなければ、大規模化には対応できません」と指摘しています。

調査結果の要点: 継続的デリバリを牽引するFortifyのスケーラビリティ

アプリケーションの数が増えるのに伴い、組織はソフトウェアセキュリティプログラムを拡張し、リリースやアップデートのデリバリに遅れが生じないようにする必要があります。調査対象企業はいずれも、プロセスのスケーラビリティの妨げになる一連の要因を認識していました。これには、以下が含まれます。

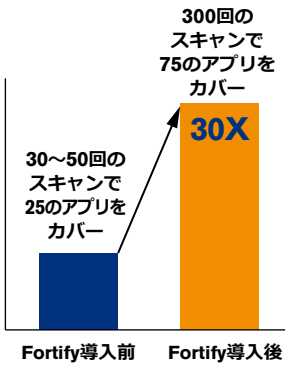
- 多様な個別ソリューション
- 手動プロセス/自動化の欠如
- 脆弱性の識別が不十分
- 誤検出が多い
- セキュリティの専門知識にアクセスできない

企業はFortifyソリューションと関連するマネージドサービスを組み合わせて使用することで、ソフトウェアセキュリティ保証を、エンタープライズレベルの開発を行う組織で増大する業務ニーズに対応できるスケーラブルで再現性の高いプロセスに変革することができました[8]。

本当の意味でのスケーラビリティとはどのようなものなのでしょうか。調査対象のある企業は、Fortify導入前には、四半期あたり約30 ～ 50回のスキャンを実行することができ、これにより約25のアプリケーションをカバーしていました。Fortify導入後は、300回のスキャンを実行して75のアプリケーションをカバーできるようになり、スピードと対応力が30倍高くなりました。

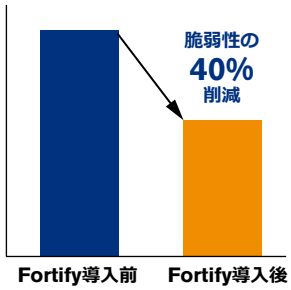
より多くのスキャンで、より多くのアプリに対応

お客様は、Fortifyおよびマネージドサービスサポートにより誤検出の数が最大95%削減されたと報告しています。



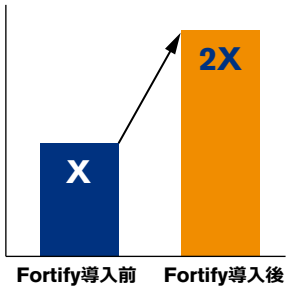
繰り返し現れる脆弱性の削減

お客様は、繰り返し現れる脆弱性が40%削減されることで、高品質でセキュアなアプリケーションを構築できると報告しています。



将来の拡張性

調査結果:
Fortifyのお客様は、将来的にスキャンされるアプリケーション数が2倍に増えると予想しています。



調査結果の要点: 市場投入までの期間短縮を可能にするFortify

Fortifyを使用してソフトウェアセキュリティテストと修復の迅速化と品質向上を行うことで、ソフトウェア開発ライフサイクルの期間が大幅に短縮されました。これは、組織内の各チームが短いリリース期限に対応するのに役立ちました。下の図に示すように、Fortify導入前は、テストに長い期間を費やしていました。これは、スキャンや修復の作業を行う頻度が少なく、これらの作業を開発サイクルの後半に行っていたためです。調査対象企業は、開発サイクルの後半にセキュリティ上の「サプライズ」が起きると、市場投入が脅かされやすいと報告しています。

Fortifyを使用すると、ライフサイクルの早い段階からコードをスキャンして、脆弱性の発見と修復を頻繁に繰り返し、高度なトリアージ手法を利用してサイクルをさらに短縮することができます。その結果、より多くの関連する脆弱性を検出して早い段階で修復を行い、最終段階でセキュリティ上のサプライズが起きるのを最小限に抑えることができます。さらに、開発者がセキュアなコーディングを学習することで、繰り返し現れる脆弱性が徐々に少なくなります。これは、今後のサイクルでよりセキュアな脆弱性の少ないコードを作成することにつながります。

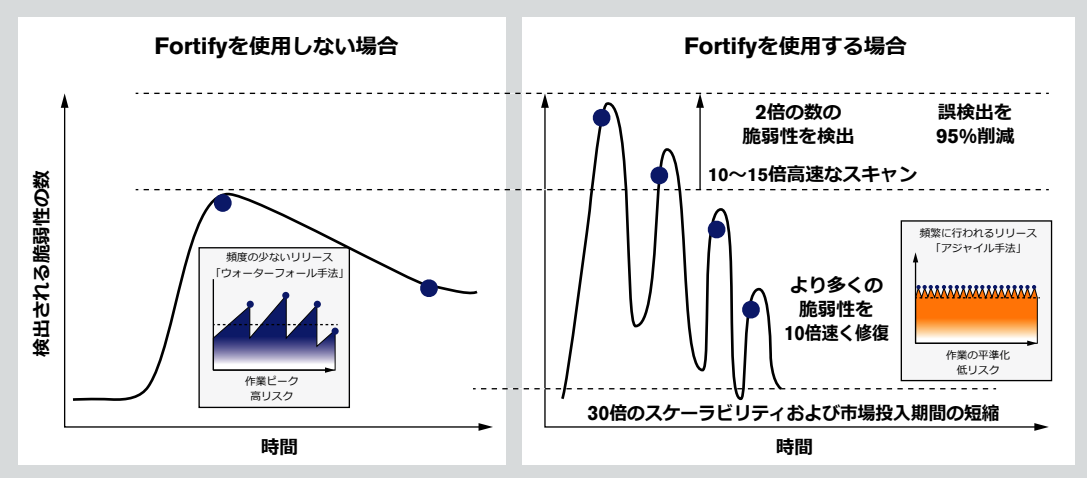
調査結果の要点: Fortifyによる外部開発パートナーの管理の改善

サードパーティ開発者の管理

多くの組織では、社内の開発者に加えて、コーディング作業をサードパーティに外部委託しています。しかし、これらの外部チームを含めてソフトウェアセキュリティプロセスを運用できるようにすることは、開発組織にとって複雑な課題になる可能性があります。

当社が調査を行った企業のいくつかは、Fortify on Demandを使用してセキュリティテストと品質管理をサードパーティ開発者に広げていました。一部の企業では、納品されたコードの「脆弱性の少なさ」に基づいてアウトソーシングパートナーに支払う金額を調整できる、革新的な「成果報酬」型のプログラムを構築していました。その結果、外部ベンダーに支払う金額に見合った製品品質の改善と価値の向上が実現しました。

Fortifyによる市場投入期間の短縮



利点のまとめ

以下の図は、組織がFortifyを採用することで実現できる利点をまとめたものです。業務の改善に加えて、多くの組織がFortifyの導入の効果として以下を挙げています。

- アプリケーションの市場投入の迅速化
- ディザスタリカバリとデータ侵害のコストの低減
- サードパーティ開発ベンダーのサービスからより多くの価値の入手

Fortifyによる業務改善のまとめ

利点	Fortify導入前	Fortify導入後
SSAセットアップの簡素化と時間短縮	10種類の個別ツール	エンドツーエンドの単一ツール
スキャンの高速化	アプリケーションあたり1～3週間	数時間から1日
より多くの脆弱性を検出	アプリケーションあたり数千件	検出される本物の脆弱性の数が2倍以上
トリアージと監査の迅速化	アプリケーションあたり1～2週間	1～2日
誤検出数の削減	アプリケーションあたり1,000～50,000	数十から数百、95%削減
修復作業の軽減	3～4週	1～2週
繰り返し現れる脆弱性の回避	繰り返し現れる脆弱性が一般的	繰り返し現れる脆弱性が40%削減
スケーラビリティ	四半期あたり30～50回のスキャンで25のアプリをカバー	四半期あたり300回のスキャンで75のアプリをカバー

継続的デリバリの実現を支援

Mainstayの以前の調査では、組織がより多くの脆弱性を見つけるのに役立ち、ソフトウェア開発ライフサイクルの早い段階で脆弱性の検出を行えるという点で、Fortifyをリーダーの1つに位置付けていました。今回の調査では、以前の調査の結論を明確に再確認できました。企業はFortifyを使用することで、競合ソリューションと比べて2倍の数の関連する脆弱性を検出できました。

ただし、今回の調査で、企業は成果を収める上で同じように重要な別の利点を指摘していました。これには、Fortifyで生成される誤検出が少ないことや、詳細な分析と相関付けを利用して本物の脆弱性を効率的に修復できることなどが含まれます。こうした機能を組み合わせることで、組織は開発環境の拡大とリリースサイクルの大幅な短縮に対応する手段を得ることができます。

Fortifyとの連携による優れたセキュリティ保証

SSAプログラムの潜在能力を最大限に発揮するために組織は、Fortifyソリューションに加えて、マネージドサービスやFortifyのプロフェッショナルサービスチームのリソースを活用しています。これには、予測可能で評価しやすいソフトウェアセキュリティプロセスを実現するのに役立つベストプラクティス、評価指標、およびテンプレートなども含まれます。

これからの方向性

競争力強化にソフトウェアを活用している企業にとって、アプリケーションの開発とアップデートを迅速に行えることは、戦略上不可欠なものになっています。アプリケーション開発チームは、1年または四半期に1回だったリリースを、毎月、毎週、または毎日のリリースに移行することで、継続的なソフトウェアデリバリのニーズに対応しています。

このため、ソフトウェアセキュリティチームは、できるだけ多くの脆弱性を、できるだけ早期に発見するだけでなく、いくつもの課題に対処する必要があります。テンポの速い継続的デリバリ環境と増加を続けるアプリケーション量に対応するには、セキュリティチームが自動化を推進し、業務効率をさらに向上させる必要があります。

主要企業を対象とした今回の調査では、Fortifyによって開発チームとセキュリティチームの状況が一変していることがわかりました。Fortifyのエンドツーエンドのアプリケーションセキュリティソリューションを使用すると、組織は、アプリケーションコードのテストと脆弱性の修正を、これまで以上に高速かつ効果的に実行することができます。スピードとパフォーマンスの押し上げを実現しているのは、誤検知をほぼゼロにし、根拠がしっかりした脆弱性を分離して迅速な修復を行う、新世代のトリアージツールおよびテクノロジーです。

これからは、リリースサイクルは速くなる一方で、IT部門には開発サイクルのさらなる短縮が求められます。ビジネスのソフトウェア依存度が高まる中で、急速な拡張に対応でき、継続的デリバリを実現するのに役立つ次世代型のセキュリティ保証テクノロジーを導入する企業が増えるのは当然の流れです。この新しい時代に、Fortifyは革新を続け、組織が高性能なアプリケーションセキュリティソリューションやサービスに対応できるよう支援していきます。

Fortifyの詳細については、fortify.comをご覧ください。

注

1 自動車メーカーであるテスラは、自社の自動車に問題があることを見つけた場合に、所有者に車内からソフトウェアをダウンロードしてもらうことで、ソフトウェアを所有者に直接提供します。これにより、テスラは何百万ドルものコストを節約できます。これに対して、従来の自動車では、設計または製造上の問題が見つかった場合にリコールを行う必要があり、多大なコストがかかります。

2『成果の改善と迅速化: 継続的なデリバリとビジネスパフォーマンスの改善に向けた取り組み』、Forrester Thought Leadership Paper、委託元: HP (現Hewlett Packard Enterprise)、2013年12月

3 平均的な開発組織では、10種類ものセキュリティテストツールや修復用ツールを使用しています。

4 今回の調査は、Fortifyソリューションのビジネスインパクトに関する以前の調査に基づいています。参照:『Does Application Security Pay? Measuring the Business Impact of Software Security Assurance Solutions』、Mainstay、2010年 (2013年更新)、http://h30528.www3.hp.com/Security/Fortify_Mainstay_ROI_Study.pdf

5『成果の改善と迅速化: 継続的なデリバリとビジネスパフォーマンスの改善に向けた取り組み』、Forrester Thought Leadership Paper、委託元: HP (現Hewlett Packard Enterprise)、2013年12月

6 ある主要銀行は、大規模なアプリケーションでスキャンを行うと、50,000件もの脆弱性が検出されることがあると報告しています。

7 Fortifyの複数のプログラミング言語に対応した50,000以上の定義済みルールが、より多くの脆弱性を発見するのに役立っていると、複数の企業が答えています。

8 一般的なFortify on Demand環境は、約400の開発者と、Java (80%)、.NET (12%)、モバイル (8%) を使用して構築された75のアプリケーションで構成されています。

9『成果の改善と迅速化: 継続的なデリバリとビジネスパフォーマンスの改善に向けた取り組み』、Forrester Thought Leadership Paper、委託元: HP (現Hewlett Packard Enterprise)、2013年12月

委託元:

Mainstay
www.mainstaycompany.com

2929 Campus Drive, Suite 150
San Mateo, CA, 94405

Phone: 650-638-0575
Fax: 650-638-0578

この事例研究の調査および分析は、Mainstayが実施しました。
Mainstayは、Cisco、Oracle、SAP、Microsoft、Dell、Lexmark、HP、EMC、
NetAppなどの主要なIT企業に関する300件以上の調査を行ってきた
独立系コンサルティング会社です。

この事例研究は、現在SSAソリューションを利用しているセキュリティ
エグゼクティブからの聴き取りに基づいています。本書に記載されている内容は、
信頼できる情報源から得たものですが、Mainstayが保証するものではありません。