ホワイトペーパー

セキュリティ

シームレスなアプリケーションセキュリティ：DevOps のスピードのセキュリティ

MICRO FOCUS

目次

ページ

製品化リードタイムは企業にとって重要なため、さまざまな組織で DevOps などのアジャイル手法が採用され、迅速な開発が行われています。実際に、企業は 2020 年までに、アプリケーションを通じて組織とやり取りするお客様とパートナー様の需要に対応するため、各アプリケーションの年間リリース回数を 30 回増やす必要があると考えています。

今日のアプリケーションセキュリティの課題

近年、ソフトウェアはビジネスをサポートするものからイノベーションの中核へと進化を遂げ、あらゆる業界と規模の企業にとって欠かせない、競争上の差別化要因となっています。こうしたソフトウェアの役割の変化に伴い、今日の企業ではアプリケーションの数とリリースの頻度が大幅に増加していますが、機能以外の要件はほとんど考慮されていません。また、スピードが求められ、モダンなアプリケーションの複雑化が進んだ結果、開発者がコードの再利用とオープンソースおよび COTS (市販の既製品) のコンポーネントに依存するケースも劇的に増加しました。このため、セキュリティチームが脆弱性を見つけ、管理することが非常に重要になっています。実際に、近年の有名なセキュリティ侵害の一部は、サードパーティコードのコンポーネントの脆弱性に起因しています。

ビジネスニーズに主導され、Web サイトや Facebook などのソーシャルメディアプラットフォームのアプリケーション、モバイルアプリケーション、クラウドアプリケーションが増えています。さらに、アプリケーションの中には、マーケティングチームが推進するものや、サードパーティソフトウェアによって作成されるものがあります。それらのアプリケーションは、通常のビジネスプロセス外にあることも多く、ガバナンスがほとんど行われていません。

アプリケーションの数の増加によって生じる多数の課題に加え、複雑化やリリースの短期化、GDPR などの規制、ビジネス目的での顧客データの取得が当然のことになっています。複数のインスタンスの顧客データを所有する場合は、セキュリティ侵害の確率と影響が増加します。今日のセキュリティ侵害の大半がアプリケーションの脆弱性によるものであるため、これは特に懸念すべき事項です。Micro Focus® Software Security Research の『2018 年アプリケーションセキュリティリスクレポート』によれば、アプリケーションの 80% に重大な脆弱性が 1 つ以上あり、セキュリティインシデントの 90% は、ソフトウェアの設計やコードの欠陥の悪用に起因しています。

課題は増加の一途

製品化リードタイムが企業にとって重要になるにつれ、迅速な開発を目指して DevOps などのアジャイル手法の採用が進んでいます。実際、2020 年までには、お客様やパートナー様の需要に対応するため、各アプリケーションを 1 年間に 30 回リリースすることが必要になると多くの企業が考えています。つまり、セキュリティがソフトウェアのライフサイクルに必須の要素とならなければ、驚異的なスピードで、多くの脆弱性を抱えたソフトウェアがリリースされる可能性があります。

従来のアプリケーションセキュリティの手法が機能しない理由

大半の組織では、アプリケーションセキュリティは開発の最終段階を担当するチームに割り振られており、スピードの阻害要因とみなされています。開発チームはセキュリティチームに対し、80 対 1 の速さで拡大[1]しているため、セキュリティチームは追いつくことができません。セキュリティの脆弱性が後半の段階で見つかると、組織はプレッシャーにさらされることになり、結果としてチーム間の摩擦や、リリースの遅延、さらに悪い事態を招く可能性があります。プロジェクトのスケジュールを順守するため、セキュリティ上の既知の不具合があるリリースが本番環境に導入され、企業やお客様が攻撃のリスクにさらされます。

リリースの遅れやチームの機動性の低下以上に、アプリケーションセキュリティにおいて事後対応型のアプローチを取ることは、コストの増加を招きます。NIST によると、セキュリティ上の不具合を修正するコストは、開発の初期段階で発見した場合と比べて、本番環境では 30 倍、テスト環境では 10 倍になります。こうした問題と潜在的なリスクのすべてが示しているのは、コストをかけずにアプリケーションを保護する唯一の方法は、シームレスなアプリケーションセキュリティモデルに移行することであるということです。

シームレスなアプリケーションセキュリティとは

シームレスなアプリケーションセキュリティとは、関係者にさらなる負担をかけることなく、アプリケーションセキュリティをソフトウェアのライフサイクルに必須の要素として組み込むことです。DevSecOps アプローチを取る場合でも、単により効果的なセキュリティプログラムを作成する場合でも、必要なのは、ライフサイクルの初期段階からセキュリティを考慮することです。アプリケーションセキュリティのベストプラクティスとテストは、ソフトウェア開発ライフサイクルプロセス全体に組み込む必要があります。これらを適切に実施することで、市場に要求される頻度のリリースサイクルを達成するためにアプリケーションセキュリティを犠牲にする必要がなくなります。

シームレスなアプリケーションセキュリティを実現する方法

シームレスなアプリケーションセキュリティを実現するには時間と労力がかかりますが、克服すべき最大の障壁は、ソフトウェア開発ライフサイクル全体にセキュリティを組み込むために必要な、文化の変化です。セキュリティチームと開発者の間のあつれきをなくすことが重要です。DevOps のように、チームの分断をなくし、透明性を高めて互いに連携することが必要です。これは「言うは易く行うは難し」ですが、経営陣の承認を得て、中心となる担当者を任命することで、このイニシアチブを推進できます。必要な文化の変更以外に、シームレスなアプリケーションセキュリティへの移行を成功させるための重要なステップは、以下のとおりです。

シームレスなアプリケーションセキュリティとは、関係者にさらなる負担をかけることなく、アプリケーションセキュリティをソフトウェアのライフサイクルに必須の要素として組み込むことです。

1 **出典：『10 Things to Get Right for Successful DevSecOps』、Gartner, Inc.、2017年**

コーディングの過程でセキュリティの不具合を見つけ、修正すれば、開発者はテスト環境や本番環境に移行する前に潜在的なセキュリティの脆弱性をなくすことができ、組織の時間とコストの削減につながります。

ステップ 1：セキュリティを考慮した開発

「開発者」対「セキュリティ専門家」の比率が 80 対 1 に増加している今、自身のコードに責任を持つよう開発者に権限を付与することは必要不可欠です。コーディングの過程でセキュリティの不具合を見つけ、修正すれば、開発者はテスト環境や本番環境に移行する前に潜在的なセキュリティの脆弱性をなくすことができ、組織の時間とコストの削減につながります。このような考え方への変化には、セキュリティを考慮してコーディングするよう開発者に対してトレーニングを実施し、コードについてリアルタイムのフィードバックを得るための適切なツールを提供することが必要です。開発者のセキュリティトレーニングには多数の選択肢がありますが、コードについてリアルタイムのセキュリティフィードバックを提供するツール (セキュリティスペルチェッカーのように動作して、開発時にコードについてリアルタイムのセキュリティを提供する Fortify Security Assistant など) や、統合ゲーム形式の開発者トレーニングであれば、簡単に導入し、短時間でトレーニングできます。さらに、セキュリティチームが既知の脅威に関する情報を共有し、フィードバックを提供するとともに、業務の透明化と可視化を図ることで、開発者を支援することも重要です。開発のリーダーがアプリケーションセキュリティのトレーニングを受講し、セキュリティ担当者としてセキュリティチームと連携することで、ポジティブな成果を上げることができます。このように、従来の機能と品質の視点に加え、開発のリーダーによって開発ライフサイクルの初期にセキュリティの視点が追加されます。

ステップ 2：初期に迅速なテストを頻繁に実施

ソフトウェア開発ライフサイクルには、今日のリリースへの対応に必要なスピードを維持するために従うべき、いくつかのアプローチがあります。このアプローチとは、初期に迅速なテストを頻繁に実施することです。

初期のテスト

静的アプリケーションセキュリティテスト (SAST) は、セキュリティ問題の根本原因を特定し、開発の初期段階に生じるセキュリティ上の不具合の修正を支援します。リリースのスピードを維持するため、開発者がインテリジェンスをすぐに使えるようにして、コードを迅速かつ簡単に送信できるようにする必要があります。Fortify Static Code Analyzer は、以下の機能によりこの方法を主導します。

- ソース、バイナリ、バイトコードの脆弱性の特定と解消
- スキャン結果のリアルタイムでのレビュー、推奨事項へのアクセス、およびコード行のナビゲーションによる脆弱性の迅速な検出と共同監査の実現
- 一般的な統合開発環境 (IDE) との完全な統合

Fortify Security Assistant は、コード記述時に、コードの脆弱性に関するインサイトと推奨事項を開発者にリアルタイムで提供することにより、これをさらに一歩進めます。これは、一般的な既知の脆弱性に対する開発者のセキュリティの「スペルチェック」として機能するだけでなく、そうしたミスが発生することを防止できます。

頻繁なテスト

動的アプリケーションセキュリティテスト (DAST) では、実行中の Web アプリケーション上の攻撃のシミュレーションや、セキュリティホールとなる脆弱性の特定を行います。セキュリティホールとなる脆弱性にフォーカスし、すべてのコンポーネント (サーバー、カスタムコード、オープンソース、サービス) を網羅することで、アプリケーションセキュリティを包括的に把握できます。開発、品質保証、本番環境に DAST ツールを統合することにより、継続的で包括的な情報が得られます。**Fortify WebInspect** は、以下の機能により効果的なソリューションを提供します。

- 既存のアプリケーションに存在するリスクの迅速な特定
- 開発から本番環境に至るまでのあらゆるテクノロジーの動的アプリケーションセキュリティテストの自動化
- 実行中のアプリケーションの脆弱性の検証と、根本原因分析のための最も深刻な問題の優先度設定
- 脆弱性の修正プロセスの合理化

迅速なテスト

インタラクティブアプリケーションセキュリティテスト (IAST) は、動的アプリケーションセキュリティテスト (DAST) と、テスト実行時にテストされるアプリケーションからのランタイムフィードバックを統合した、アプリケーションセキュリティテストの 1 つです。ただし、IAST アプローチを使用しても、脆弱性の検出は工数のわずか 3 分の 1 にとどまります。多くの場合、工数の残りの 3 分の 2 は、誤検出の検証と修正に費やされます。IAST に関するもう 1 つの反論は、このテスト方法は技術的に制約があるため、真の脆弱性を見落としてしまいがちであるという事実です。より効率的な代替方法として、機械学習アルゴリズムと監査自動化を適用すれば、時間と監査の工数を削減しながら、統計情報の分析の精度を向上できます。

Fortify Audit Assistant は、画期的な機械学習テクノロジーです。オンプレミスとクラウドの両方で提供される Fortify Audit Assistant は、スキャン結果のメタデータを活用して誤検出を予測して除去し、修正時間を 50% 短縮します。あるお客様は、8,000 件の Java に関する問題を検出し、このテクノロジーに基づいて 3,000 件まで減らしました。Micro Focus の 18.2 リリースは、このアプリケーションバージョンに自動予測機能を追加してお客様のプロセスをさらに自動化しており、新たな問題が追加された際に自動予測を自動的にリクエストします。

Fortify Audit Assistant は、セキュリティテストのフェーズで最も時間のかかる、スキャン結果の監査を合理化します。Fortify Audit Assistant は、幅広いセキュリティ知識と機械学習を適用し、誤検出の除去を自動化するとともに、結果に優先度を設定し、会社にとって重要なセキュリティ上の脆弱性を特定します。つまり、静的スキャンの開始後、数分後に検証済みのスキャン結果が得られ、修正対象として開発に送られます。

IAST アプローチを用いても、検出される脆弱性は労力のわずか 3 分の 1 にとどまります。多くの場合、労力の 3 分の 2 は、誤検出の検証と修正に費やされます。

ソフトウェア開発ライフサイクル全体に統合されたシームレスなアプリケーションセキュリティは、大幅なリスクの軽減とプロセスの制御を可能にし、最終的にはコストの削減、製品化リードタイムの改善、労力の最適化を実現します。

ステップ 3：統合機能の活用によるライフサイクルにおけるアプリケーションセキュリティの標準化

シームレスなアプリケーションセキュリティを実現するには、現在のツールとの統合機能を、ソフトウェア開発ライフサイクル全体で活用することが重要です。**Micro Focus Fortify** は、アプリケーションセキュリティソリューションで業界をリードする製品です。ソフトウェアライフサイクル全体を対象とした豊富な統合オプションが付属しており、動きの速いチームがアプリケーションセキュリティを使用できるようにします。今日の多くの組織では、様々な場所に多数のチームを擁しており、そうしたチームのすべてが異なる開発ツール、QA ツール、モニタリングツールを使用しています。必要とされる全社的な可視性とインサイトを得るためには、**Micro Focus ALM Octane** などのライフサイクル管理ツールを活用するのが一般的です。

ALM Octane と Fortify を統合することで、シームレスなアプリケーションセキュリティを実現する多数の主なメリットを得られ、ニーズに対応できます。セキュリティスキャンをビルドの一環として開始し、スキャン結果を ALM Octane に自動的にインポートできるため、効率的なガバナンスとトラッキングを行えます。そのため、セキュリティの脆弱性がコードに導入されるとすぐに公開され、チームに対してそれらをトラッキングし、修正するために必要な情報が提供されます。このプロセスにより、リスクを早期に特定するとともに、開発者の認識を高め、初めから脆弱性が含まれるコードを作成することがないようにします。

ソフトウェアの迅速な導入

静的スキャンと動的スキャンの自動化オプションに加え、Visual Studio、Eclipse、Jenkins などの一般的な開発ツールとの統合機能により、開発チームは時間を節約し、摩擦を避けることができます。JIRA や BugZilla などの不具合管理システムとの統合により、セキュリティ問題の対処と修正を向上するとともに、組織が機能の問題に対処するのと同様の方法で確実に対処することができます。こうした効率的なアプローチにより、ビジネスに必要なスピードに対応した迅速なソフトウェアの開発と導入が可能になります。

軽減されたリスク

セキュリティを早い段階に組み込み、ソフトウェアの開発ライフサイクル全体でシームレスに対応することにより、脆弱性をプロセスの早期に低コストで修正できるため、リスクが軽減されるとともに、関連コストが削減されます。**Fortify Security Assistant** と、ALM Octane や Jenkins の推進するセキュリティスキャンの自動化により、開発部門が早期に、さらにはプロセス全体にセキュリティテストを導入できます。

投資収益率の向上

Fortify は、既存の開発ツールと連動します。既存の投資を保護し、開発チームは引き続き好きなツールを使用できます。Fortify Security Assistant を使用すれば、既存の IDE 内で機能するため、コードのセキュリティスキャンを実行するために開発者が別のツールの使用法を学習する必要はありません。また、静的スキャンの統合機能により、セキュリティスキャンがビルドプロセスの一環として実行され、開発者がセキュリティ問題を不具合管理システム内で受信できるため、既存のツールやプロセスが複雑化することはありません。

ステップ 4：開発およびテストプロセスの一環としてのセキュリティの自動化

開発、プロセス、サーバーのプロビジョニング、アプリケーションの導入を自動化することが、DevOps イニシアチブで効率化を図るための鍵となります。自動化により、高品質のアプリケーションを迅速に開発し、リリースできます。シームレスなアプリケーションセキュリティの実現に向けて、迅速化を図りながら品質を維持するため、セキュリティテストと同様の方法で自動化を活用できます。セキュリティテストを自動化することにより、ユニットテストや統合テストのような自動化されたセキュリティテストを作成し、実行できます。

自動化された静的分析や動的分析により、ソースコードのセキュリティの脆弱性を効率的に特定し、セキュリティ評価にかかる多大な労力を最小限に抑えます。コードの自動分析は、コードのレビュー、セキュリティ評価、テスト時間を削減するだけでなく、脆弱性を早期に検出することにより、修正にかかるコストも削減します。

ステップ 5：リリース後のモニタリングと保護

あらゆるアプリケーションセキュリティイニシアチブの最初のステップは、リスクがどこにあるかを把握することです。これは、すでに脆弱性が存在している可能性のある本番環境では特に必要です。開発プロセスの一環としてセキュリティに対応することは優れたアプローチですが、本番環境の既存のアプリケーションを保護することも重要です。新規アプリケーションや問題のあるアプリケーション、リスクプロファイルの変更、ゼロデイ脆弱性により発生するアプリケーションセキュリティのリスクに対し、本番環境を継続的にモニタリングし、保護することが不可欠となっています。これは、ランタイムアプリケーション自己保護 (RASP) を活用することで行えます。

RASP は、ランタイム計測を使用して、実行中のソフトウェア内部からの情報を活用することで、コンピュータ攻撃を検出し、ブロックします。**Fortify Application Defender** は、本番環境の可視性を向上するとともに、さらなる調査のための「警告」を発します。

まとめ

ソフトウェア開発ライフサイクル全体に統合されたシームレスなアプリケーションセキュリティは、大幅なリスクの軽減とプロセスの制御を可能にし、最終的にはコストの削減、製品化リードタイムの改善、労力の最適化を実現します。統合および自動化されたアプリケーションセキュリティの実現に向けた明確な計画と、測定可能な KPI を設定することにより、会社の成功のチャンスが増大します。アプリケーションセキュリティは、他のサイバーセキュリティ関連の投資と比べ、メリットの実証が容易です。進捗状況と投資利益率を実証すれば、アプリケーションセキュリティへの継続的な投資が保証されます。

統合および自動化されたアプリケーションセキュリティの実現に向けた明確な計画と、測定可能な KPI を設定することにより、会社の成功のチャンスが増大します。

Fortify は、オンプレミス、オンデマンド、およびハイブリッドモデルの、柔軟なエンドツーエンドのシームレスなアプリケーションセキュリティソリューションを提供します。

そうしたプロセスのロードマップを作成する際に考慮すべき重要な点は、次のとおりです。

- シームレスなアプリケーションセキュリティの担当者を任命する
- 実装前に戦略と主要なプロセスを策定する
- 以下のような初期の領域と主要指標を規定する
  - 最初に開始するアプリケーションと開発チーム
  - SAST、DAST、またはその両方のどれを使用するか
  - どの統合機能を活用するか
  - オンプレミス、オンデマンド、ハイブリッドのアプリケーションセキュリティツールを使用するかどうか
  - ベースラインと比較した 12 か月の改善予測
- 組織に適したサポートを見つける

人、プロセス、テクノロジーは、シームレスなアプリケーションセキュリティの必須要素です。Micro Focus Fortify には、テクノロジー、人、プロセスに関して、(**Fortify on Demand** とプロフェッショナルサービスを通じて) すべてのステップをサポートしてきた経験とリソースがあります。

Fortify は、オンプレミス、オンデマンド、およびハイブリッドモデルの、柔軟なエンドツーエンドのシームレスなアプリケーションセキュリティソリューションを提供します。Fortify は、製品化リードタイムの 30 倍高速化、誤検出の 95% 減少、10 ～ 15 倍高速のスキャン、10 倍迅速な修正、脆弱性の検出の倍増など、**測定可能なメリット**[2] で、アプリケーションセキュリティツールの業界のリーダーとしての地位を確保し続けています。

Fortify を選ぶ理由は、以下のとおりです。

- **簡単に開始可能：Fortify on Demand** を使用して、1 日で開始できます。
- **使いやすさと既存プロセスとの直感的な統合：**Fortify は、開発者が使用しているお気に入りのテクノロジーと簡単に統合し、既存のツールやプロセスにセキュリティをシームレスに追加できます。
- **高速の自動化および拡張機能：**Fortify スキャンの大半は数分で完了し、生のスキャン結果から数分で機械支援の監査結果を取得できます。自動スキャンは、CI/CD パイプラインのコードのチェックイン、ビルド、リリースなどの構成要素の一環として開始できます。Fortify のお客様は、一元的なスキャン手法、Fortify on Demand、またはハイブリッドアプローチを使用して、簡単にオンプレミスで拡張できます。
- **プログラミング言語の精度とカバレッジ：**Fortify のお客様は、他の製品に比べて多い真陽性 (多い検証済みの結果) と少ない誤検出 (少ないノイズ) をレポートします。Fortify は、2018 年 11 月時点で、25 のプログラミング言語に対応しており、非常に幅広いプログラミング言語をカバーしています。
- **継続的な業界の認知度：**Fortify は過去 13 年でアプリケーションセキュリティのリーダーとして認知されています。Gartner 社の「Magic Quadrant for Application Security」で 8 年連続リーダーとして認められており、世界中のさまざまな業界のトップ企業に信頼されています。

2 **出典：『Continuous Delivery of Business Value with Micro Focus Fortify』、Mainstay Customer Evidence Research**

お問い合わせ先：
www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp