Micro Focus Fortify の SAST と DAST を選ぶ 5 つの理由

静的アプリケーションセキュリティテスト(SAST)と動的アプリケーションセキュリティテスト(DAST)の方式を組み合わせることで、アプリケーションのリスク状況を包括的に把握できます。Micro Focus FortifyのSASTとDASTを選ぶ5つの理由をご説明します。

静的アプリケーションセキュリティテスト (SAST) と動的アプリケーションセキュリティテスト (DAST) の方式を組み合わせることで、アプリケーションのリスク状況を包括的に把握できます。静的分析ツールでは、ソフトウェア開発ライフサイクル (SDLC) の初期段階において徹底的なフィードバックを提供します。動的分析ツールでは、本番環境または本番前の環境のいずれかにおいて、悪用される可能性のある脆弱性をただちに検知することにより、セキュリティチームによる迅速な対応を可能にします。この 2 つの方法でテストすることにより、アプリケーション内の弱点と脆弱性によるリスクの全体像を把握することができます。

1.

テスト全体で分類法が統一されているため、脆弱性の全体像を把握できます。Micro Focus Fortify のソフトウエアセキュリティリサーチ (SSR) チームは、アプリケーションセキュリティ業界の専門家チームです。このチームは、Micro Focus の静的、動的、ランタイム製品を制御するルールを作成します。新たな脆弱性を調査する場合は、このチームが協業して検知のための最も効率的で最適なモダリティを特定します。Fortify では、3 つのすべてのテスト方法で統一した分類法を使用するため、まず Fortify Static Code Analyzer (SCA) でソースコードの弱点を発見し、次にその弱点が実際の脆弱性となる稼働環境においても同じ検出が行われることを、Fortify WebInspect の動的分析により確認することができます。静的分析と動的分析の両方で脆弱性を検出できる場合は、正確性と速度に重点を置きつつ各テクノロジーにルールが提供されます。

お客様にとっての価値

静的・動的アプリケーションセキュリティテストは、SDLC 全体 (開発から QA、あるいは本番まで) で脆弱性を特定する機能を互いに補完しあうテクノロジーです。これらの 2 つのテクノロジーを共通の分類法で統一することで、それぞれのテクノロジーが相互に補強され、組織の脅威となる脆弱性の全体像を把握できるため、包括的なソリューションが実現します。

実際の例

強度の弱い基本的な SSL 暗号の脆弱性について考えてみます。この脆弱性は静的テストと動的テストの両方で検知できます。検知された場合は、本番環境へのアプリケーションの導入に大きく影響します。静的テストのモダリティでは、一般的にアプリケーション内から SSL が構成されている場合の限られた結果しか返されませんが、動的テストでは、SSL がアプリケーションの外部で終了した場合の Web サーバーの構成も確認できます。Fortify では、共通の分類法を利用するツールを活用することにより、脆弱性の実際のセキュリティリスクを高い正確性で分析することが可能です。

1. テスト方法の分類法が統一されているため、脆弱性の全体像を把握できます。
2. 一貫した修正ガイダンスによりコラボレーションと修正が可能です。
3. 強力な優先度設定によりノイズを軽減します。
4. 多層防御で安全を実現します。
5. 統一された脆弱性管理によりフィードバックループを実現します。

2. **一貫した修正ガイダンスにより、コラボレーションと修復が可能になります。**静的と動的の両方のテスト方法で統一した分類法を使用するため、推奨されるアドバイスとセキュリティマッピングを開発者が共有することができます。

お客様にとっての価値
開発者にとって使いやすい言語のソフトウェアを使用することで、開発者はレポートを理解するためのトレーニングに多くの時間を費やす必要がなくなり、脆弱性の調査ではなく修正に多くの時間をかけることができます。

実際の例
DevOps の手法が普及するにつれて、アプリケーションセキュリティにおいては、チームスポーツのような連携が重要になっています。開発、運用、セキュリティの各チームには、SDLC の各段階で使用されるツールから脆弱性についての一貫した詳細情報を受け取る必要があります。脆弱性に関する共通の分類法に基づいた Fortify の静的および動的テストテクノロジーを活用することで、脆弱性について明確で簡潔な方法でチームが連携することができます。

3. **強力な優先度設定によりノイズを軽減します。**すべての脆弱性が同じように生じるわけではありません。ソースコード分析によって特定された脆弱性は、コード外で緩和され、実際にはリスクスコアが低くなる可能性があります。静的分析に加えて動的分析を行う事で、より完全な実世界のリスク全体像を見ることができ、追加のリスク指標を得ることができます。

お客様にとっての価値
すべての問題を修正することは現実的ではありません。現在のアプリケーションセキュリティの専門家は、どの問題を修正し、どの問題を保留にするか、難しい判断が求められます。静的分析と動的分析の両方で統一した分類法を活用することで、最初に修正すべき項目を選択できる追加の指標を得ることができます。全体的なセキュリティ体制が強化されるだけでなく、開発者は最も重要な調査結果に最初に集中できるため、時間を効率的に使用できます。

実際の例
今日のアプリケーションセキュリティプログラムでは、様々なテクノロジーと手法によってリスクを軽減しています。静的分析は、脆弱性のカテゴリを広範囲にわたって詳細に特定するのに優れていますが、本番アプリケーションのコンテキストには対応できません。Web アプリケーションファイアウォール (WAF) でクロスサイトスクリプティング (XSS) を保護している組織は、安全でないデシリアライゼーションなど、WAF で保護されていない脆弱性の修正を優先することになります。

4. **多層防御で安全を実現します。**静的分析では、広範囲にわたって問題を分析できますが、構成とデプロイメントのオプションがアプリケーション全体のリスク状況に多大な影響を及ぼす可能性がある本番環境に対しては実行できません。動的分析により、SDLC 後半で問題を特定し、最大のリスクをもたらす本番環境で問題を特定できます。

お客様にとっての価値
DAST は、SAST では特定できない脆弱性のセーフティネットとして機能します。セキュリティチームは、静的分析を活用して SDLC の初期段階で脆弱性を特定し、動的分析を使用して SDLC の後期段階および本番環境で顕在化する脆弱性を特定することにより、より高いセキュリティを提供する階層型アプローチを実現することができます。

実際の例
DevOps サイクルによってリリースサイクルが短くなり、セキュリティ上の欠陥を特定して修正する機会が増えることは事実ですが、リリースの回数が増加しているため、ミスの発生も増えています。動的分析では、開発者のミス、デプロイメントエラー、環境の微妙な差異によってセキュリティの隙間をすり抜ける脆弱性を効率的に特定できます。

5. **統一された脆弱性管理によりフィードバックループを実現します。**セキュリティチームと開発チームがリスクを特定して修正する際には、様々な要因を考慮する必要があります。Micro Focus Fortify は、調査結果を簡単に分析できる統合された脆弱性管理プラットフォームを提供するため、チームが考慮すべき要因が 1 つ減ります。

お客様にとっての価値

セキュリティチームには、特定の分野に特化した複数のポイントソリューションから大量のセキュリティ情報が届きます。統合されたアプリケーションセキュリティ脆弱性管理プラットフォームの重要性は、簡素化された優先度設定とそれによるトリアージのワークフローを実現できるだけでなく、データからパターンを収集できることにあります。

実際の例

統合された脆弱性管理プラットフォームを使用することの最大の利点は、データが中心であるということです。このメリットの基本的な例は、脆弱性のパターンの発見です。静的分析などのテクノロジーにより SDLC の初期段階で脆弱性を特定することは重要ですが、DAST スキャンによりこれらの調査結果が実行環境でいつ顕在化するかを特定できるフィードバックループを作成することも極めて重要です。SDLC の初期段階で XSS などの問題を特定し、本番環境でそれらの問題を検知することができれば、体系的にトレーニングと開発のリソースを問題の対処に集中させることができます。

詳細情報はこちら：
https://www.microfocus.com/ja-jp/solutions/application-security

Micro Focus Static Code Analyzer について

Micro Focus Fortify Static Code Analyzer (SCA) は、ソースコードにおけるセキュリティ脆弱性の根本原因を特定し、問題の重大度に基づいて優先度を設定して、詳しい修正方法を提供します。開発者は、一元管理されたソフトウェアセキュリティ管理を通じて迅速に問題を解決できます。

Micro Focus WebInspect について

Micro Focus Fortify WebInspect は、デプロイ済みの Web アプリケーションとサービスについてアプリケーションの脆弱性を特定するための動的アプリケーションセキュリティテスト (DAST) ツールです。

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