MICRO FOCUS

お客様成功事例

セキュリティ

SAP

SAP SE（以下、SAP）は、エンタープライズソフトウェアおよびソフトウェア関連サービスの売上においてトップの企業です。この位置づけを維持するため、SAP は、最高品質のソフトウェアソリューションの提供に取り組んでいます。これには、単にリスク管理とセキュリティ管理を Idea2Market (I2M) プロセスに統合して設計どおりに動作するアプリケーションを提供する以上のことが必要です。Micro Focus® Fortify は、このプロセスに不可欠な要素です。2012 年の時点で、SAP は Fortify を使用して約 1 億 7800 万行の重要な Java コードの静的分析を実施しています。

概要

SAP の製品セキュリティ戦略では、製品開発中の静的コード分析が義務付られており、すべてのアプリケーションの安全性とサイバー攻撃の脅威に対する耐障害性を確保することで、ソフトウェア障害による経済的損失、知的財産の損害、または業務の中断から、お客様、そして SAP 自身を保護しています。

SAP は、同社固有の ABAP 言語で書かれたアプリケーションには独自の静的分析ツールを使用していますが、同社内で ABAP に続いて最もよく使用されているプログラミング言語である Java に対しては、サードパーティの専門知識を活用することにしました。SAP は業界のリーダーを選択し、Fortify ソフトウェアを開発ライフサイクルに完全に統合しました。

「Fortify ソフトウェアは、開発ライフサイクルの早い段階で脆弱性を検出できるため、当社の製品セキュリティ戦略の実現に不可欠な要素となっています。脆弱性を早く発見できれば、より効率的に修復できるからです。Fortify ソフトウェアは、SAP のコードの安全性向上に確実に役立っていると言えます。」

UWE SODAN氏

TIP Security, Engineering Excellence and Education, Code Analysis Team Manager
SAP

課題

「Java コードは、重複を除外して約 8000 万行あると見積もっています」と、SAP の TIP Security, Engineering Excellence and Education, Code Analysis Team Manager、Uwe Sodan 氏は説明します。「さらに、多数のアプリケーションについて旧バージョンを維持する必要があるため、特定の製品を複数回スキャンすることがよくあります。当然、常に最新バージョンについてスキャンしますが、修復が必要なものが見つかるたびに、古いバージョンについてもどこまで修正する必要があるか検討しなければなりません。」

ソリューション

Fortify 導入の現場

SAP では、Java、C#、JSP、および、その他複数のプログラミング言語で書かれたアプリケーションの静的コード分析を、Fortify で設計および導入しています。ベースとなるのは、Fortify Software Security Center (SSC) および Fortify Static Code Analyzer (SCA) ソリューションです。

Fortify Software Security Center は、ソフトウェアがデスクトップ、モバイル、または

SAP

概要

■ 業種

ソフトウェアおよびテクノロジー

■ 所在地

ドイツ、ヴァルドルフ

■ 課題

Java、C#、JSP、およびその他言語で書かれたアプリケーションコードに対して静的分析を実行し、ソフトウェア開発ライフサイクルの早い段階で脆弱性を特定して修正する。

■ 製品とサービス

Fortify Software Security Center (SSC)
Fortify Static Code Analyzer (SCA)

■ 成果

+ SAP および同社の顧客をソフトウェア関連の経済的損失、業務の中断、企業ブランドへのダメージから保護
+ ソフトウェア開発ライフサイクルの早い段階で脆弱性を特定・修正することで、修復のコストを抑制
+ 新しいアプリケーションおよび旧バージョンに対して効率的に静的分析を実行可能

クラウドのどこで構築されたかに関わらず、社内および外部のセキュリティ要件の遵守を確保することで、組織のセキュリティリスク管理をサポートします。高度な静的および動的セキュリティテスト機能と、予防的セキュリティ管理のための統合型フレームワークを通じて、Fortify SSC は開発プロセスおよびレガシーアプリケーション、そしてソフトウェア開発ライフサイクル全体に存在するリスクを特定し、低減します。SAP の開発グループは分散されていますが、同社は Fortify SSC 内ですべての結果を統合し、追跡できます。

Fortify Static Code Analyzer は、Fortify SSC ソリューションの一部です。受賞歴のある静的分析を使用し、ソースコード中の脆弱性を広範囲にわたって検出します。Fortify SCA はソースコード中のセキュリティ脆弱性の根本原因を特定し、リスクの重大度に基づいて分類された結果に優先度を設定して、脆弱性の修正方法についてコード行レベルの詳細なガイダンスを提供します。Fortify SCA は、組織がソフトウェアの信頼性を確保し、アプリケーション脆弱性検出および修正のコストを抑制するとともに、安全なコーディングベストプラクティスの基盤を確立するのに役立ちます。

「SAP には、製品セキュリティ規格を担当するコアグループがあります」と、Sodan 氏は説明します。「当社の製品セキュリティ戦略は、分散された開発チームが一元化されたガイダンスに沿って安全な製品を開発することを目標としています。セキュリティ要件は一元的に収集、維持、記録、ロールアウトされる、機能外の要件の一部です。開発ライフサイクル全体にわたるテスト手法を定めており、静的分析は必須となっています。Fortify ソフトウェアは、我々のビジネスの成功に不可欠な要素なのです。」

Micro Focus Services からのサポートも、ソリューション全体の重要な要素です。「2 年間にわたり、現場常駐コンサルタントの専門知識に大いに助けられました」と、Sodan 氏は語ります。「ツールだけでなく、プロセスの側面からも、チームが Fortify ソフトウェアを理解できるように教えてくれました。」

利点

このソフトウェアのどこに最大の価値を見出しているかという問いに、Sodan 氏は複数の利点を挙げました。「第一に、セキュリティカバレッジが優れている点です。」「また、Fortify Software Security Center でのコラボレーション機能も我々にとって重要です。データを保護し、アクセスを管理するには、スキャン結果をすべて保存できる中央集約型のインフラストラクチャが望ましいですし、このインフラストラクチャは、複数の開発チームが容易に結果にアクセスして作業できるものでなければなりません。Fortify ソフトウェアは、我々の開発モデルにとても合っています」。

もう 1 つの重要な利点は、お客様の特定のニーズに合わせて Fortify ソフトウェアを構成できる機能です。「これにより、結果の分類と優先度設定の両方、および微調整が可能になります」と、Sodan 氏は説明します。「カスタムルール機能で独自のルールを作成し、ツールの挙動を変更して、専有のライブラリ、インターフェイス、フレームワークに適応させることができます」。

開発者の生産性向上は SAP の主要な目的の 1 つであるため、SAP は、Fortify ソリューションにカスタムルールと修正推奨事項を適用しています。Sodan 氏は、検出結果の解釈方法に関するドキュメントが豊富なことと、脆弱性修正に関する詳細なガイダンスが、SAP 開発環境における Fortify ソフトウエアの価値を一層高めていると付け加えます。

Fortify ソフトウェアの使用を推進する 1 つの要因は、SAP の製品規格セキュリティ要件遵守の必要性です。「すべてのソフトウェアについて、クロスサイトスクリプティング (XSS)、SQL インジェクション、パストラバーサル、メモリ破壊、XML エンティティ、バッファーオーバーフローなどを回避する必要があります」と、Sodan 氏は語ります。「また、OWASP Top 10 および CWE/SANS Top 25 の脆弱性も常に参照しています。これらが当社の静的分析の対象範囲です。SAP のすべての製品において、これらの脆弱性を除去しなければなりません。これらの厳格な要件に対応し、お客様と当社の企業ブランドを守るにあたり、当社は Fortify ソフトウェアを信頼しています。」脅威がより巧妙な標的型のものになっても、静的コード分析により、脆弱性が悪用される前にそれらを特定し回避することで、SAP は競争上の優位を確保することができます。

早期に修正

SAP は、Fortify ソフトウェアをその開発ライフサイクルに完全に統合しました。具体的な数値はまだ出ていないものの、費用対効果はすでに明白になっています。「最もコストがかかる修正は、バグが本番機に影響し、お客様、または外部のセキュリティ専門家がそれを報告してきたときです」と、Sodan 氏は説明します。「複数の研究によると、リリース済みソフトウェアと開発ライフサイクル中の脆弱性修正コストは、約 100 対 1 の比率となっています。これが、コードをできる限り早期にチェックすることが重要であると考える理由です」。

SAP では、1,000 人近くの開発者が積極的な Fortify ソフトウェアのユーザーです。「Java 開発者全員ではありませんが、各開発チームで 1 ～ 2 人以上をターゲットとしています」と、Sodan 氏は説明しています。Fortify SCA の Eclipse プラグインは、この環境で特に役立ちます。「開発者は、このプラグインですぐにチェックを実施できるため、処理中にコードを直接改善することができます」と、Sodan 氏は語ります。「また、プラグインとセントラルサーバーの統合も気に入っています。開発者が動作を理解すれば、普段の開発環境で直接スキャン結果を利用できます。これも利点の 1 つです。」

SAP には、セキュリティに関する包括的なフィードバックプロセスがあります。外部から報告された潜在的脆弱性はすべてセキュリティ対応プロセスにおいて修正され

ます。その後、別のフィードバックステップで脆弱性パターンを分析し、静的分析でそれが検出されるか判断します。その結果が「Yes（検出される）」であり、かつ影響を受けるコードがJavaまたはSAPがFortifyを使用しているその他言語のいずれかに属する場合は、根本原因を分析し、その脆弱性がスキャンの範囲外なのか、またはツールの調整が必要なのかを調べます。このフィードバックプロセスによって、SAPはFortifyソフトウェアの使用を継続的に調整し、最適化することができます。

「Fortifyが対象としているプログラミング言語の数、および脆弱性のタイプやパターンに対応したチェックカテゴリの数を考えると、このソリューションはかなり完全であると思います。」Sodan氏は締めくくります。「Fortifyソフトウェアは、開発ライフサイクルの早い段階で脆弱性を検出できるため、当社の製品セキュリティ戦略の実現に不可欠な要素となっています。これは我々にとって不可欠な要素です。脆弱性を早く発見できれば、より効率的に修復できるからです。Fortifyソフトウェアは、SAPのコードの安全性向上に確実に役立っていると言えます。」

成果

Fortifyは、アプリケーションセキュリティの向上を通じて、SAPおよびその顧客をソフトウェア関連の経済的損失、業務の中断、企業ブランドへのダメージから守っています。さらに、ソフトウェア開発ライフサイクルの早い段階で脆弱性を特定し、修正できるため、修復コストが抑えられます。また、新しいアプリケーションと旧バージョンに対して静的分析を効率的に実行できるため、SAPはこれまでに1億7800万行以上のコードをスキャンしています。

Fortifyの導入で、SAPの開発者のスキルが向上し、開発プロセスも改善されました。Fortifyソフトウェアツールおよびプロセスの詳細なトレーニングを通じ、安全なコーディングプラクティスに対する開発者の意識が大幅に高められました。FortifyのEclipseプラグインにより、コード開発中にすばやく簡単にセキュリティチェックを実施できます。また、Fortifyは、特定された脆弱性の修正に関して、コード行レベルの詳細なガイダンスを提供します。さらに、SAPは、特定の顧客の要件に合わせてFortifyソフトウェアをカスタマイズすることができます。そして、パイロットプロジェクトや製品カスタマイズを支援する現場常駐エキスパートのコンサルティングが、導入を成功させる鍵となりました。

詳細情報はこちら：
software.microfocus.com/software/fortify

「2 年間にわたり、現場常駐コンサルタントの専門知識に大いに助けられました。ツールだけでなく、プロセスの側面からも、チームが Fortify ソフトウェアを理解できるように教えてくれました。」

UWE SODAN氏
TIP Security, Engineering Excellence and Education, Code Analysis Team Manager
SAP

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