ホワイトペーパー

Micro Focus Security Fortify

Audit Assistant

MICRO FOCUS

目次

はじめに

Micro Focus® Security Fortify Static Code Analyzer (SCA) の結果に対して、機械学習を利用した監査が可能になりました。

Micro Focus Security Fortifyによって、アプリケーションセキュリティテストの歴史上初めて、SCA結果から得られるコンテキストアウェアネスとセキュリティ専門知識の活用と再現が可能になります。

開発した理由

静的コード分析の基本的な問題は、その結果を何かしらのアクションに結びつけるために人手による監査が必要なことでした。監査作業が、付加価値を生まない時間の最大の部分を占めているのです。

提供する価値

- 人手による詳細な検査が必要な問題の数を削減
- SDLCの早い段階で関連する問題を特定
- アプリケーションセキュリティの確保を既存のリソースで実現可能
- 監査とレポート作成での一貫性の維持
- 既存のFortify製品のROIの改善

静的アプリケーションセキュリティテストが必要な理由

静的アプリケーションセキュリティテスト (SAST) とは、ガートナーの定義によると、アプリケーションのソースコード、バイトコード、またはバイナリコードを分析してセキュリティ脆弱性を検出する製品やサービスの市場です[1]。米国国立標準技術研究所 (NIST) によると、静的解析ツールは、開発中あるいは展開後にソフトウェアのセキュリティ脆弱性を取り除くための最後の砦の1つです[2]。これらのソフトウェアセキュリティツールやサービスは、敵対者に利用されて企業に損害を与える恐れがある脆弱性につながるソースコード内の弱点を報告します。ソースコードにセキュリティ上の弱点があると、企業にとってのリスクが増えることになります。このようなリスクは、SASTを実行しない場合は発見できません。静的アプリケーションセキュリティテストを利用することで、企業はリスクを知り、セキュリティに対する姿勢を改め、ビジネスを守るために情報に基づく意思決定を行うことができます。

ソフトウェアの脆弱性は深刻な問題であり、単純な誤りや、不十分なセキュリティ手法や、内部の脅威主体による意図的行為によって導入されます。多くの場合、ソフトウェア開発プロセスは、このような脅威を最小化するように制御されていません。静的分析を利用することで、企業は、アプリケーションのソースコードから生じるビジネスリスクの特定、監視、削減に必要な情報を入手し、問題解決のための推奨される方法を知ることができます。静的コード分析は、20年近くにわたり、デジタルエンタープライズのセキュリティ確保に不可欠な要素として認識されてきました。米国大統領の情報技術諮問委員会が1999年のレポートで述べたように、従来の標準的なソフトウェア開発方法では、ITインフラストラクチャーで要求される高品質、高信頼性、高セキュリティのソフトウェアを実現することはできません[3]。

---

1 Gartner 「Magic Quadrant for Application Security Testing」、2015 community.hpe.com/t5/Protect-Your-Assets/HP-Fortify-The-Undisputed-Leader-in-2015-Gartner-Magic-Quadrant/ba-p/6776163#.WC5FZrIrKM8

2 NIST Source Code Security Analyzers samate.nist.gov/index.php/Source_Code_Security_Analyzers.html

3 NITRD 2005 President's Information Technology Advisory Council nitrd.gov/Pitac/Reports/20050301_cybersecurity/cybersecurity.pdf

ソフトウェア脆弱性の確認

SASTレポートでは、問題が重要度別に分類されています。その後に、専門のアプリケーションセキュリティ監査者による確認作業が行われ、問題が悪用可能か、あるいは非問題かが判別されます。非問題という判定には、いくつもの理由があります。検出自体が誤検出である場合もありますが、もっと多いのは、組織のポリシーのために検出が無関係であったり、軽減策が実施されているため悪用が不可能であったり、脆弱性のあるコードが実際には実行されなかったりする場合です。

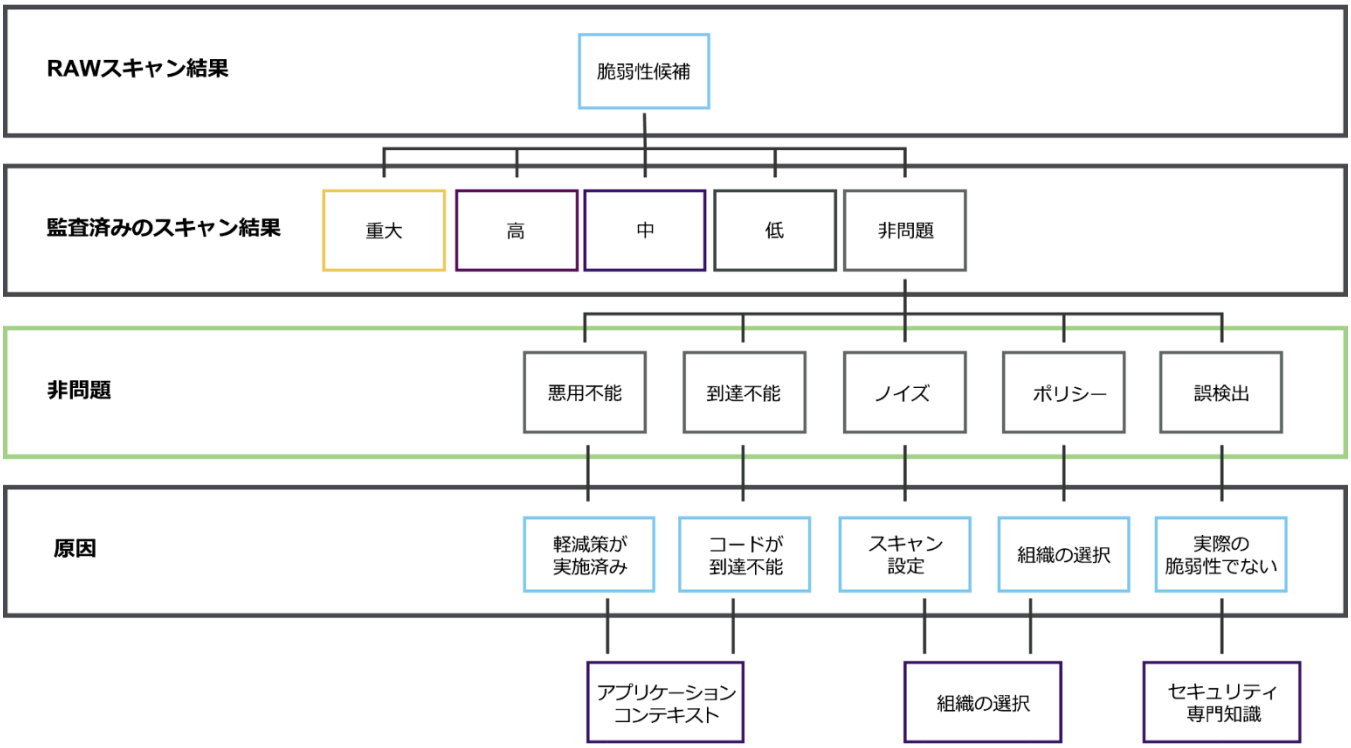

図1: スキャン検出結果の分類

SASTツールは、汚染、構造、制御フロー分析といったさまざまな分析方法を使用して、アプリケーション内の潜在的な脆弱性を検出して報告します。専門監査者は、アプリケーションと展開のコンテキストといった会社に固有の詳細情報を使用して、検出結果を検証する必要があります。潜在的なソフトウェアセキュリティ脆弱性が非問題であると監査者が判定した場合、検証に費やされた時間は付加価値を生まない時間です。このような時間のかかる監査は、企業にとって多大なコストがかかり、セキュアなアプリケーションの実現にとっての基本的な課題となってきました。問題は、ツールやテクノロジーによって生成された情報が即座に利用可能とはならないことです。

ソフトウェアセキュリティの確保の課題をさらに難しくしているのが、よく知られているサイバーセキュリティスキルのギャップです[4] 。スキルのあるセキュリティプロフェッショナルは、当然、高額の給与を要求します。また、定義上、どれほど能力のある個人でも、企業全体のニーズに効果的に対応することはできません。静的分析ツールは、コードのセキュリティ確保という不可能な仕事を可能にするものであり、スキルのある監査者のソフトウェアセキュリティに関する専門知識は、検出結果の実用性を検証する役割を果たします。最高のセキュリティチームであっても、結局は利用可能な人手による制限を受けます。このため、組織が直面している膨大な数の潜在的なソフトウェア欠陥には、到底対処しきれません。セキュアアプリ

[4] CSO Online csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

ケーションの次の進化は、機械学習を利用して、アプリケーション開発のセキュリティ確保の速度と効率を改善することから始まります。この手法により、セキュリティプロフェッショナルの専門知識の到達範囲とスケールが拡大し、セキュリティ開発のライフサイクル全体をカバーできるようになります。

機械学習と予測分析: 次世代のSAST

情報の実用性の問題には、Micro Focus Security Fortifyのスキャン分析プラットフォームによって対処できます。Micro Focus Fortifyは、Fortify on Demandを通じて、この方法を1年以上にわたって検証してきました。その結果、問題監査のプロセスに画期的な進歩がもたらされたのです。オンプレミスのお客様も、Fortify Software Security CenterのAudit Assistant機能を通じて、この機能を利用できるようになりました。Audit Assistantは、新しい静的スキャン結果の中から、組織に固有の悪用可能な脆弱性を識別します。この識別は、スキャン分析の機械学習分類機能によって行われます。この機械学習のトレーニングには、スキャン結果から得られた匿名のメタデータを、ソフトウェアセキュリティの専門家が事前に監査した結果が用いられています。スキャン分析プラットフォームでは、この機能はクラウド上のWebサービスとして提供されています。この機能によってSCAスキャン結果に付加される監査予測は、98%の精度を持ちます。

Audit Assistantにより、機械学習を使用した監査が可能になり、Micro Focus Security Fortifyコミュニティ全体のセキュリティ専門知識を、機密情報を一切送信することなく利用できます。Audit Assistantが送信するのは、スキャン結果から得られた**匿名問題メトリックス**と呼ばれる匿名のメタデータだけです。スキャン結果やコードが、SSC環境の外に出ることはいっさいありません。実証済みのFortify Static Code Analyzerによって指摘された問題は、Audit Assistantによって機密情報を含まない属性に変換されます。これらの属性には、脆弱性のカテゴリ、重大度、コードおよびソフトウェアセキュリティ脆弱性の複雑さの指標 (入力の数、分岐の数、メソッドの出力型、プログラミング言語、ファイルの拡張子、問題を発見したアナライザーなど) が含まれます。トレーニングデータの場合、監査者の過去の判定も含められます。匿名問題メトリックスは、Micro Focus Fortifyのスキャン分析に送信され、機械学習分類機能のトレーニングと適用に使用されます。これにより、最高98%の精度で問題を特定できます。

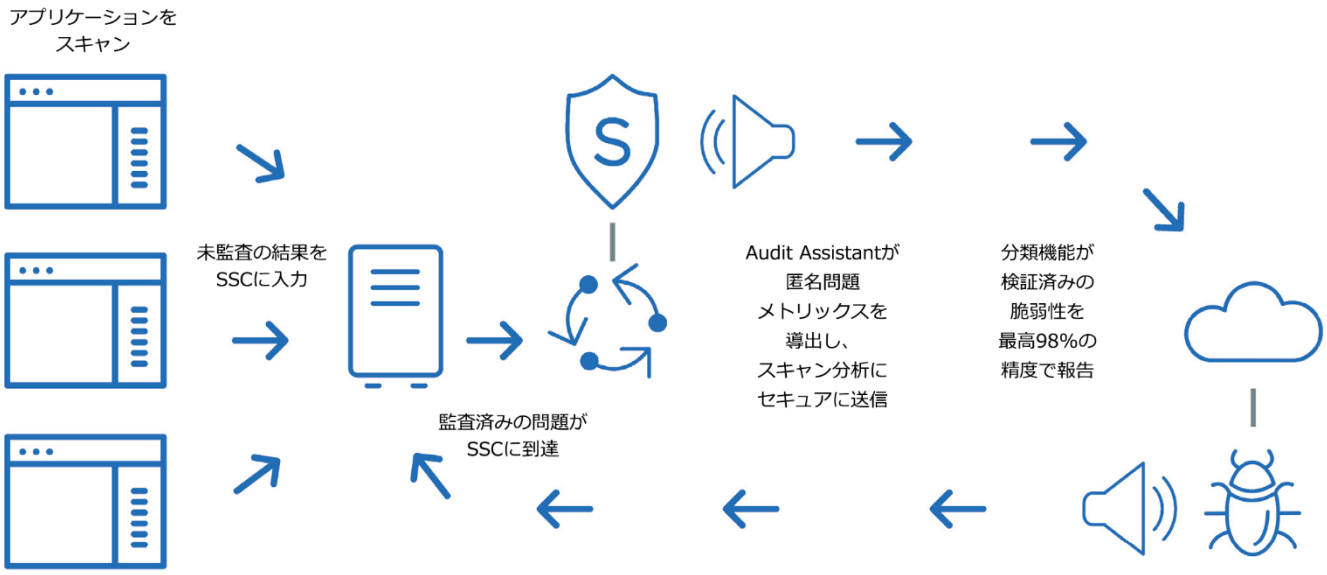

図2: Audit Assistantのワークフロー

新しい静的スキャン結果が処理された後で、Audit Assistantが予測と予測信頼度をスキャン結果に付加します。組織のリスク許容度と事前に設定された信頼度しきい値に基づいて、これらの問題は、**悪用可能**、**判定不能**、**非問題**のいずれかに分類されます。

- 予測値は、Audit Assistantが問題を悪用可能、非問題、あるいは判定不能 (予測信頼度がしきい値を下回った場合) のいずれと判断したかを示します。
- 予測信頼度は、Audit Assistantが予測の精度に関して持っている信頼の大きさを示します。

こうして、機密情報や識別情報を外に出すことなく、Audit Assistantの判定結果がスキャン結果に付加されて、組織のセキュリティ監査者によるレビューが可能になります。匿名のメタデータは、クラウド内で伝送される間、TLS暗号化通信チャネルによって保護されています。送信されるのは**匿名問題メトリックス**だけなので、企業は機密データを通常の保護の範囲外に出すことなく、ソフトウェアセキュリティ保証プログラムのスケールを拡大し、リスクを削減できます。

Audit Assistantを使用すれば、お客様のスキャン結果から問題メトリックスを導出することで、何千人ものセキュリティプロフェッショナルによる、総計で何十億行ものコードの評価から得られた知識を利用できます。人員を増やしたり追加予算を割り当てたりしなくても、機械学習を通じて企業のアプリケーションセキュリティプログラムの効率と有効性を改善できます。希少な人間の専門知識から無限に拡張可能な人工知能へというSASTのパラダイムシフトにより、非問題の検出を最大90%減らすことができます。

非問題とは

非問題とは、監査の結果修正が不要と判断された検出結果です。非問題は、以下のような原因から生じます。

- すでに実施された修正作業の結果、問題が悪用可能でない場合
- 設計上、コードが到達不能である場合
- 不適切なツール設定から生じるノイズ
- リスクを受け入れるという組織の判断
- 誤検出

非問題の削減率:	25%～90%
精度:	80%～98%
検出漏れ:	<1%

ROIの大幅な向上

新しいSAST実装による投資利益率 (ROI) の指標は、すでに何年かにわたって入手可能になっています[5]。ソフトウェアセキュリティのライフサイクルの早い段階で対策を行い、アプリケーションセキュリティの向上を通じて侵害を防ぐことで、企業は大幅な節約を実現しています。Audit Assistantは、スキャン完了後の監査と問題修正の時間を大幅に短縮することで、既存の投資からの収益を最大化し、組織の**シフトレフト**[6]を容易にする効果があります。Audit Assistantは、機械学習の技術を利用することで、希少なセキュリティ専門知識の到達範囲を拡大します。Micro Focus Fortifyコミュニティ全体の何千人ものセキュリティプロフェッショナルから学習した分類機能によって、専門家の時間を最適化できます。ソフトウェアセキュリティ保証プログラムの精度と一貫性を維持しながら、企業全体にその対象範囲を広げることができます。

[5] 『Continuous Delivery of Business Value with Fortify』https://software.microfocus.com/en-us/assets/enterprise-security-products/continuous-delivery-business-value-fortify

[6] 『Integrate application security into your DevOps program』http://files.asset.microfocus.com/4aa6-3394/en/4aa6-3394.pdf

ベンダーは、ノイズと検出漏れの間のトレードオフを図ってきました。これは、あらゆるセキュリティプロフェッショナルを悩ます問題です。Audit Assistantは、ノイズを最大90%削減しながら、同時に検出漏れの割合を1%未満に抑えています。Audit Assistantの分類機能は、最高98%の精度で、Fortify SCAの検出結果を非問題と監査します。スキャン分析の分類機能の精度は、以下の2つの方法で提供されたトレーニングデータを通じて改善されます。

- **Fortifyコミュニティインテリジェンス**
  分類機能は、Fortifyコミュニティインテリジェンスを利用してトレーニングされています。これは、Micro Focus Fortify on Demandの監査者、専任のソフトウェアセキュリティ調査担当者、およびコミュニティインテリジェンスに参加しているその他のFortifyのお客様の専門知識を利用しています。ユーザーは、**匿名問題メトリックスだけ**をFortifyコミュニティインテリジェンスデータセットに含めることを選択できます。これにより、すべてのユーザーにとって予測の品質が向上します。Fortifyコミュニティインテリジェンスとお客様のローカルデータによってトレーニングされた分類機能は、最も正確かつ堅牢であり、ルールとゼロデイに関する最新情報を含みます。これに加えて、Fortifyコミュニティインテリジェンスでトレーニングされた分類機能は**標準で**利用できるので、お客様がトレーニングデータを送信しなくても正確な予測が可能です。

- **プライベートインテリジェンス**
  分類機能は、お客様の過去の監査済みスキャン結果から得られた匿名問題メトリックスだけを使用してトレーニングされます。新しいスキャン結果に関する予測を行う前に、過去のスキャン結果が解析され、トレーニングのためにAudit Assistantに送信されます。組織の匿名問題メトリックスは、他のユーザーのトレーニングには利用されません。

? お客様データの保護の仕組み

問題メトリックスはローカルに計算されて匿名化されるので、それが存在するFortify SSCインスタンスの外部では識別不能です。セキュリティ管理としては、以下の方法が用いられます。

- 問題メトリックスをローカルに導出
- 問題メトリックスに機密情報は含まれない
- 予測要求IDによる難読化
- エンドツーエンドの暗号化

ユーザーがFortifyコミュニティインテリジェンスへの参加を選択した場合でも、自身のプライベートデータだけで分類機能をトレーニングすることを選択した場合でも、**問題メトリックスはローカルに導出され、匿名化されます**。Micro Focus Security Fortifyは、もっぱらセキュリティに注力しており、過去のセキュリティの問題を専門知識によって解決しながら、未来のセキュリティ機能を提供します。

セキュリティリスク

静的分析から得られる問題データは、企業がアプリケーションレイヤーを通じたリスクに関する情報を得るために利用できます。問題データが企業の外部で識別可能になると、侵害の手がかりとなるため、Audit Assistantは問題データを決して企業の外部に出しません。問題データは送信前にローカルに匿名化されるので、問題の発見やその場所の特定に利用されることはありません。

Audit Assistantからスキャン分析サービスへの予測のための接続は非同期に行われるため、監査や修正のプロセスの進行を止めることはありません。スキャン分析サービスが何らかの理由で利用できなくなった場合でも、ワークフローはAudit Assistantの予測を使用せずに継続します。サービスが利用可能になると、予測が再び得られるようになります。Audit Assistantをセキュアソフトウェア開発ライフサイクルの一部として採用することで、企業はリスクを軽減できます。分類機能

は何千人ものセキュリティ専門家のレビューを使用してトレーニングされているからです。企業のセキュリティ専門家は、企業にとって最も重要な検出結果や疑わしい検出結果を選別して、優先的に処理することができます。

精度

Audit Assistantの精度は、トレーニングに使用されたデータによって決まります。監査された問題が、分類機能のトレーニングに使用される問題メトリックスで50%の場合に正しいとすれば、その分類機能も50%の場合に正しい結果を出します。したがって、Fortifyコミュニティインテリジェンスによって分類機能をトレーニングすれば、精度と一貫性をさらに高めることができます。世界レベルのセキュリティプロフェッショナルによる何百万ものトレーニングレコードから得られた専門知識の総計が含まれているからです。Fortifyコミュニティインテリジェンスによってトレーニングされた分類機能は、98%の精度を持つという測定結果が得られています。匿名問題メトリックスをFortifyコミュニティインテリジェンスに含めることを選択すれば、Fortifyとそのコミュニティ内の定評あるセキュリティ専門家のセキュリティに関する知識と各領域の専門知識の総計を利用できるとともに、自社のセキュリティプロフェッショナルの能力を活かして、すべてのユーザーのために98%の精度をさらに高めることに貢献できます。

たとえば、組織内に特定のフレームワークでのSQLインジェクション脆弱性の検出と修正に関する世界最高の専門家がいたとしても、企業のコードには複数のフレームワークや言語が使用されている場合があります。Fortifyコミュニティインテリジェンスに参加することを選択すれば、サポートされるすべての言語とフレームワークに関する専門家の最高の専門知識を利用できます。分類機能の精度は、専門知識を供給して継続的トレーニングを行うことで向上します。企業は、現在公開されている分類機能の高レベルの精度を利用しながら、自社の専門知識を活かしてその改善に寄与することができます。

まとめ

静的分析のこのパラダイムシフトによって、監査結果を得るための時間とコストを大幅に削減でき、ROIの劇的な向上につながります。何千ものセキュリティプロフェッショナルが、自身のソフトウェア保証プログラムでAudit Assistantを使用して、合計何十億行ものコードを評価した結果から得られた知識を利用できます。Micro Focus Security Fortifyは、アナライザーのレポート対象を制限することでセキュリティ問題の幅を狭めるのではなく、非問題を実際の問題から自動的に識別するスキャン分析プラットフォームを開発しました。この革新的方法は、ビッグデータ分析を利用して、スキャンの詳細さや完全性を犠牲にせずに、セキュアソフトウェア保証を企業全体に広げることを可能にします。

組織がDevOps環境に移行するにつれて、アプリケーションセキュリティをプロセスに組み込むことが必要になっています。Micro Focus Security Fortify Audit Assistantは、監査プロセスの自動化を直接に支援することで、デリバリと展開のスケジュールの遵守を可能にします。Audit Assistantは、スキャン分析プラットフォームを通じて、時間のかかる問題レビューの反復作業を削減します。
ノイズの多いスキャン結果を我慢したり、スキャンの包括性と監査時間のトレードオフを考慮したり、スキャンのレビュー時間のために製品の納期に影響が及んだりすることはもうありません。匿名問題メトリックスで分類機能をトレーニングすることにより、識別可能なデータがクラウドに送信されるリスクなしに、ソフトウェアセキュリティ保証プログラムの費用を削減できます。Fortifyコミュニティインテリジェンス分類機能の使用を選択すれば、脆弱性の予測を通じて、セキュリティに関するワークロード全体をすぐに減らすことができます。

Micro Focus Security Fortifyは、2003年に設立され、業界をリードするFortify Static Code Analyzer (SCA) ツールを10年以上にわたって提供しています。これは、ソフトウェア開発のセキュリティを確保するための科学的裏付けのある手法であり、仕様と実装の一貫性に関する意味のある実用的なテストを可能にします。

詳細情報

https://software.microfocus.com/software/application-security