CyberRes

ホワイトペーパー

Fortify による静的スキャンの自動監査を使用した効率化

**機械学習を利用した自動監査により、
平均 97% の精度で組織の時間とコストを削減**

目次

エグゼクティブサマリー 1
はじめに 2
予測型機械学習の力を解き放つ 5
自動監査の価値 7
まとめ 8

エグゼクティブサマリー

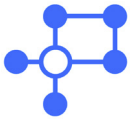
Fortify Audit Assistant は攻撃に利用される可能性のある診断結果を平均 97% の精度で予測します。

静的アプリケーションセキュリティテスト (SAST) ツールでソースコード、バイトコード、バイナリコードをスキャンすることにより、アプリケーションの潜在的な弱点を明らかにすることができます。2020 年 12 月現在、Fortify Secure Coding RulePack は、27 のプログラミング言語と 100 万以上の個別 API において業界トップクラスとなる 817 種類の脆弱性カテゴリを検出しています。アプリケーションが組織にもたらす真のリスクを評価するためには、このような徹底的なカバー率が不可欠です。しかし、診断結果には重要なコンテキスト情報が不足しているため、実用的ではありません。監査担当者は診断結果を確認し、アプリケーション固有の環境、緩和策、ビジネスロジックを考慮して、悪用の可能性を判断しなければなりません。SAST が利用可能となってから 20 年近くにわたり、診断結果の監査に費やす時間は、セキュリティチームと開発チームが付加価値のない作業に費やす時間の大部分を占めてきました。Micro Focus Fortify の自動監査技術により、監査プロセスに費やされる時間は大幅に削減されます。

Fortify Audit Assistant は攻撃に利用される可能性のある診断結果を平均 97% の精度で予測します。Audit Assistant を使用されている Fortify のお客様は、社内チームに限定的に導入した最初の年に、手動での監査時間を 58% 削減するなどのメリットを得ました。静的アプリケーションセキュリティに関する診断結果の監査を自動化することにより時間と労力を削減できることが実証され、その価値が証明されました。Audit Assistant は、主に次の 3 つの方法で、SAST の投資収益率を向上させます。

深堀りが必要な
手動検査数を削減

関連する問題を
特定して誤検出を
迅速に除去



既存のリソースでアプリケーションセキュリティを強化

セキュリティチームにとってのメリット

手動調査が必要な問題の数を減らすことで、監査担当者はより限定されたデータをより深く調査することに時間を集中させることができるため、スキルセットをより効果的に活用できます。組織は、興味深い調査と管理可能な脆弱性の数により、優秀なセキュリティ人材をより容易に確保することができます。セキュリティチームは、同じリソースでより多くのアプリケーションを監査することができ、関心対象ではないデータを機械学習により自動的に除外して信頼性の高いデータを検証することができます。

開発チームにとってのメリット

修正作業が円滑に進むと、組織は優秀な人材により多くのインセンティブを与えることができるようになります。開発チームは、最も関連性の高い問題の緩和のみに効率的に集中し、静的セキュリティスキャンが完了したら直ちに信頼性の高い問題の修正を開始できるため、人間がスキャン結果を監査することによる待ち時間を大幅に削減することができます。セキュリティが負担やゲートキーパーではなく、企業文化のシームレスな一部となっていれば、組織は優秀な開発人材の獲得がより容易になります。

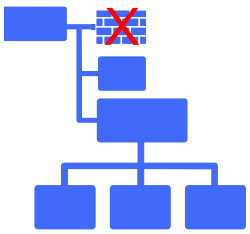
はじめに

ソフトウェアの脆弱性は、ソフトウェア開発プロセスにおいて最小限に抑えるための管理がされていないことが多い深刻な問題です。

ソフトウェアの脆弱性は、ソフトウェア開発プロセスにおいて、最小限に抑えるための管理がされていないことが多い深刻な問題です。SAST は、組織がアプリケーションのソースコードからビジネスリスクを特定、監視、軽減することを可能にします。SAST は、20 年近くにわたり、デジタル企業のセキュリティに必要なコンポーネントとして広く認識されています。SAST ツールは、テイント解析、構造分析、制御フロー分析などの分析手法により潜在的な脆弱性を調査結果として報告します。その後、専門家がアプリケーションやデプロイメント環境の状況などの組織に特有の情報を使用して結果を監査します。監査担当者が潜在的なソフトウェアセキュリティ脆弱性を「問題なし」と判断した場合、検証に費やされた時間は付加価値のない時間となります。このような監査は安全なアプリケーションを提供する上で基本的な課題ですが、通常、ツールやテクノロジーがすぐに実用的な結果を生み出すものではないため、時間と多大なコストを要します。

ソフトウェアセキュリティの調査結果を「問題あり」として監査する場合、攻撃者が脆弱性を悪用するが実際の害は及ぼさない概念実証攻撃が含まれることがよくあります。これらの脆弱性は、コードベースの変更によって修正するか、修正に代わる制御によって緩和する必要があるリスクです。監査で「問題なし」とされた調査結果は、これらの脆弱性が悪用される可能性が低い理由、またはその悪用が許容できるリスクであるという判断、さらには最悪の場合、同じ調査結果が以前にも「問題なし」とされているなどを問わず、人間の監査担当者が時間を費やすためコストとなります。調査結果が「問題なし」と判断される理由の簡単な例としては、アプリケーションのコンテキスト、組織のポリシー、審査担当者の専門知識などがあります。

カテゴリ	監査の決定	監査メモの例

アプリケーション
コンテキスト
	問題なし
	問題のコードにはどの
	ような手段でも到達できない。
	 
		問題なし：到達不可能なコードスニペット
		adminDebug = false;
		if(true == adminDebug)
		adminstratorExecute(cmds);
		到達可能な状態にコンパイルされた
		場合は高リスク、リスクプロファイル
		[employee-dev-risk-03] に準拠

次のページに続く

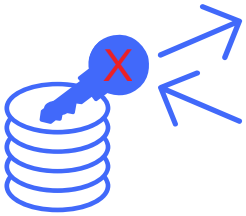
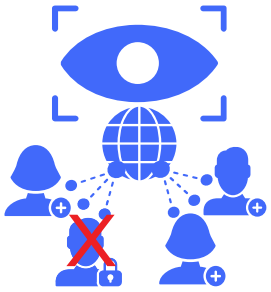
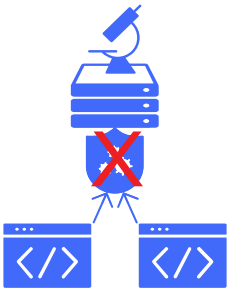
カテゴリ	監査の決定	監査メモの例
アプリケーションコンテキスト	問題なし アプリケーション外部に既存の緩和策がある。 	問題なし：データベースは保護されている Voltage Format-Preserving Encryption がこのデータベースを保護 データベースのバックエンドが平文でデータを扱う場合は高リスク、リスクプロファイル [consumer-commerce-risk-01] に準拠
組織のポリシー	問題なし スキャンがアプリケーション向けに最適化されていない。 	問題なし：スキャンの最適化 1.5 Java Developer Environment のスキャンは 1.8 のランタイムで解決。 ランタイム JDE が 1.8 でない場合高リスク、リスクプロファイル [employee-dev-risk-03] に準拠
組織のポリシー	問題なし 組織のポリシーにより、リスクを限定的に許容。 	問題なし：監視された安全なログイン Active Directory システムを Security Operations Center の ArcSight で監視、二要素認証と VPN 必須 信頼性が低い認証は高リスク、リスクプロファイル [employee-dev-risk-03] に準拠
セキュリティの専門知識	問題なし セキュリティ担当者が悪用の難易度が高すぎると判断した場合。 	問題なし：信頼できるシリアル化されたオブジェクト 信頼できるシリアル化されたオブジェクトのみ受け入れ、悪用でサーバー障害が発生 アップストリームサーバーが侵害を受けて悪用が安定した場合高リスク、リスクプロファイル [consumer-commerce-risk-01] に準拠

表 1. 診断結果の監査に費やす時間の例

発見事項は、手動監査プロセスを通じて、「問題なし」の理由を表す 1 つ以上の分析タグにマッピングされます。オンプレミスまたはサービスとして提供される Audit Assistant では、これらのラベルが特定の信頼性範囲内の調査結果に自動的にマッピングされるため、チームが実行しなければならない付加価値のない作業の時間をさらに削減することができます。スキャンプロセスの調整、表示テンプレートでの抑制、コンプライアンスやポリシーに準拠したレポートからの除外など、関心対象ではない調査結果に対する従来の対策は、関心対象ではない結果と検証済みの脆弱性の両方についての信頼性の高い予測を自動的に監査する機能により強化されます。

Audit Assistant により特定の信頼性範囲内の調査結果に自動的にラベルが割り当てられるため、チームが行わなければならない付加価値のない作業時間をさらに削減することができます。

問題の大きさは、簡略化したアプリケーションのスキャンの例で見るとよくわかります。

- 0.5 時間のスキャンで 1,000 件の調査結果を検出
- 40 時間の監査時間で 500 件の対応可能な問題を特定
- 1 件あたり 5 分として 40 時間の問題修正時間

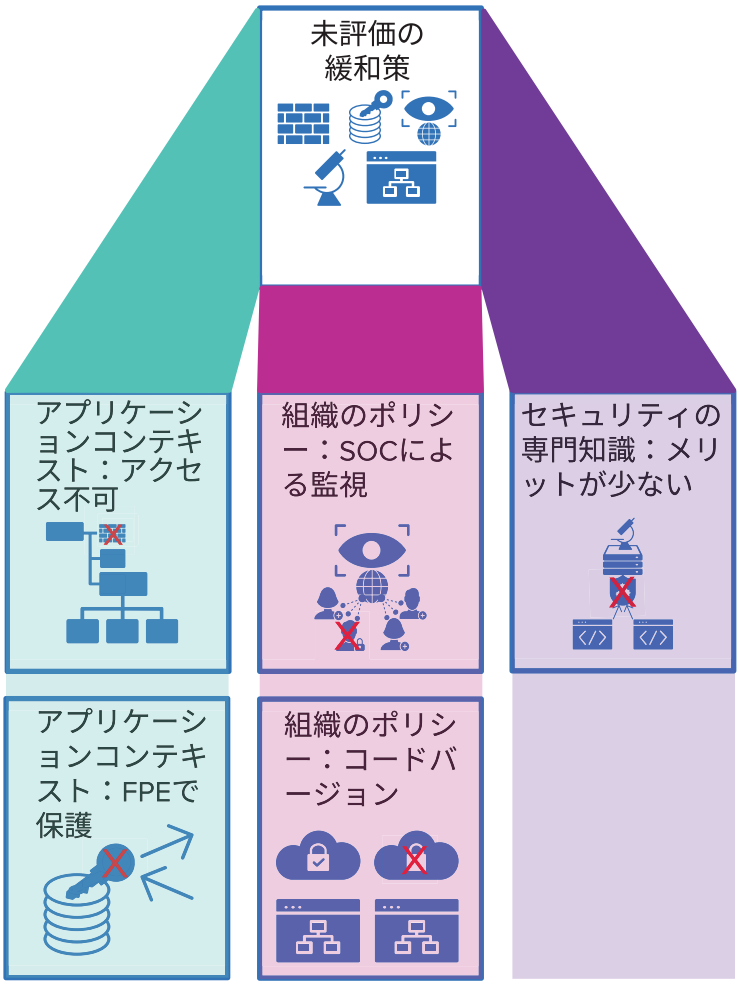


図 1. アプリケーションの例として見た問題

大規模な自動監査の重要性は、スキャン時間に関して非常に説得力があり、これは現代の SAST において無視できない要素です。お客様は、アプリケーションセキュリティテストに費やす時間の 50% を監査に費やしています。このデータは、調査結果の全体的件数の制限、監査が必要な件数の削減、最も重要な問題への修正作業の集中など、改善のための道筋をいくつか示唆しています。Audit Assistant は、監査を必要とする件数を削減して、最初に集中すべき問題について信頼性の高い判定を行います。人間による監査を待つということは、セキュリティの問題がセキュリティスキャンから数日または数週間後にしか確認できないことを意味し、開発者はその後に対処法を変え、自分が一度も触れたことがない可能性のあるコードの問題を緩和しなければならなかったため、摩擦が生じていました。Fortify が初めて機械学習による Audit Assistant を市場に投入するまで、監査は緩和努力における大きなボトルネックとなっていました。

お客様はアプリケーションセキュリティテストに費やす時間の 50% を監査に費やしています。

予測型機械学習の力を解き放つ

Audit Assistant は、Fortify on Demand (FoD) または組織のプライベートデータセットにある数十万件の監査履歴を使用してトリアージ作業の優先度設定に関する予測のインサイトを作成します。Audit Assistant は Fortify のすべてのお客様に無料でご利用いただけます。Fortify Software Security Center (SSC) と統合したオンプレミス型、または FoD を通じたサービスとして提供されます。使い始めのお客様により、メタデータの匿名問題のみを使用して監査結果の正確な予測に機械学習が有効であることが確認されています。

ソースコードはスキャン環境から出ることなく、以下の限られたメタデータ値に絞られます。

- 脆弱性カテゴリ
- 重大度
- 入力
- ブランチ
- 出力
- プログラミング言語
- ファイル拡張子
- 検出アナライザー

Audit Assistant は、ソースコードを 1 つも共有することなく、問題のフィンガープリントを作成してそれを使用することにより匿名化して安全に予測を行います。

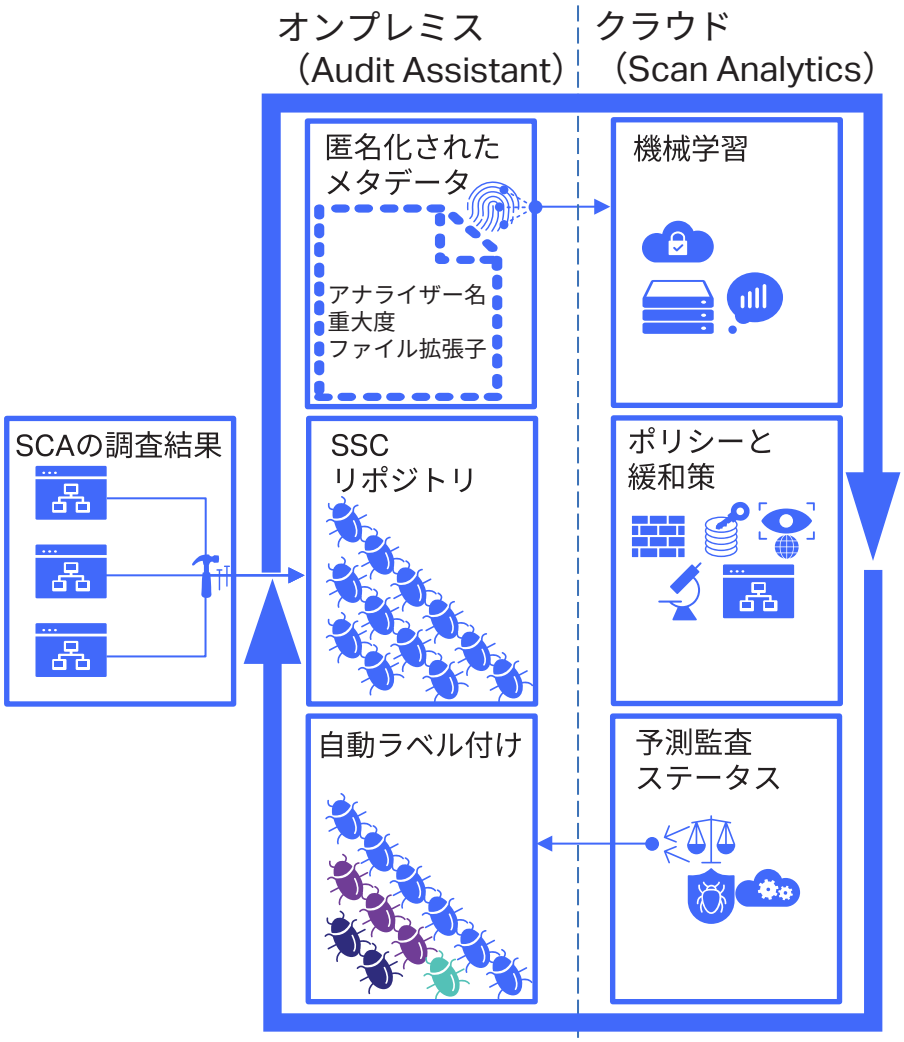


図 2. Audit Assistant の簡素化されたアプローチ

メタデータは、問題の発生元である組織、コード、およびそれが示す特定の脆弱性を完全に匿名化すると同時に、問題を高い信頼性で予測するのに十分なものとなっています。Audit Assistant のポリシーは、既知のコンテキストの違いによって異なる予測をもたらす監査データを使用して組織が個々のニーズとユースケースに応じてこれらの予測を活用できるようにします。

ポリシーは、カスタム監査データセットと信頼性しきい値を使用し、組織固有のニーズに合わせて予測を改善し、より正確なコンテキストを予測に適用させます。「外部」ポリシーでは、緩和のためのコンテキストを予測に反映させて、より高い信頼性しきい値の範囲内のインジェクションの結果を「問題なし」として自動的にラベル付けすることができます。一方、「内部」ポリシーは、緩和的なコンテキストを持たないアプリケーションを予測し、ラベルを適用する前に手動による確認を要求することができます。ベースラインスキャンと予測ポリシーを導入することにより、静的アプリケーションセキュリティの調査結果は機械学習による予測の恩恵を受けることができます。

調査結果はローカルで問題の数値へと匿名化され、このメタデータのみのパケットは送信中 TLS 暗号化チャネルで保護されます。匿名化された問題の数値のみを送信することにより、ソースコードや個人を特定できる情報を 1 行も社外に送信することなくソフトウェアセキュリティを拡張することができます。機械学習アルゴリズムは、メタデータと予測ポリシーを使用して、0 (信頼性なし) から 1 (信頼性あり) までの信頼性スコアに加え、結果について、問題なし、問題なしのしきい値未満、悪用可能、悪用可能のしきい値未満、予測なしのいずれかのステータスを返します。

あるお客様のサンプルでは、結果の約 20% が範囲から除外され、1 つのアプリケーションの結果の約 50% について調査のための効率的なシーケンスが提案されました。実用的な結果を IDE に取り込むか、SSC で表示するか、連携されたバグトラッキングシステムで自動更新するかを問わず、監査結果はチームがすでに選んで使用しているツールを使用した通常のワークフローのシームレスな一部となります。問題の監査ステータスを予測する機能には、信頼性しきい値内の調査結果に対して監査ラベルを自動的に適用する機能も含まれます。この機能により、非常に高い信頼性で悪用可能な問題が予測された場合にのみビルドを中断し、管理のオーバーヘッドを削減することができるため、Audit Assistant の価値がさらに高まります。

あるお客様のサンプルでは、結果の約 20% が範囲から除外され、1 つのアプリケーションの結果の約 50% について調査のための効率的なシーケンスが提案されました。

自動監査の価値

Audit Assistant は、マッピングされた分析ラベルに対して予測、自動的に監査することによりセキュリティチームの能力を拡張し、開発チームの効率を向上させます。人間が脆弱性を調査することを排除することで、容易に監査時間を半分に削減できます。複雑さが中程度の単一アプリケーションについて 1,000 件の結果を監査して、500 件の対応すべき脆弱性を特定するにはすぐに 40 時間費やしてしまうこともあります。監査時間の削減のみを簡略化すると、X * H * C = S として定量化できます。200 のアプリケーション (X) を持つ企業では、1 時間あたりの監査コストが 150 米ドル (C) のときにアプリケーションあたり年間 20 時間 (H) を削減した場合、年間 60 万米ドルの削減 (S) となります。この削減の効果は、以下の 3 つのユースケースで明確に実証されており、それぞれの監査にかかる時間 (H) に影響します。

図 3. Fortify Audit Assistant による監査時間の削減の例

ユースケース 1
既知のコンテキストの中で高い信頼性で予測された場合に自動的に監査ラベルを適用することにより、デプロイメントサイクルを加速させることができます。ある大手ソフトウェア会社では、Audit Assistant による予測を連携することにより、問題が非常に高い信頼性で「悪用可能」と予測された場合にビルドを中断し、より少ない、より重大度の低いリスクでデプロイメントを自動化しています。このアプローチでは、信頼できるリスクプロファイルと階層型のセキュリティにより信頼性の低い調査結果を緩和することで、企業にとって真に摩擦のないアプリケーションセキュリティを DevOps の速度で実現することができます。最終的に、このユースケースでは、迅速なデプロイメントごとに定義されたリスクを許容するための、細かく調整された監査ポリシーが必要になります。興味を持たれた場合はオンプレミスの API コールについて Fortify GitHub のサンプルプロジェクトにある「Batch Train」および「Batch Predict」機能をご参照ください。

ユースケース 2
監査担当者が初期診断結果のサブセットに集中できるようにすることで監査担当者の時間にかかわるコストを削減することができます。世界有数のある石油・ガス会社は、「Scan Analytics のおかげで、誤検出の分析に費やす時間が大幅に削減されました」と絶賛しています。アジアのある大手金融サービスグループでは、手動監査を必要とする問題が 37% 減少し、8,000 件の調査結果のうち 3,000 件の問題を予測して、37,500 米ドルを直接削減できたと報告しています。Fortify 独自の自動監査機能をベータテストしたある大手ソフトウェア会社では、診断結果の 20% が人間による監査から完全に除外されました。人間による確認から問題を除外することで、予算編成の改善、市場投入までの時間の短縮、集中的な緩和作業が可能になります。

ユースケース 3
専門家である監査担当者の知識が将来の調査に活用できる強力なツールを手に入れることができます。「スター」である監査担当者がキャリアアップした後も、その専門知識により予測的価値が提供されます。このケースでは、Audit Assistant をトレーニングして将来の予測をより正確に調整して、一般的なポリシーや特定のポリシーですぐに期待できる平均精度を 97% に向上させます。デフォルトの分類子にトレーニングが提供されると、その分類子を作成した企業にのみアクセスが制限されるプライベート分類子に提供されるトレーニングとは異なり、すべての Fortify ユーザーがそのメリットを享受することができます。

アジアのある大手金融サービスグループでは、手動監査を必要とする問題が 37% 減少し、8,000 件の調査結果のうち 3,000 件の問題を予測して、37,500 米ドルを直接節約しています。

まとめ

組織は、SAST の一部としてノイズの多いスキャン結果を受け入れたり、スキャンの包括性と監査時間の間でコストのトレードオフをしたり、関心対象ではない調査結果に開発者の反発を受けたりする必要はもうなくなります。Fortify Audit Assistant は、機械学習アルゴリズムと、数十億行のコードにわたる数百万件の匿名化された監査判定を使用して自動的に監査予測を行います。このテクノロジーは、未監査の診断結果に対して数千人のアプリケーションセキュリティ専門家の知識でトレーニングされた機械学習を活用し、驚くほど正確な予測によって診断結果の監査コストを大幅に削減し、投資収益率を高めます。Audit Assistant は、SAST が報告する内容を制限することで発見される問題の幅を狭めるのではなく、問題でないものを脆弱性と区別して、自動的にラベル付けを行います。ビッグデータ分析に対するこの革新的な機械学習アプローチは、スキャンの深さやセキュリティの完全性を犠牲にすることなく、あらゆる規模の組織にソフトウェア保証を拡大するだけでなく、スキャン環境の外には識別属性やソースコードの行を一切送信しません。

アプリケーションセキュリティは、組織がデプロイメントを加速させる中で、ソフトウェア開発ライフサイクルにシームレスに適合する必要があります。FoD の静的評価の 74% が 1 時間以内に完了しており、お客様は完全に自動化された監査を選択することで DevOps のスピードでセキュリティを促進しています。Fortify オンプレミスのお客様は、認証トークンを取得して、設定オプションを有効化するだけで予測の要求を開始することができます。この簡単な導入によりシンプルで迅速に採用できます。問題が 99% の信頼性で悪用可能であると予測された場合にビルドを中断するなどの追加要件は、SWAGGER API を使用して洗練されたソフトウェア保証プログラムで使用できます。

オンプレミス、オンデマンド、およびハイブリッドのすべてのお客様が Audit Assistant を使用して投資収益率の向上を開始できます。Fortify にお問い合わせください。
まとめ：

- 監査に費やす時間を削減することにより成果物とデプロイメントのスケジュールを順守
- 深堀りが必要な手動検査数を削減を削減することにより人間の監査の労力を集中
- 既存のリソースでアプリケーションセキュリティを強化することにより健全なビジネス上の意思決定に必要な忠実度の高い監査に不可欠な組織の知識を維持
- 関連する問題を早期に特定することにより問題の監査に要する反復的な時間のかかる作業を削減
- 監査の自動化によりビジネス目標とセキュリティ目標の摩擦を削減

Audit Assistant のインスタンスはこちらから今すぐリクエストできます。

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

Audit Assistant のインスタンスを こちらから今すぐリクエストしてください。

お問い合わせ先：CyberRes.com
この記事はいかがでしたか？シェアはこちら

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

CyberRes
A Micro Focus Line of Business