Software Risk Manager

エンタープライズ規模のAppSecプログラム管理を簡略化

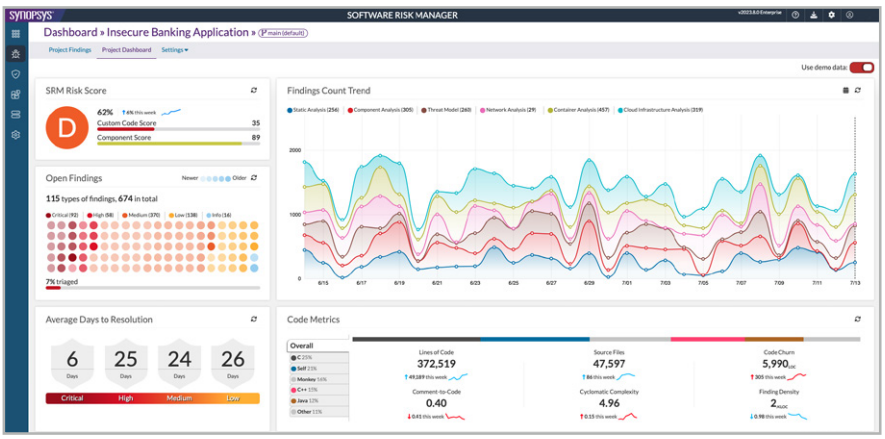
概要

ブラック・ダック Software Risk Manager はオンプレミス型のアプリケーション・セキュリティ態勢管理（ASPM ＝ Application Security Posture Management）ソリューションで、セキュリティ・チームと開発チームはアプリケーション・セキュリティ・プログラムを簡略化しながらリスク・ポスチャを高めることができます。内蔵の静的アプリケーション・セキュリティ・テスト（SAST）およびソフトウェア・コンポジション解析（SCA）エンジンに加え、ポリシー、テスト・オーケストレーション、問題の相関付け（コリレーション）を集約することにより、ソフトウェア開発ライフサイクル（SDLC）全体のセキュリティ・アクティビティを一貫性のある形でインテリジェントに統合します。Software Risk Manager を使用すると、セキュリティ・チームと開発チームは、信頼できる唯一の情報源（SSOT）に基づいて意思決定を行い、回復力のあるアプリケーションを大規模な環境でデリバリーできるようになります。

サイロ化を解消し、実用的な知見を提供

Software Risk Manager はアプリケーション・セキュリティ（AppSec）ワークフローに透明性、効率、説明責任の要素を導入することにより、SDLC のあらゆるステージでのチェックを統合する基盤としての役割を果たします。また、以下の主要な機能により、大規模な環境でのテスト、修正、およびリスク管理を支援します。

- 135 種類以上のセキュリティ・ツールとの統合をサポート（現在市販されている ASPM ツールとして最多）
- スキャン前とスキャン後のポリシー管理を中央から一元的に実行可能
- 業界をリードするブラック・ダックの SAST および SCA テスト・エンジンを標準で内蔵
- 20 種類以上のコンプライアンス標準に対応
- カスタマイズと拡張が可能な相関ツール
- Jira、ServiceNow、Azure DevOps、GitLab、GitHub、Jenkins、TeamCity、Bamboo などの代表的なバグ追跡ツールや開発者ツール、および Visual Studio、Eclipse、Visual Studio Code、IntelliJ 用の IDE プラグインとの双方向の統合
- 16 種類のオープンソース・テスト・ツールを標準で内蔵し、検出された言語に基づいて適切なツールを自動で推奨



Software Risk Manager のダッシュボードにアプリケーション・セキュリティ・テスト結果と重要評価指標を表示

主な利点

集中型の AppSec 記録システム（SoR）の可視化

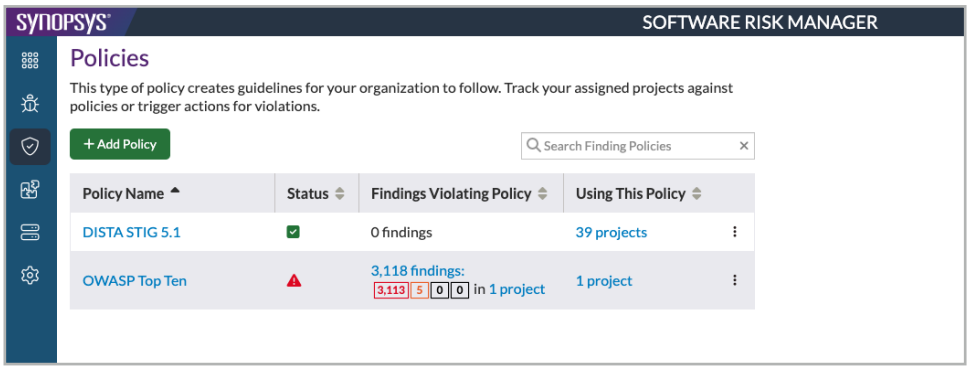
- 手動および自動テストで見つかったすべての結果を記録システム（SoR）に流し込むことで、AppSec テスト・アクティビティ、セキュリティ・データ、およびポリシーを完全に追跡。SDLC のあらゆるステージにおけるアプリケーション・セキュリティ・ポスチャをきめ細かく可視化
- さまざまな種類のテスト・ツールの結果を自動で相関付けて重複を排除し、一元的なユーザー・エクスペリエンスを提供することで、問題の可視化と優先順位付けが容易に
- SAST、SCA、動的アプリケーション・セキュリティ・テスト（DAST）、インタラクティブ・アプリケーション・セキュリティ・テスト（IAST）、InfraSec、脅威モデリング、およびモバイル、コンテナ、クラウド・インフラストラクチャ向けテストなど、代表的なセキュリティ・テスト・ツールを 135 種類以上サポート
- 個々のコードベースに最適な AppSec ツールを自動で選択
- 内蔵の SAST および SCA に対する自動オンボーディングにより、SCM リポジトリ、アプリケーション、および関連する開発者とセキュリティ・ユーザーを動的に検出

トリアージ、テスト、修正のワークフローを迅速化

- 一貫性のあるリスク評価に基づいて重大な問題を自動で特定して優先順位付け
- バグ追跡システムとの双方向同期により、高優先度の脆弱性と正確なコード行へのリンクを開発者に直接提示
- 内蔵の SAST および SCA エンジンでソースコードおよびオープンソースに含まれる脆弱性を迅速かつ正確に検出。プリセット・ルールを使用することで、必要なテスト・ワークフローを最小限のセットアップで構築
- 言語、脆弱性タイプ、およびソースに基づいてコンテキストに応じた修正ガイダンスを開発者に提供。過去のトレンドに基づいて推奨される修正アクションを提示
- セキュリティ・アクティビティがブランチ・レベルで表示されるため、開発者は修正を効率よくテストでき、ビルド中断の頻度が減少
- ブラック・ダックのツール（内蔵エンジンまたは単体製品）やサードパーティ・ツールによるスキャンを中央からオーケストレーション

リスクの可視化とガバナンスを一元化

- すべてのプロジェクトおよびソースコード（カスタム開発、サードパーティ、オープンソースを含む）について、リスク・スコア、テスト結果、重要評価指標のトレンドを全方位で可視化
- テスト結果を規制コンプライアンス標準（NIST、PCI、HIPAA、DISA、OWASP Top 10 を含む）に対応付け、重大な違反については監査レポートを作成
- ソフトウェア資産全体にわたるセキュリティ・ポリシーの作成から適用、監視までのワークフローを UI ベースと API ベースの両方で提供
- 問題のタイプごとのリスクしきい値、望ましいアプリケーション・セキュリティ・テスト・ツール、不具合修正時間に関する SLA、開発ステークホルダーへの必要な通知などをセキュリティ・チームが指定可能



ポリシーに違反しているテスト結果をプロジェクト、ソースコード、重大度ごとに追跡可能

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp