

開発者にとっての利点

直感的なワークフロー

- ・ セキュリティの専門家でなくてもコードの弱点や脆弱なオープンソース依存ファイルを修正できる
- ・ 問題のあるファイルはオープン、保存、編集時に自動アラートで通知。オンデマンドで手動による高速スキャンも可能
- ・ 自分のタスクのみに集中することも、ローカル・スキャンとチーム・ビューでプロジェクトのコードベース全体をサポートすることも可能

コード品質の改善

- ・ ソースコード、オープンソース依存ファイル、R 呼び出し、暗号化、**6** (E) などに含まれる問題を指摘
- ・ 明確なガイダンスにより問題の修正方法がすぐに分かると同時に、開発者のリスクへの意識とセキュリティ能力が向上
- ・ パイプライン・スキャンから優先課題に即座にアクセスすることで、エンドツーエンドのセキュリティ標準を維持

生産性の向上

- ・ コードのチェックイン前に問題を解決できるため手戻りが減少
- ・ D に最適化した高速スキャン機能により俊敏性を維持
- ・ 下流テストの前に脆弱性の問題を取

7 は D プラグインのため、開発者は複数のツールを行き来する必要がなく、日々の開発業務をこなしながらアプリケーション・セキュリティの水準を高めることができます。静的アプリケーション・セキュリティ・テスト(**8**)とソフトウェア・コンポジション解析(**9**)を組み合わせた **6** は、以下の項目に対してリアルタイムにアラートを通知し、高い可視性をもたらします。

- ・ コードに含まれるセキュリティ上の弱点(**10**)
- ・ オープンソース依存ファイルに含まれる既知の脆弱性(**11**)
- ・ **6** (E) の安全でない構成
- ・ 秘密情報 / 機微なデータの潜在的な漏洩リスク
- ・ 脆弱な R の使用

迅速な **12** ワークフローおよび C パイプライン向けに設計された **6** は、コードベース全体または変更されたプロジェクト x 頼 夫坏嵯帙薈銚は他のシノプシス

アプリケーション・セキュリティ・テスト(**8**)ツールで検出された問題や関連するセキュリティ・ポリシー違反のアラートを開発チームに送ることにより、他の **8** を補完し、その効果を高める役割を果たします。開発者が問題を迅速に修正できるように、**6** は詳細な修正ガイダンスを D 内に直接表示します。これには、推奨されるオープンソース・パッチ、コーディングのベストプラクティス、および **13** によるインタラク

Code Sight IDE プラグイン | 開発者ファーストまたはエンドツーエンドのセキュリティ

CS はスタンドアロンのプラグインで、開発チームが開発の初期からセキュアなソフトウェアを作成するのを支援します。また、シノプシスの **CS** ツール・スイートの **CS** 拡張機能として利用することで、後段のパイプラインで実行されるセキュリティ・テストから優先すべき問題と修正ガイダンスが開発者に直接提示されます。

シノプシス AST ツール向け Code Sight プラグイン

エンタープライズ環境でのライフサイクル全体にわたるアプリケーション・セキュリティに最適。

CS、**CS**、**CS**、および **CS** の完全なアプリケーション・セキュリティ機能を、既存のワークフローを妨げることなく拡張します。パイプライン・ベースのテストはこれまで通りセキュリティ・チームが管理しながら、開発者は **CS** 内で直接リスクへの意識を高めることができます。

CS、**CS**、**CS**、および **CS** に付属します。利用条件はソリューションにより異なります。

コード解析

CS
フル・スキャン(**CS**)

オープンソース解析

CS

リスク・インサイト

脆弱性の深刻度、優先度、到達性の指標(**CS** など)
安全でないコーディング作法(**CS** など)
CS!

シノプシスがご提供する統合型ソリューションは、ソフトウェア開発とデリバリのあり方を根底から変革し、
