SYNOPSYS®

Intelligent Orchestration

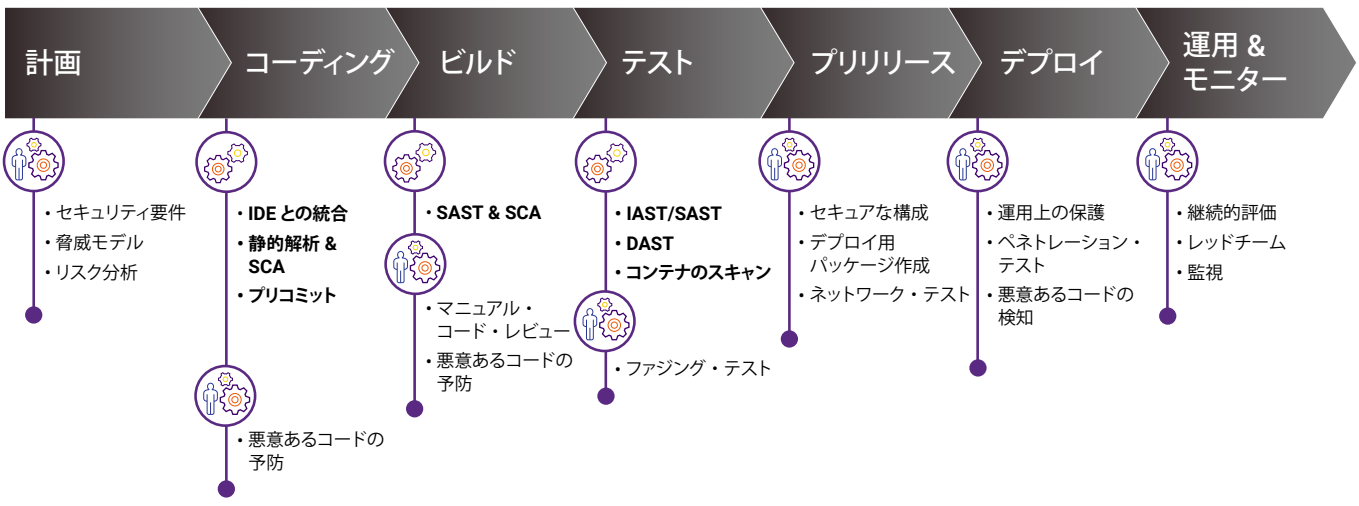
組織におけるリスク管理の方法をルールとして定義するだけ。あとは Intelligent Orchestration がテスト実行、ポリシー適用、課題の優先付けとフィルター処理をすべて管理します。

概要

シノプシスの Intelligent Orchestration は、ソフトウェア開発ライフサイクル（SDLC）の一部のステージだけでなく、全体を通じてセキュリティ・テストを自動化する AppSec パイプラインをカスタマイズした形でご提供します。コード変更の重要度、トータル・リスク・スコア、企業独自のセキュリティ・ポリシーに基づいて、Intelligent Orchestration が自動で適切なセキュリティ・ツールを実行し、マニュアル・テスト・アクティビティを開始します。これにより、大規模なエンタープライズ環境であっても、セキュリティ・チームは組織全体にわたってすべてのアプリケーションに対してセキュリティ・プロセスおよびポリシーを容易に適用できるようになります。

Intelligent Orchestration はシノプシスの AppSec ツール（Coverity®、Polaris Software Integrity Platform®、Black Duck®、Seeker®、Tinfoil™）およびサービスのほか、サードパーティの商用およびオープンソース・ツールとの連携も可能で、GitHub Actions、業界標準のソースコード管理システム（SCM）、継続的インテグレーション（CI）ビルド・サーバー、バグ追跡システム、ダッシュボード・システムとの統合もサポートしています。また、オンプレミスでの運用のほか、Amazon AWS および Microsoft Azure クラウド・パイプライン上でのホスティングも可能です。

専用のアプリケーション・セキュリティ・パイプライン
Intelligent Orchestration



主な特長

開発チームにとっての特長

- Intelligent Orchestration は専用のパイプラインを使用するため、メインの開発パイプラインを邪魔しません。セキュリティ解析結果をメインの開発パイプラインにマージするだけで、既存の課題管理システムや通知チャネルを通じて、適切な情報が適切なチームに配信されます。

導入のメリット

- **短時間での導入とオンボーディングが可能：**Intelligent Orchestration には、シノプシスの静的アプリケーション・セキュリティ・テスト（SAST）、ソフトウェア・コンポジション解析（SCA）、動的アプリケーション・セキュリティ・テスト（DAST）およびインタラクティブ・アプリケーション・セキュリティ・テスト（IAST）ツールが含まれるほか、その他の商用およびオープンソース・ツールも追加できます。新規および既存アプリケーションのオンボーディングは数時間、あるいは数分で完了します。
- **セキュリティ・リスクの可視性を向上：**Intelligent Orchestration は、各種セキュリティ・ツールから出力されたレポートを単一の共通スキーマに変換します。ダッシュボード・ツールには、リスク計算結果、アプリケーションの各種リスク要因に対するスコア、直近のパイプライン実行で選択されたセキュリティ・アクティビティが表示されます。
- **柔軟な構成オプション：**セキュリティおよび開発チームは以下のものを構成できます。
  - リスク・スコアに基づくスキャンの実行頻度とアウトオブバンド・アクティビティ
  - ツールの実行方法（非同期か同期か）
  - 通知方法（Slack、電子メール）
  - ビルドおよびバグ追跡の一時停止 / 中断 / 継続に関する基準
- **開発スピードの向上：**ビルドごとにすべての AppSec スキャン（SAST、SCA、IAST、DAST）を実行するのではなく、適切なタイミングで適切なツールのみを実行する（場合によってはツールをまったく実行しない）ため、貴重な時間を無駄にしません。
- **セキュリティ・テストを早期に効率良く実行：**コーディングの時点で即座に解析結果と具体的な修正アドバイスが得られるため、ソフトウェアの不具合を早い段階で簡単かつ正確に修正できます。チケットは Jira で自動的に作成され、課題の管理とトリアージが可能です。
- **開発者トレーニングのための指標と知見：**個々の開発者のコードに見つかった脆弱性のタイプと頻度はデータとして収集され、開発者への効果的なフィードバックとトレーニングに活用されます。

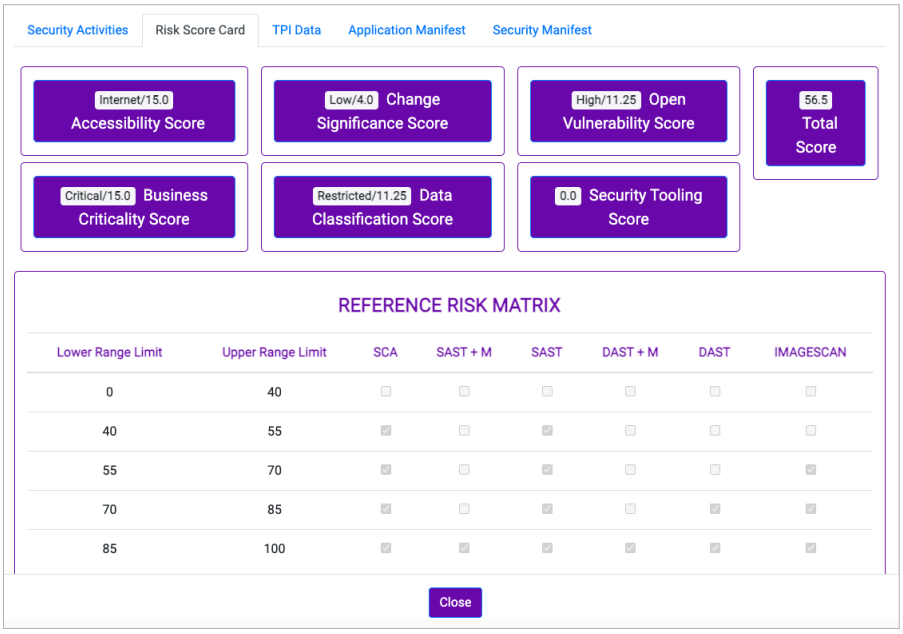
- Intelligent Orchestration では、組織のセキュリティ・ポリシーに基づいて優先度の高い脆弱性（重大な脆弱性や、重大な SQLi 脆弱性など）に関する情報のみが開発者に提示されるため、大量の解析結果に圧倒されることがありません。特定のスキャンを実行するかどうかは、実際のコード変更の内容や動的に算出されるトータル・リスク・スコア、および事前に定義したセキュリティ・ポリシーに基づいて Intelligent Orchestration がスマートに判断します。
- 開発チームは、開発者がコードの変更をプッシュするたびに GitHub Actions を実行するように指定できます。不具合が特定された場合は、コードを修正してメイン・ブランチにマージするのに必要なすべての情報（詳細な説明、具体的な修正アドバイス、変更されたファイルの名前、行番号、およびコミット ID など）が開発者に提示されます。

セキュリティ・チームを支援

- Intelligent Orchestration では、スキャン後のフィードバックをユーザーが設定できます。例えばビルドの一時停止や失敗、または重大なセキュリティ脆弱性や不具合があった場合は、開発、セキュリティ、および DevOps チームの指定した責任者にただちに通知を送るように設定することで、迅速な修正が可能となります。
- 設定可能な合否基準に基づき、セキュリティ・ゲートや品質ゲートを容易に実装できます。これらのゲートで特定された重大な不具合は、Jira などの課題管理システムへ自動的にプッシュされます。これにより、開発チームは継続的なフィードバックを受け取り、セキュリティ・テスト結果への見通しも良くなります。
- ガバナンスおよびコンプライアンスの要件は、セキュリティ・チームが簡単に設定できます。セキュリティ・アクティビティの深さと幅、開発ワークフローの定義、およびスキャンのコンプライアンス要件は、事業部門単位、製品チーム単位、アプリケーション単位、または組織全体でポリシーとして設定できます。

ポリシー管理のカスタマイズ

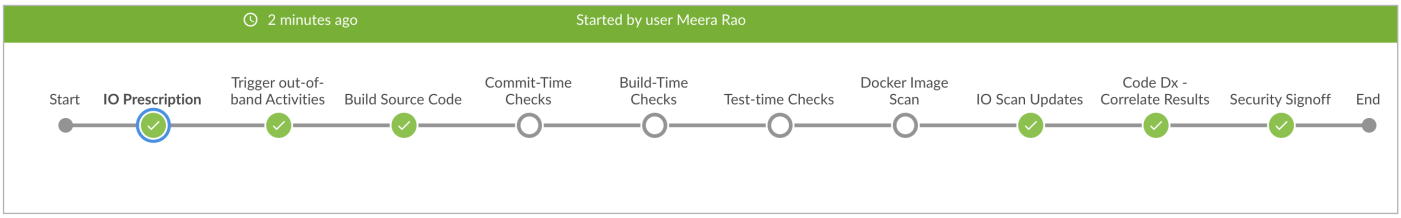
- Intelligent Orchestration では、トータル・リスク・スコアの算出基準にどのような重みを割り当てるかを定義およびカスタマイズできます。例えば、そのアプリケーションがインターネット上に公開されているか、ビジネスの基幹系アプリケーションであるか、アクセス制限されたデータを含んでいるか、未解決の重大な脆弱性を含んでいるか、大規模なコード変更があったか、などの基準に対してリスク・スコアを設定できます。スコアの範囲、および実行するセキュリティ・ツールの種類は、各企業のセキュリティ・ポリシー、コンプライアンス、およびガバナンスの要件に基づいてカスタマイズできます。



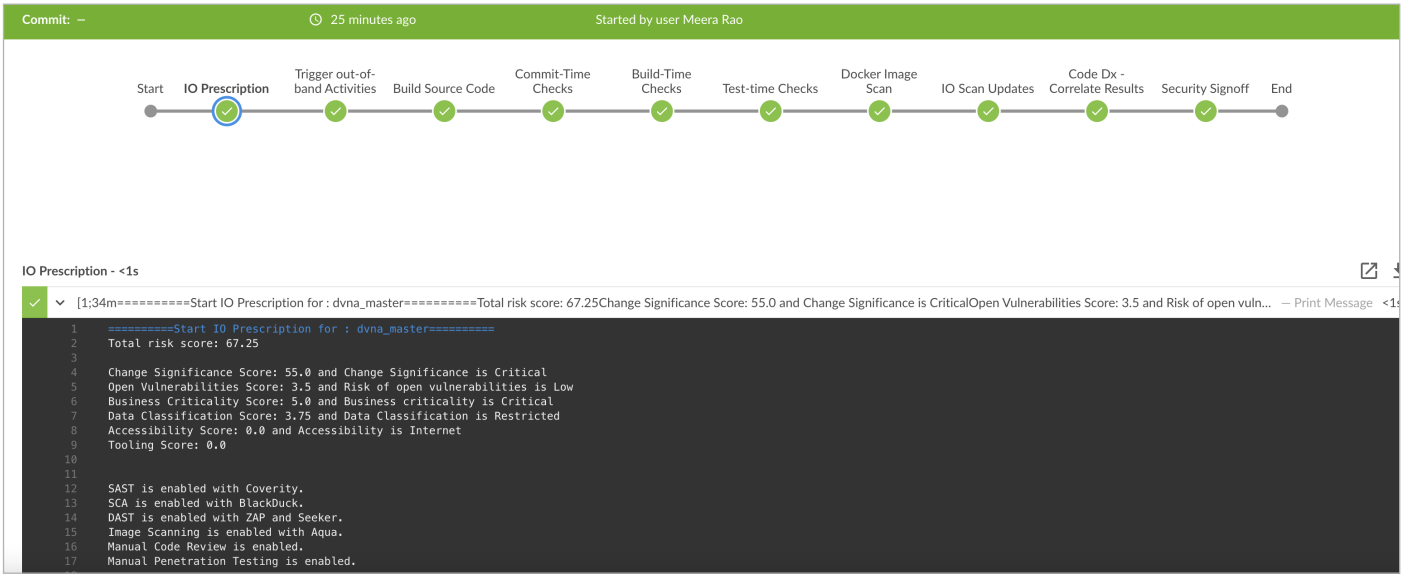
注・上記はサンプルイメージです

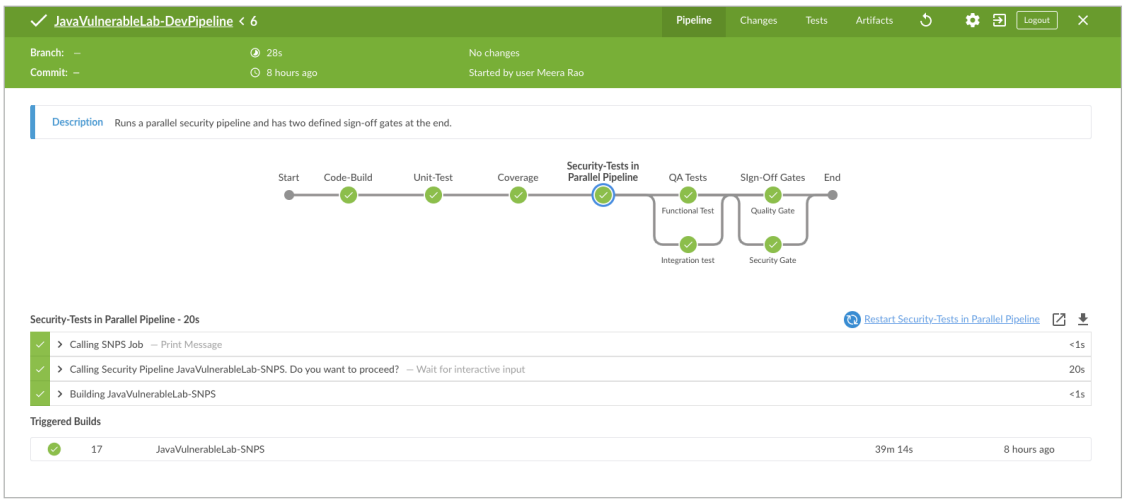
Intelligent Orchestration の仕組み

Intelligent Orchestration は、実際のコード変更の内容、リスク・スコア、企業独自のポリシーに基づいてどのスキャンやマニュアル・テストが必要なのかをスマートに判断します。例えば、ある HTML ファイルで CSS を使用してフォントを変更するといった軽微なコード変更はリスク・スコアが低く、セキュリティ・スキャンは不要と判断されます。このため、貴重な時間とリソースが節約されます。



一方、認証 API の変更といった大がかりで重要なコード変更には高いリスク・スコアが割り当てられ、SAST、SCA、DAST など複数のセキュリティ・テスト・スキャンが実行されます。また、マニュアル・コード・レビューとマニュアル・ペネトレーション・テストも必要なアクションとして開始されます。





Intelligent Orchestration では、セキュリティ・ツールとその他のテストを並列に実行することもできます。

Intelligent Orchestration | 技術仕様

SDLC とのネイティブ統合

ソースコード管理（SCM）

- GitHub
- GitLab
- Bitbucket
- その他の Git ベース SCM

CI ビルド・サーバー / 開発者ツールチェーン

- Jenkins
- GitLab CI
- Bitbucket Pipes
- GitHub Actions

バグ追跡 / 課題管理

- Jira
- GitHub Code Scanning Alerts
- Bitbucket Code Insights

セキュリティ・ツール

- Synopsys Coverity/Polaris
- Synopsys Black Duck
- Synopsys Seeker
- Synopsys Tinfoil
- その他の商用 AppSec ツール *
- オープンソースの SAST、SCA、および イメージ・スキャン・ツール *

ダッシュボード・ツール

- Polaris のレポート機能および Intelligent Orchestration
- Code Dx*
- サードパーティのレポート / ダッシュボード・ツール *

クラウドおよびクラウド・パイプライン

- Amazon Web Services / AWS Data Pipeline*
- Azure / Azure Pipelines*

その他の開発環境

- Docker（イメージ・スキャン）*
- Kubernetes*

通知手段

- Slack
- Teams
- Email

* カスタム統合も可能

シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質なソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や不具合を迅速に見つけて修正します。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス

TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software