SYNOPSYS®

シノプシスの Intelligent Orchestration：金融サービス企業への導入事例

適切なセキュリティ・テストを適切なタイミングで実行

顧客企業紹介

今回紹介する金融サービス企業（匿名希望）は Fortune 500 にもランキングされる業界大手で、総額 2 兆米国ドルの資産を運用しています。同社のデータベースには、数百万人にのぼる米国市民の重要な個人情報が保存されています。金融サービス業界全般の例にもれず、この企業でもアプリケーション・セキュリティ・テストの重要性が高まっていますが、それと同時にテスト・プロセスが開発スピードを低下させないようにすることも重要な課題となっています。

同社の継続的インテグレーション / 継続的デプロイ（CI/CD）環境の構成は以下のとおりです。

- シノプシス Black Duck® SCA（オープンソース依存ファイルに存在する脆弱性を検知）
- Amazon Web Services クラウド・プラットフォーム
- Jenkins オートメーション・サーバー（CI/CD ビルド、テスト、デプロイ用オートメーション・サーバー）
- Micro Focus Fortify Static Code Analyzer（プロプライエタリ・コードに存在するセキュリティの不具合を検知）
- Contrast Assess（実行時のセキュリティ解析を担当するインタラクティブ・アプリケーション・セキュリティ・テスト・ソリューション）
- Palo Alto Networks Prisma Cloud（Palo Alto Networks のプリプロダクション・コンテナ・セキュリティ・イメージ評価ソリューション）
- OWASP Zed Attack Proxy (ZAP)（動的セキュリティ・テスト・ソリューション）
- コーディング言語：Java、JavaScript、Python

課題

開発スピードを低下させることなく、複数のツールからのアプリケーション・セキュリティ解析結果を DevOps パイプラインに統合すること。ソフトウェア開発ライフサイクル（SDLC）イベントおよび定義されたポリシーに基づいて適切なセキュリティ・テストを適切なタイミングで自動的に実行する、クラウド・ベースの専用 CI/CD パイプラインを開発すること。

ソリューション

シノプシスの Intelligent Orchestration は、開発チームのスピードを妨げることなくガバナンス、コンプライアンス、法規制、その他のポリシーを必要に応じて確実に適用できるように最適化された、リスク・ベースの適応型アプリケーション・セキュリティ・テスト・オーケストレーション・ソリューションです。

理想的なアプリケーション・セキュリティ・テスト・オーケストレーション・ソリューションにはどのような条件が求められるでしょうか。使用しているセキュリティ・テスト・アプリケーション用のルールを自分で設定しておけば、適切な解析が適切なタイミングで自動的に実行されること。コード変更の重大度、アプリケーションのリスク・プロファイル、およびそのアプリケーションにどのセキュリティ・テスト・ポリシーを適用するかをインテリジェントに理解してくれること。特定のセキュリティ・テストを適用するかスキップするかの意思決定プロセスを自動化し、Slack、Teams、Jira など DevSecOps チームが使用しているプラットフォームの通知機能を利用して継続的なフィードバックを送ってくれること。

また、ツールに依存せず、商用の静的解析、動的解析、インタラクティブ解析、ソフトウェア・コンポジション解析ツール、および OWASP ZAP、SpotBugs、OWASP Dependency Check などのオープンソース・ツールと自由に組み合わせて使用できること。そして拡張性とスケーラビリティ、適応性に優れていること、などが挙げられます。

これらすべての条件を満たしているのが、シノプシスの Intelligent Orchestration です。

Intelligent Orchestration：インテリジェンスに裏打ちされた経験

今回紹介する金融サービス企業（重要な個人情報を扱っているため、企業名は非公開を希望）のアプリケーション・セキュリティ・イニシアティブ担当シニア・テクニカル・リードは、次のように述べています。「アプリケーション・テストには、高速であることと邪魔にならないことが求められます。開発者は必要以上にセキュリティ・テストに時間を取られることを最も嫌います」

「当社が求めているのは、適切なテストを適切なタイミングで実行し、適切な量のデータを適切なタイミングで取得することです。例えば CSS ページを 1 つだけ変更した場合のように、Web アプリケーションに軽微な変更を加えただけなら、その時点で静的解析を再度実行する必要は恐らくないでしょう。オープンソース依存ファイルに変更がなければ、SCA（ソフトウェア・コンポジション解析）スキャンも不要なはずです」

「そこで、開発者がコードに加えた変更の重要度、および開発中のアプリケーションのリスク・プロファイルを考慮してくれるアプリケーション・セキュリティ・テスト・オーケストレーション・ソリューションの開発支援をシノプシス社のコンサルタントに依頼しました。要するに、当社のセキュリティ・アクティビティ全般を自動で誘導してくれる交通整理をしてくれる警察官のようなものを開発しようと考えたわけです。こうして完成した Intelligent Orchestration は、セキュリティ・アクティビティを適切な方向へ導いてくれ、交通渋滞を解消してくれています」

「しかも、Intelligent Orchestration は処方箋なのです。病院に行った時のことを考えてみてください。医師は患者が受診するたびに MRI 検査を実施するのではなく、患者の現在の健康状態を評価し、それに応じて適切な処置を施します。MRI を受けた方が良いのか、そこまでの検査は不要なのかは、医師が自らのインテリジェンスに裏打ちされた経験に基づいて判断します。Intelligent Orchestration の場合、この「インテリジェンス」が「コード」に相当し、「経験」が「ポリシー」に相当します」

コードとしてのセキュリティ・ポリシー

どの組織にも、ルールを定義するポリシーが存在します。例えば、「外部に公開された重要なアプリケーションは、90 日ごとに手動のペネトレーション・テストが必要」といったものがポリシーです。ほとんどの組織では、これらのポリシーはセキュリティ・グループによって適用されますが、セキュリティ・グループが 1 名で構成されている場合もあり、ポリシーの適用がボトルネックとなって本番環境への投入スケジュールが遅れることもしばしばです。常に誰かがポリシーを監視し、DevOps チームのプロダクション・パイプラインとの同期に注意を払っていないと、締切直前になってセキュリティ要件への適合に追われることになります。本番環境へのデプロイが 4 日後に迫った時点で、ペネトレーション・テストやマニュアル・コード・レビューの担当者を探し始めるといったことになりかねません。

Intelligent Orchestration なら、セキュリティ・ポリシーはコードに変換され、既存のビルド / リリース・パイプラインと並行して動作する専用の CI パイプラインに適用されます。例えば、あるアプリケーションに対して 90 日ごとにペネトレーション・テストを実行するようにポリシーで定められている場合、Intelligent Orchestration は 80 日（などポリシーが示すタイム・フレーム）が経過した時点でチームに注意喚起の事前通知を送信します。ほとんどの組織は、何らかの内部テクノロジーを使用してポリシーを格納しています。シノプシスはクライアントのセキュリティ・チームに対し、手動で適用されるこれらのポリシーを Intelligent Orchestration で自動的に適用できるコードに変換する作業の支援を提供しています。

成果：混乱が緩和され、リソースへの負担が軽減

前出のシニア・テクニカル・リードは次のように述べています。「リリース候補やプル・リクエストが上がってくるたびに、これらはアプリケーション・セキュリティ・テスト・オーケストレーション・パイプラインを通じて実行されます。このソリューションを導入して本当に良かったのは、不必要なテストが削減された結果、管理すべきデータの量が減ったことです。以前は重複するテストからのデータの整合性をとろうとして現場は混乱していましたが、そうしたことも緩和され、最終的にリソースへの負担が軽減されました。ほとんどの組織がそうだと思いますが、当社もリソースは既に逼迫しています。Intelligent Orchestration のおかげでより付加価値の高い作業に専念できるようになりました」

「アプリケーションをプロダクション環境へデプロイする際に、アプリケーションのリスク・プロファイルを Intelligent Orchestration に入力します。例えば、そのアプリケーションはどのようなデータを管理するのか、実行時間は長いか、数ミリ秒か、どの部分がアタック・サーフェスとなるのか、といったことです。低リスクのアプリケーションであれば、頻繁なセキュリティ・チェックは必要ないと考えられます。Intelligent Orchestration のリスク・プロファイル機能は、監査人との関係においても重要な役割を果たしています。これらの決定がどのようになされたのかを記録した文書がなければ、監査人に対してその決定の正当性を主張するのは困難です。Intelligent Orchestration は詳細なアプリケーション・リスク・プロファイル情報を提供してくれるだけでなく、いつどのような理由でテストの決定がなされたのかをログとして記録し、その決定によって生じた結果を示してくれます。これらはすべて文書化されており、その文書があるだけで監査人の心証を良くすることもあります」

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