WhiteSource ユーザー事例

GLOBAL IT AND SERVICES

GLOBAL IT AND SERVICES 社のオープンソースのセキュリティとコンプライアンス管理を顧客に提供する方法

IT&Services

コンシューマ・トランザクション・テクノロジーのリーディング・プロバイダーである GLOBAL IT AND SERVICES 社はオープンソースのセキュリティリスクを回避しました。

課題

約 200 カ国に顧客を持ち、複数の地域に 30,000 人以上の従業員を持つ、コンシューマ・トランザクション・テクノロジーのグローバルリーダー GLOBAL IT AND SERVICES 社は、常にオープンソースのコンポーネントとその使用を手動でモニターしていました。

近年、脆弱なオープンソースコンポーネントが一番の脅威になり、既知のセキュリティ脆弱性が依然としてデータ漏洩やサイバー脅威の主な原因です。

GLOBAL IT AND SERVICES 社が行なっていた手動トラッキングシステムは、時間と人的資源の両方の面において非常にコストがかかり、また欠陥もあり、会社とその顧客を複数のリスクにさらしていることがわかってきました。

オープンソースセキュリティの脆弱性について

• オープンソースソフトウェアのセキュリティ上の脆弱性を手動でトラッキングすることは実質不可能です。現時点において、すべての既知のオープンソースの脆弱性に対する単一のリポジトリは存在しません。

•多数の利用可能なオープンソースのリポジトリとデータベースにおいて脆弱なコンポーネントに適切なパッチや修正を見つけ出すには多くの労力を必要とし完全にそれを完了させることはできません。

• オープンソースコンポーネントとライブラリ間の依存性はさまざまです。脆弱性が発見されたら、危険なコンポーネントを手動で探し、コンポーネントと関連するブランチのリスクを軽減することは時間のかかる作業であり、完璧に完了させることは不可能です。

HIGHLIGHTS

✓ コンシューマトランザクションテクノロジーのトッププロバイダーである同社は手動でのオープンソースのトラッキングから、自動オープンソース管理に移行することを決めました。

✓ 手作業によるトラッキングは、コストがかかり、非効率的であり、またセキュリティリスクとライセンスコンプライアンスの問題にさらされていました。

✓ WhiteSource プラグインはビルドツールや CI ツールへ簡単に統合でき、リアルタイムでオープンソースコンポーネントをモニターし、レポートすることができます。

✓ 研究開発チームはセキュリティ上の脆弱性、コンプライアンスリスクおよび推奨される改善策に関するリアルタイムのデータを受け取ることができます。

✓ オープンソースコンポーネントと製品ライブラリの修正と更新は、開発ライフサイクルの初期段階で実装されています。

WhiteSource は自動的に 20 以上の開発プロジェクトがモニターでき、1 万以上のライブラリをカバーしています。

製品デリバリの遅延について

• オープンソースコンポーネントは様々なオンラインリポジトリにおいて提供されているため、コードに組み込まれているオープンソースコンポーネントの品質や安全性を開発者が把握する方法がありません。

• ソフトウェア開発ライフサイクル（SDLC）の後半段階でオープンソースのバグまたは脆弱性が発見された場合、その修正に多くの遅延が発生します。

WhiteSource

ライセンスとコンプライアンスのリスクについて

• オープンソースのコンポーネントがライセンスされ、他の製品のソフトウェアに準拠していることを確認することは必要不可欠であり、理想的には開発初期段階で行なっておくべきことです。このステップを手作業で行なった場合、開発の遅れや期間の長さ、またコストもかかる可能性があります。

GLOBAL IT AND SERVICES 社はオープンソースコンポーネントを手動でモニターするという選択肢はないと認識し、SDLC の初期段階においてもオープンソースのライセンスへの準拠だけでなく、リアルタイムでセキュリティ脆弱性を見つけ、対処するための自動で継続的なソリューションに投資することを決定しました。

ソリューション

同社は自動化されたオープンソースのセキュリティおよびコンプライアンスソリューションのいくつかの製品を評価しました。

１つのソリューションはコードスキャナでした。
以前はコードスキャンがオープンソースの使用状況をモニターし管理する方法として普及していましたが、SDLC 全体でリアルタイムデータを提供するには非常に時間のかかるプロセスであることがわかりました。
また、オープンソースの脆弱性を自動で継続的にリアルタイムでモニターすることが必要であったため、コードスキャナはその適切な選択肢ではなく、彼らは開発に遅延を引き起こすことなく、SDLC プロセスに統合し、オープンソースコンポーネントを配置、トラッキングし、リアルタイムでアラートおよびその救済策の提供を行なう継続自動ソリューションを選択しました。

WhiteSource は複数のプログラミング言語を使用したプロジェクトでテストされ、プロバイダーが使用する様々な言語をサポートすることができることを確認し、2 つの WhiteSource プラグインでテストを実施しました。１つは彼らの Java ビルドツールである Maven にあり、もう 1 つは彼らの継続統合サーバーである Jenkins にあります。プラグインは両方とも数分で簡単に導入することができ、ビルドプロセスにシームレスに統合することができました。

Screen image : ダッシュボード（スキャン結果の全体情報）

WhiteSource を導入して以来、数百の CVE が検出されセキュリティリスクの約 70%が処理されました。

結果

開発チームは毎日、ビルドが実行されるたびにレポートを作成することができ、オープンソースコンポーネントに関するリアルタイムのデータを受け取ることができました。これにより開発の初期段階から、アプリケーションライフサイクル全体にわたりコンポーネントを管理することができるようになりました。

同社の製品において WhiteSource とは異なるソリューションを実行した結果と比較すると、**WhiteSource の継続自動化ソリューションは誤検出率ゼロの最も包括的なレポートを作成できていることがわかりました。**
そのレポートではライセンスにおける問題点に加えて、修正のための特定の解決策を提示し、オープンソースの脆弱性とその重大度が詳細に記述されていました。

メリット

1. リアルタイムでの脆弱性の自動検出と修復

WhiteSource ソリューションを使用して、開発プロジェクトのうち 20 件を自動的にモニターし、10,000 を超えるライブラリをカバーしています。ビルドが実行されるたびに、脆弱なオープンソースコンポーネントが自動的に検出され、リスクの程度や推奨される修復に関するすべてのデータが開発者に自動的に配信されます。

2. DevOps 全体に渡る継続的なレポートとセキュリティ

WhiteSource のデータベースを CI サービスに接続する様々なプラグインがあり、SDLC の様々な段階でオープンソースのセキュリティを監視し、オープンソースの脆弱性に関するさまざまなレポートとセキュリティアラートを作成します。

3. ライセンスとコンプライアンスのリスク管理

アラート通知する自動ポリシーを作成することにより、開発者が GPL ライセンスコンポーネントをソフトウェアに追加しようとするたびに、GPL ライセンスコンポーネントを監視し、その使用を防止することができます。

4. 組織全体でのオープンソースの管理

数百以上ものエンドユーザーをサポートする数十のプロジェクトにおいて製品が稼動しており、異なるユーザーグループが特定のプロジェクトやプロセスにとって重要なアクセス許可をモニターできるように構成されています。

WhiteSource を導入して以来、数百の CVE が検出され、セキュリティリスクの約 70%が処理されました。

●お問合せは

WhiteSource 国内販売元
GDEP Solutions
GDEPソリューションズ株式会社
〒113-0033 東京都文京区本郷三丁34番3号 本郷第一ビル8階
TEL：03-5802-7050　FAX：03-5842-4123
E-mail：gdepsales@gdep-sol.co.jp