SDLC 早期での脆弱性除去に成功した Société Française du Radiotelephone (SFR)

企業概要

Altice France はフランス国内でテレコムとメディアの統合をリードする企業で、Société Française du Radiotelephone（SFR）事業部門を通じて 2300 万の個人および法人顧客に対し、音声、ビデオ、データ、インターネット・テレコミュニケーションおよびプロフェッショナル・サービスを提供しています。

課題：コード・セキュリティを開発の中心に

2300 万以上の顧客を擁する SFR の B2C（Business-to-Consumer）IT 部門は、Web、フロントエンド、オフィス・アプリケーションなど年間数十におよぶ大規模プロジェクトをデプロイしています。こうした開発の早期段階でコード・セキュリティを確保するため、B2C IT 部門は現行のサイバーセキュリティ・ストラテジーを改善すること、および現在使用中のツールを補完する形で動的スキャナーを導入することを検討しました。動的スキャナーとは、複数のアプリケーション間、またはフロントエンドとバックエンド間のコード実行および連携のフレームワーク内で動的にセキュリティ対策をとることができるものを言います。

具体的に、SFR は以下の条件を満たしたソリューションを求めていました。

- 開発者がサイバーセキュリティに積極的に関与し、問題の発生状況を知ることができる。
- プロジェクトの本番環境で脆弱性の数を削減できる。
- 顧客への潜在的な影響、および監督官庁による罰金のリスクを軽減できる。
- 開発者 / テスト担当者が SDLC の早期にバグを修正できる。
- CI/CD ワークフローの一環として自動セキュリティ・テストを実行し、脆弱性を即座に検知できる。
- コンテキスト情報を取得して脆弱性を容易に再現し、リアルタイムに修正できる。
- すぐに結果が得られ、速やかに修正を完了できる。
- SAST スキャナーに比べ、検知の精度が高い。
- 部門横断的なコラボレーションが容易。

「SFR が Seeker を選んだのは、Web アプリケーションのコード脆弱性を防ぐこと、およびリアルタイムに結果を取得して速やかに修正することが目的でした。」

Robert Cohen 氏
SFR、バリデーション / セキュリティ担当ディレクター

ソリューション：SDLC の早期に脆弱性を特定できるエンタープライズ・クラスの IAST

ブラック・ダックの IAST ソリューション Seeker は、開発チームとセキュリティ・チームのコラボレーションを促しながら、リスクの高いセキュリティ上の弱点を簡単に見つけられるように設計されています。Seeker は Web アプリケーションの脆弱性を検知し、これらをビジネスへの影響に直接関連付けて、リスクを明確に説明します。Seeker は CI/CD ワークフローへシームレスに統合して自動でアプリケーション・セキュリティ・テストを実行できるため、リリース・サイクルの遅れもありません。

Seeker を使用すると、開発者は SDLC の早期に重大なセキュリティの欠陥を修正できるため、貴重な時間とリソース、コストの節約につながります。また、本番環境にデプロイする前にアプリのセキュリティを確保できるため、リスクも軽減されます。

Seeker は検知結果をリアルタイムに自動で検証するため、他のアプリケーション・セキュリティ・テスト・ツールのように誤検知が頻繁に発生することもなく、深刻度の高いものから優先的に対応するトリアージも容易となります。

また、コード内での脆弱性の正確な場所、修正アドバイス、およびコード実行フローの情報も Seeker から得られるため、開発者は脆弱性を速やかに修正できます。

成果：開発者がセキュリティ・テストの中心に

SFR はまだ Seeker の実装途中ですが、最終的にはすべてのコード・レビューにこの IAST ソリューションを常時活用する予定です。B2C IT 部門は現在、1 日あたり約 12 のオンプレミス・アプリケーションをテストしており、最終的にはこの数字を数十にまで引き上げることを計画しています。このソリューションの導入が完了すれば、誤検知が減少し、生産性が飛躍的に向上するものと期待されます。

まだ導入初期にもかかわらず、SFR では既に以下のような形で Seeker の効果が現れています。

- 従来型の SAST など、他のソフトウェアよりも検知能力が向上。
- 開発者がセキュリティ対策の中心となって、コード開発に従事しながらセキュリティ規範への適合にも権限を行使。

SFR、B2C IT 部門のサイバーセキュリティ担当シニア・マネージャー、Zine-Eddine Yahoui 氏は、Seeker の特に気に入った特長として、コード実行時に脆弱性を特定できること、情報量の豊富なレポート、コード行を特定できるため開発チームによる修正プロセスが容易なこと、そして修正アドバイスなどを挙げています。

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

©2024 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2024 年 9 月