Parkeon が Seeker で 最高レベルのセキュリティを提供

「Seeker は、統合や自動化といった当社のニーズに応えてくれました。ユーザーは Seeker からトレーニングや知識を得ることができます。Seeker は、当社のセキュリティを向上させ優れたソフトウェアを開発するための完璧なツールです」

L. Porchon

Parkeon マネージドビジネスサービス
担当最高情報
セキュリティ責任者

ビジネスの概要と課題

Parkeon は、都市モビリティ分野におけるキープレーヤーで、駐車場および輸送管理ソリューションのグローバルプロバイダーです。同社は、独自の駐車場管理および料金支払いサービスを世界 55 か国 3,000 以上の都市で展開しています。

Parkeon は、クレジットカードやデビットカード、携帯電話アカウント、プリペイドカード、電子財布スキーム、接触・非接触カード技術など、さまざまな販売チャネルに適合したリアルタイムの料金支払いシステムを開発しています。これらのソリューションは、舗道のパーキングメーター、パーキングチケット発券機、駐車場精算機など、同社独自の POS 端末で利用されています。

E コマースや遠隔 POS の販売に影響を及ぼすセキュリティ侵害が増え続けていることを受けて、Parkeon は、自社のアプリケーションのセキュリティを地理的な設置場所を問わず可能な限り高いレベルに引き上げるプロセスの導入を決めました。

Parkeon の IT 部門は、同社の電子チケッティングおよび販売の主要プロダクトである ArchiPEL のエンドツーエンドのセキュリティおよび PCI (Payment Card Industry) コンプライアンスを検証するために、Seeker® を選定しました。Seeker を選定した理由は、脆弱性の確実な検出機能および PCI コンプライアンスの検証機能を併せ持っていることに加え、開発プロセスに統合可能で、セキュリティに関する技術を持たない開発者やテスターでも簡単に使えることでした。

ソリューションの評価

Parkeon は、料金の支払いに関する幅広いソリューションを開発しており、その顧客に代わって電子支払いフローの集約化も提供しています。いずれの活動でも、ソリューションアーキテクチャ全体が PCI-DSS (PCI データセキュリティスタンダード) などの業界標準や基準に適合している必要があります。

Parkeon はかつて、動的アプリケーション・セキュリティ・テスト (DAST) ツールをインテグレーション環境に導入し、アプリケーションのセキュリティの検証を行っていましたが、満足な成果を得ることはできませんでした。

Parkeon のアプリケーションはアジャイル方式で開発され、アップデートは四半期に 5 回実施されています。セキュリティ検証は、既存の自動化されたプロセスに統合する必要があり、セキュリティの専門家ではない一般の開発者やテスターでも行える必要がありました。

ビジネス上の利点

- Seeker は、各リリースのセキュリティ標準への適合性をシステム全体すなわちエンドツーエンドで確保します。
  Seeker はデータに着目することで、PCI-DSS セクション 6 をはじめとするクリティカルなデータ要件に対して、強い優位性を発揮します。
- Seeker は検証チームと開発チームのコミュニケーションを円滑にします。
  すべての脆弱性は、適切な修正案とともに、問題のあるソースコードに自動的にリンクされます。
- Seeker は開発者の意識を高め、よりセキュアなコーディング方法の習得に役立ちます。
  開発者は単に脆弱性を修正する訳ではありません。自らのコードの問題点を修正することによって、セキュアなコーディング方法を習得でき、次に活かすことができます。

「Seeker を選んだのは、テスターおよび開発者がセキュリティ関連のタスクに定例的に時間を費やすことや、特別な技術を必要としないためです。Seeker によって提供される脆弱性と影響を受けるソースコードとの関連付け情報により、開発者の負担が減少しました」

L. Porchon

Parkeon マネージドビジネスサービス
担当最高情報
セキュリティ責任者

導入後の利点

Parkeon は、Seeker を使い始めて 3 つの大きな利点に気づき、Seeker が求めていたツールであることが分かりました。

第一に、Seeker は、アプリケーション全体のデータフローを把握し、PCI-DSS などのセキュリティ標準への適合性をシステム全体すなわちエンドツーエンドで確保します。Seeker は、機密データに対する影響度との関連性で脆弱性を特定します。

Seeker のデータ中心のアプローチは、PCI-DSS セクション 6 の要件に対するテストに強い優位性を発揮します。クレジットカード情報などのクリティカルなデータは、支払いに関連する複数のコンポーネントにわたって、情報漏洩の危険がある脆弱性（デバッグデータの消し忘れ、セキュアでないデータ操作、ファイルやデータベースへのセキュアでない保存（一時保存を含む）、第三者へのセキュアでない送信など）がないか検証するため、自動的にトラッキングされます。

Seeker の導入によって、Parkeon は、各リリースにおいてシステム全体のセキュリティ標準への適合性を自動的に確認できるようになりました。

第二に、Seeker は、脆弱性と問題のあるソースコードをリンクさせることによって、検証チームと開発チームのコミュニケーションを円滑にします。脆弱性を URL として提示する他の動的テストツールとは異なり、Seeker は脆弱性を修正の必要があるソースコードに自動的に結び付けます。これにより、誤検知が排除されるとともに、ソースコードの脆弱な箇所が特定され、テスト対象アプリケーション用に作成された明確な修正アドバイスが開発者に提供されます。

Parkeon は、セキュリティを向上させると同時にセキュリティテストに費やしていた時間を削減し、セキュリティ担当者と R&D 担当者のコミュニケーションの活性化に成功しました。

- 開発者は、対処が必要な脆弱性に集中できるようになり、Seeker が提示する方法に従ってソースコードを修正すればよくなりました。
- テスターは、Parkeon の全社セキュリティ標準である OWASP Top 10 の基準に従って、作成されたアプリケーションにどのようなビジネスリスクがあるかを明確に把握できるようになりました。

第三に、Seeker は、セキュリティに対する意識を高め、開発者のよりセキュアなコーディング方法の習得に役立ちます。Parkeon の開発者およびテスターは、OWASP Top10 を基準とした訓練を受けていますが、情報セキュリティの専門家ではありません。Seeker は、さまざまな攻撃の再現や、具体的なビジネスリスクの説明および適切な修正策を提示します。検証チームおよび開発チームは、Seeker の利用を通じて問題意識を獲得するとともに、スキルを強化することができ、結果としてコードのセキュリティ向上につながっています。

まとめ

Seeker は、Parkeon のセキュリティオートメーションプロセスにシームレスにフィットしました。Parkeon の開発チームおよび検証チームは、生産性およびセキュリティ意識を向上させながら、標準に準拠したセキュアな本番リリースを高頻度で実施できるようになりました。

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