opentext™ | Cybersecurity

お客様事例

DATEV eG

OpenText Fortify は、変化する要件に合わせて対応し、複雑さの低減と開発コラボレーションの向上をサポートします。

DATEV について

DATEV は、税理士、監査役、弁護士、およびそのクライアントを対象にソフトウェアを提供しています。200 万社を超えるドイツの企業が、財務会計に DATEV のソフトウェアを使用しています。ニュルンベルクにある DATEV の印刷 / 発送センターでは、毎月約 200 万件のビジネスアセスメントが処理されています。毎月 1,100 万件以上の給与明細が、DATEV のソフトウェアを使用して処理されています。

ハイブリッドクラウドインフラストラクチャへの移行による柔軟性とスケーラビリティの向上

DATEV は常にデータ保護とセキュリティを優先してきました。同社が数年前に OpenText™ Fortify™ を導入して、ソフトウェア開発ライフサイクル内のコードレベルでアプリケーションセキュリティ (AppSec) を強化することを決断したのも、そのためです。その当時の DATEV の IT 戦略は、2,000 人以上の社内開発者をサポートするために、オンプレミスのデータセンターベースのインフラで管理されていました。Fortify は、DATEV で使用されていた多くのプログラミング言語をサポートしていたため、静的コードスキャンに最適なソリューションであると判断されました。

「Fortify を CI/CD パイプラインの一部として使用することで、脆弱性が大幅に減少しました。このことはペネトレーションテストで明らかで、バグの修正にかかる時間が大幅に減り、お客様にメリットをもたらすような新機能を導入してアプリケーションを強化するための時間が増えるということです」

Roman Belikow 氏
セキュリティエンジニア
DATEV

DATEV のセキュリティエンジニアである Roman Belikow 氏は、この数年でどのように変化したかについて、次のように説明しています。「当社はお客様のビジネスモデルの変化に対応するため、より柔軟でオープンなアプローチを採用する必要があると感じていました。これに加えて、当社のインフラストラクチャが複雑化し、サポートや保守が困難になっていたこともあり、ハイブリッドクラウド戦略を採用することになりました。AWS や Azure などの一般的なパブリッククラウドに当社のアプリケーションを展開できるようにしたいと考えました。そうすれば、外部の開発パートナーに当社の開発プロセスを公開する機会も得られます」

Belikow 氏は次のように続けます。「ハイブリッドクラウドへの移行の一環として、DevSecOps パイプラインを完全に統合できる機能を備え、クラウドでセキュアな DevOps を提供するホスティング型 Fortify を見つけられたことは、とても良かった。オンプレミス版の Fortify と同じ使い慣れたユーザーインターフェイスを備え、通常はシングルテナントインスタンスでクラウド

DATEV

概要

業種

テクノロジー

所在地

ドイツ

課題

開発の柔軟性とスケーラビリティを高めることを目的とした、オンプレミスからハイブリッドクラウドへの移行戦略をサポートするため、アプリケーションセキュリティをモダナイズする

製品とサービス

ホスティング型 OpenText™ Fortify™

成功ポイント

- 外部パートナーとシームレスに連携できるようになり開発の柔軟性が向上
- SAST 機能と DAST 機能の統合による複雑さの低減
- コードの脆弱性を減らすことでアプリケーションの品質を向上
- オンプレミスインフラストラクチャの保守とサポートが不要になったことに伴う関連コストの削減

にホストされるため、保守とサポートを簡素化できます。それでも、Fortify を他の主要な AppSec ソリューションと比較して、Fortify が当社に最適であることを確認する良い機会となりました。Fortify のスキャン品質は、比較した競合ソリューションよりも優れていることがわかりました。非常にユーザーフレンドリーなソリューションであり、長年にわたって言語サポートがさらに拡張されていたために当社に必要なすべてが網羅されていることを確認できたのは幸いでした。ホスティング型 Fortify が当社に最適なソリューションであることは明らかでした」

ホスティング型 Fortify への効果的な移行により開発コラボレーションを強化

OpenText の専門的なサポートを受けながら、DATEV チームが自ら、オンプレミス版 Fortify からホスティング型 Fortify への移行を行いました。Belikow 氏とチームは、Fortify Command Line (fcli) などのさまざまなツールを使用して、独自の Fortify スクリプトの移行を実施しました。Fortify は DATEV の CI/CD 開発パイプラインに完全に統合され、自動化サーバーとして Jenkins、問題追跡に GitLab と Azure を使用し、Azure の DevOps 機能を活用しています。Belikow 氏は、DATEV の多くの開発チームが Fortify を日々どのように使用しているかについて、次のようにコメントしています。「当社ではすべての開発チームがアジャイル手法を採用しており、Fortify はアプリケーションに応じて、毎日またはときには毎週コードをスキャンするために活用されています。また、Infrastructure as Code (IaC) のベストセキュリティプラクティスを適用する目的でも使用されています」

このような大規模な開発コミュニティ内で効果的に知識を共有するため、DATEV はセキュリティチャンピオンを任命しました。これらの担当者は Fortify に関する高度なトレーニングを受けており、開発チームからのあらゆるセキュリティ関連の質問に回答できます。Fortify やその他のツールから得られたセキュリティ関連の知見は適切な情報交換が行われており、この情報を効果的に共有することで、往々にして問題が迅速に修正されるようになり、誤検出が減少します。

Fortify DAST の導入による複雑さの低減

Fortify が導入されたのは、その業界をリードする静的アプリケーションセキュリティテスト (SAST) 機能によって、開発サイクルの初期段階でコードの脆弱性を特定し、迅速に修正を行うためでした。DATEV にとっての最優先事項であるデータ保護を実現するため、チームは CI/CD パイプラインの変化するニーズに応じて、SAST コードスキャンを動的にスケールアップ / スケールダウンすることができました。また、Fortify は動的アプリケーションセキュリティテスト (DAST) 機能も提供しています。これは、実行中のアプリケーションに対する外部からの実際のセキュリティ攻撃をシミュレートすることで問題を特定し、根本原因分析を行うための優先順位を付ける機能です。DATEV は、別のツールを使用して DAST を行っていましたが、ホスティング型 Fortify への移行の際に、既存の DAST ツールを Fortify に置き換えました。

Belikow 氏はその理由を次のように説明しています。「当社にはすでに 10 年以上の Fortify の経験があり、開発チーム内に広範な専門知識が蓄積されていました。クラウドネイティブのオンラインアプリケーションに移行する中で、Fortify の DAST 機能を活用するのが自然なことだと感じました。これで、開発者は SAST と DAST のスキャン結果を同じユーザーフレンドリーなインターフェイスで確認できるようになるため、複雑さの低減に役立つと思われます。すぐに、SAST と DAST の結果の相関関係も示せるようになると見込んでいます。そうすれば、誤検出率を減らして最も重要な脆弱性に注力できるようになります」

DATEV は、まだ DAST の導入の初期段階にありますが、Fortify トレーニングコースを DAST 機能に関するコースも含めて範囲を拡大しているところです。このことは、同社のセキュリティオペレーションセンターにとって特に重要です。チームが実際のサイバー攻撃と Fortify DAST によって開始されたテスト攻撃を区別できるようにする必要があるためです。

脆弱性の減少によるアプリケーションのさらなる品質向上

DATEV のような大規模な組織では、ハイブリッドクラウドインフラストラクチャへの移行を一晩で完了させることはできません。多くのアプリケーションの適応または置き換えが必要になるだけでなく、移行には意

「クラウドネイティブのオンラインアプリケーションに移行する中で、Fortify の DAST 機能を活用するのが自然なことだと感じました。これで、開発者は SAST と DAST のスキャン結果を同じユーザーフレンドリーなインターフェイスで確認できるようになるため、複雑さの低減に役立つと思われます」

Roman Belikow 氏
セキュリティエンジニア
DATEV

識改革も必要です。Belikow 氏は次のようにコメントしています。「この新しいアプローチにより、外部パートナーとの連携がよりオープンになりました。これによって、当社は俊敏性を増し、お客様が求めるスピードで業務を進めることができます。物理的なフットプリントを縮小したことで、グリーン IT 目標にも合致し、複雑なオンプレミスインフラストラクチャの管理とサポートに関連するコストを削減することもできました。ホスティング型 Fortify への移行により、当社のソリューションは常に最新のバージョンを維持できるようになり、問題が発生した場合は、OpenText が直接迅速に対処してくれます」

Belikow 氏は次のように結論付けます。「当社の開発プロジェクトは、ホスティング型 Fortify にすべて移行されました。Fortify を CI/CD パイプラインの一部として使用することで、脆弱性が大幅に減少しました。このことはペネトレーションテストで明らかで、バグの修正にかかる時間が大幅に減り、お客様にメリットをもたらすような新機能を導入してアプリケーションを強化するための時間が増えるということです。私たちは、Fortify がこれまでの長い年月を経てどれほど進化したか、また当社からの問い合わせにいついかなる時にも対応してくれた OpenText のサポートが提供してきた専門知識に、深く感銘を受けています」

お問い合わせ
www.opentext.com/products/security-cloud

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。