大手クレジットグループ

Fortify により、コードの脆弱性を 50% 削減し、ベンダーとのコラボレーションを促進しながら、サイバーレジリエンスを強化して、DORA の施行に対応。

DORA の施行に伴う新たな課題

金融業界の企業は、すでに多数の規制要件に準拠することが求められています。欧州連合 (EU) では、準拠すべき規制要件として、新たにデジタルオペレーショナルレジリエンス法 (DORA) が施行されました。DORA は、金融機関のデジタルシステムのセキュリティを強化するための要件について、欧州全体で統一することを目的としています。DORA の一環として、金融機関は新規サービスを導入 (または既存サービスを再導入) する前に、脆弱性評価を実施することが義務付けられます。また、すべての重要アプリケーション / システムを年に 1 回以上テストする必要があります。

「ソフトウェアライフサイクル管理に『セキュリティバイデザイン』の原則を採用することは、当社のサイバーレジリエンス戦略にとって不可欠だと考えています。脆弱性分析の深さ、広さ、正確さ、DevOps との統合、および柔軟なサービスモデルを備えた Fortify は、当社にとって理想的なテクノロジーパートナーとなっています」

最高情報セキュリティ責任者
大手クレジットグループ

ある大手クレジットグループは、ソフトウェア開発サイクル内に適切なテストツールを統合することで、ソフトウェアソリューションのレジリエンスを高めて、DORA に対応する必要がありました。そこで、同社は信頼できるパートナーである Join Business Management Consulting に支援を求めました。Join Business Management Consulting は、欧州で最も急成長している戦略経営コンサルティング企業として、Financial Times 紙や Il Sole 24 Ore 紙のランキングにも名を連ねている企業です。Join Business Management Consulting のリスク、コンプライアンス、サイバーセキュリティプラクティス担当責任者、Maurizio Garofalo 氏は次のように説明します。「まず、市場分析を行い、アプリケーションのライフサイクルに静的解析を導入する必要性など、クライアントの要件を満たすソリューションを特定しました」

他社製品と比較して、Fortify は期待以上の製品

Garofalo 氏は次のように続けます。「その結果、Fortify by OpenText が同クレジットグループのニーズに最適なソリューションであると判断しました。Fortify は、クライアントが定めた基準だけでなく、その他の基準においても他のソリューションに勝る点がいくつもありました。まずは、その優れた信頼性と豊富な機能を高く評価しました。Fortify は、Gartner、Forrester、IDC、G2 などの主要アナリストが市場リーダーとして評価する、定評あるソリューションです。

概要

業種
金融

所在地
イタリア

課題
外部ソフトウェアの導入プロセスを簡素化しながら、新規金融規制へのコンプライアンス対応について、金融業界のクライアントを支援する

製品とサービス
Fortify

成功ポイント
- DORA の完全遵守
- コードの脆弱性を 50% 削減
- 外部ソフトウェアの導入プロセスを簡素化して、ベンダーとのコラボレーションを向上
- 同クレジットグループのビジネスモデルに適した柔軟な導入モデル
- 「セキュリティバイデザイン」の原則でサイバーレジリエンスを強化

また、広範な言語をサポートしており、オンプレミスと柔軟なクラウドサービスのいずれでも利用できる点も評価しました。オンプレミスなら開発サイクルのインフラストラクチャに簡単に追加でき、クラウドサービスならクライアントのソフトウェアパートナーにも最適です。これだけの利点を提供するソリューションを、パフォーマンスに劣る他社製品と同等のコストで得ることができるのです」

Fortify by OpenText™ は、20 年に渡る経験と継続的な改善に基づく、包括的で拡張可能なアプリケーションセキュリティソリューションスイートです。Fortify は、静的アプリケーションセキュリティテスト (SAST) モジュールによる静的解析、動的アプリケーションセキュリティテスト (DAST) モジュールによる動的解析、およびソフトウェアコンポジション解析 (SCA) を提供することで、エンドツーエンドのアプリケーションライフサイクル管理を可能にし、あらゆるオープンソースコードコンポーネントのセキュリティを確保します。また、Fortify は、高度な人工知能 (AI) 技術を用いて、コードの記述時にそのコードのセキュリティチェックを自動的に行い、必要な変更を提案します。これにより、コードの堅牢性を確保できます。「Fortify が提供するセキュリティレベルは、金融業界など、複数の分野において DevSecOps 開発モデルとコンプライアンスを促進できます」と Garofalo 氏は述べます。

DORA の完全遵守とベンダーとのコラボレーションの向上

プロジェクトを開始するにあたっては、Fortify on Demand が使用されました。Fortify on Demand は、インフラストラクチャやリソースを追加することなく、アプリケーションセキュリティをサービスとして利用できるソリューションです。このソリューションは、外部ベンダーや商用ベンダー (通常は銀行業務ソリューションを専門とする小規模ソフトウェア会社) のソフトウェアを検証する際に特に有効です。同クレジットグループは、ソースコードを外部ベンダーと共有することはできません。ソースコードが知的財産法で保護されているためです。また、自社のソフトウェア開発基準に従って検証されていないコードを採用することもできません。Fortify on Demand を活用することで、同クレジットグループは外部ベンダーに対してアプリケーションテスト (コードセキュリティスキャン) へのアクセスを提供できます。これにより、独立したセキュリティ証明書を取得し、当該ソフトウェアのセキュリティが自社の要件に準拠していることを確認できます。

同クレジットグループは、社内の 3 つの開発拠点で Fortify のオンプレミス版を活用しており、それぞれの拠点で異なる言語を使用しています。1 つ目の拠点では、ホームバンキングアプリケーションとモバイルアクセスのための関連アプリケーションを開発しています。2 つ目の拠点では、180 の支店間の通信を管理する情報システムのためのコアアプリケーションを開発しています。3 つ目の拠点では、デビットカード、クレジットカード、プリペイドカードの作成に使用するソフトウェアを開発しています。「オンデマンド機能とオンプレミス機能を備えた Fortify のハイブリッド導入モデルは、同クレジットグループのソフトウェア開発の中核を担っています。各コードコンポーネントを本番環境に導入する前に、その場でチェックして修正できます」と Garofalo 氏は説明します。

コードの脆弱性を 50% 削減し、15 の重要アプリケーションに実装

Fortify により、15 のビジネスクリティカルアプリケーション (開発したコードとオープンソースのコンポーネントの両方) を正常かつ円滑に実装できました。Fortify のプロセスにより、すべての新規ソフトウェアリリースが、OWASP (Open Worldwide Application Security Project) のトップ 10 の標準、および SANS (Sysadmin、Audit、Network and Security) のトップ 25 の標準に基づいて、保護および認定されています。Fortify を導入し、トレーニングプログラムをゲーム化したことで、セキュリティに対する開発者の認識が向上した結果、同クレジットグループはコードの脆弱性を 50% 削減することに成功しました。同社 CISO は次のようにコメントしています。「ソフトウェアライフサイクル管理に『セキュリティバイデザイン』の原則を採用することは、当社のサイバーレジリエンス戦略にとって不可欠だと考えています。脆弱性分析の深さ、広さ、正確さ、DevOps との統合、および柔軟なサービスモデルを備えた Fortify は、当社にとって理想的なテクノロジーパートナーとなっています」

「Fortify は、同クレジットグループのソフトウェア開発の中核を担っています。各コードコンポーネントを本番環境に導入する前に、その場でチェックして修正できます」

Maurizio Garofalo 氏
リスク、コンプライアンス、サイバーセキュリティプラクティス担当責任者
Join Business Management Consulting

お問い合わせ
www.CyberRes.com

Garofalo 氏は次のように結論付けています。「同クレジットグループは、アプリケーション開発のセキュリティを強化して、コードの脆弱性を排除し、DORA の規制に準拠することを可能にする Fortify の機能に大満足しています。また、同社は決済データを確実に暗号化するために、Voltage SecureData Payments by OpenText ソリューションも活用しています。これにより、PCI へのコンプライアンスを簡素化し、e コマースアプリケーション、Web、モバイルでの決済におけるクライアントのクレジットカードデータを保護できます。Voltage と Fortify の導入がいずれも成功に終わったため、同社はこの 2 つのソリューションを統合して、さらに価値を高めたいと考えています」

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。

768-JA0107-001 | O | 10/23 |