お客様成功事例

セキュリティ

Centrica/British Gas

クラウドベースのセキュリティテスト管理により、セキュリティと効率の向上とコスト削減を同時に実現しました。

概要

Centrica は、英国バークシャーのウィンザーに本社を置く多国籍公益事業会社です。スコットランドでは Scottish Gas、その他英国内では British Gas の商号で運営している国内最大のガス供給会社であり、電力最大手の 1 つでもあります。British Gas は、英国内の約 1200 万世帯にガスや電力を供給しています。

Paul Phillips 氏は、British Gas の Software Assurance and Integration 部門の責任者です。Phillips 氏の組織は、Centrica グループの British Gas ブランド向けに提供される開発処理のすべてについて、アプリケーションのセキュリティとコードの品質保証を担当しています。過去 3 年間、Phillips 氏と彼のチームが開発中のソフトウェアのセキュリティを確保するために活用してきたのが、Micro Focus® Fortify on Demand です。

それ以前は、British Gas は、現場で Fortify Static Code Analyzer と Micro Focus WebInspect を併用していました。これらの製品は、同社の運用上のニーズをサポートしています。Fortify on Demand は、アプリケーションセキュリティをリードする最新のソリューションです。

課題

変化する状況

変化する環境が、Fortify on Demand の導入決定を促しました。「我々の担当分野は、品質の保証と管理です」と、Phillips 氏は言います。「特に、新しい技術の発展を踏まえて、安全なコード開発を重視する必要性を認識しました。当社のデジタルチャネルは重要性を増しています。実際、お客様とのやり取りの 50% 以上がデジタルチャネルを通じて行われており、特にスマートフォンの利用が目立ってきています。顧客データを保護し、業界規制を遵守するには、予防的アプローチをとる必要があったのです。」Phillips 氏は、ガバナンスのフレームワークを確立するのに最適な手段と、フレームワークをサポートしているツールについて調査しました。パフォーマンスが極めて重要でしたが、コストも決定的な要素でした。「我々の業界では、サービスの規模のメリットを活かしてコストを抑制すると同時に、人材を効果的に活用することが、戦略の方向性として極めて重要でした」と、Phillips 氏は語ります。「これらの要件を満たしているのは、サービスベースのアプローチでした。当時、Fortify は、対応環境に SAP が含まれている数少ない実用的なソリューションの 1 つでした。これは、SAP を中核とした British Gas のシステムにおいて、特に重要な点でした。」

British Gas は長期にわたって従来型の情報セキュリティを利用していましたが、状況の変化によって新しいアプローチが必要となりました。「当然、ソーシャルエンジニアリングなどの新たに出現した脅威への脆弱性に対処する方法は、従来のファイアウォールによる保護とは完全に異なります」と Phillips 氏は言います。「考え方も、アプローチも、まったく異なります。」

centrica British Gas

概要

業界

エネルギー、公益

所在地

英国

課題

British Gas のアプリケーションに含まれる脆弱性を、ソフトウェア開発ライフサイクルにおいて早期に特定して修正する。

ソリューション

Fortify on Demand を使用して、社内およびサードパーティのコードに静的および動的スキャンを実行する。

成果

+ より効率的にコストを管理しながら生産性を向上
+ 主要なデジタルチャネルおよびモバイルアプリケーション向けのアプリケーションセキュリティを強化
+ 予防的アプローチの提供により顧客の機密データを保護
+ 業界規制に対するコンプライアンス対策を改善
+ British Gas の変更プランにおける予算および生産性目標を達成

ソリューション

早期発見、早期解決

Centrica/British Gas では、開発のほとんどが SAP の ABAP で行われています。そして、他の言語 (Java および .NET を含む) も使用されています。同社内の約 1500 名の開発者と、アウトソーシングベースのサードパーティが、約 50 のビジネスクリティカルなシステムとアプリケーションを担当しています。これには、英国顧客向けの主要デジタルチャネルである **www.britishgas.co.uk**、中核となる SAP の請求および CRM のシステム、そしてセルフサービス型のお客様用アプリケーションが含まれます。社内で開発されたコードのスキャンだけでなく、British Gas は、サードパーティのコードも Fortify on Demand で監査可能な状態とする義務について契約書に明記しています。

Phillips 氏は、「当社のアプローチは、「早期発見、早期解決」というものです。ライフサイクル最初のコンセプトの段階からプロジェクトに関与し、プロジェクトに期待される成果物を把握します。我々はプロジェクトにさまざまなコアサービスを提供します。中でも、静的スキャンと動的スキャンの 2 つは重要な要素です。プロジェクトが安全なコードを提供できるように計画を立て、適正な予算を提供します。開発ライフサイクルの最後に大きな脆弱性を見つけてプロジェクトの締め切りに影響が出るというような事態を無くすよう努めています。」と語っています。

静的スキャンはユニットテスト以降に頻繁に実施され、動的スキャンはコードがより成熟したときに実施されます。プロジェクトレベルでの動的スキャンは、全体的なリリースプロセスに移行する前に、コードがクリーンな状態であることを確認するために役立ちます。この時点で、ビジネスクリティカルなコアシステムの約 90% ～ 95% が Fortify on Demand でカバーされており、新しいものが定期的に追加されています。「2 年ごとに、ビジネスクリティカルなアプリケーションにつき少なくとも 1 回はコアスキャンを実施することを目指しています」と、Phillips 氏は語ります。

Fortify on Demand を導入することで、教育という大きな副次的メリットも得られました。「当初、安全なコードの開発に関して、開発コミュニティの意識は低い状態でした。」と、Phillips 氏は語ります。「すべての開発者に対して、安全なコーディングが重要である理由を説明する初期教育段階を経て、社内教育パッケージを作成しました。この開発者の意識を高める取り組みは、経営陣から完全なサポートを得ることができました。現在、安全なコーディングプラクティスは、会社のポリシーにおいて不可欠の要素となっています。」

成果

ビジネス上のメリット

コンプライアンスの観点において、Britsh Gas のアプリケーションが業界規制に準拠していることを確認するうえで、Fortify on Demand が役立ったと Phillips 氏は語っています。「定義済みのフレームワークとガバナンスプロセスが用意されていたので、我々はこれを共有しました。コンプライアンスの観点で、何を提示する必要があるのか、チェックボックスにチェックを入れていくような感じでした」と、Phillips 氏は語ります。Application security manager の Ramesh Nagaraj 氏は同意して、「Fortify on Demand は、クリティカルなアプリケーションの品質とセキュリティの確保について自信を与えてくれ、コンプライアンス要件を満たすための大きな支えとなっています」と語っています。「当社のソフトウェアライフサイクルに不可欠の要素です。最初に重要なことに集中することで、生産性を高めることができます」。

British Gas は開発の観点でもメリットを得ています。Phillips は続けて、「コードをより迅速に成熟させることに関して、「シフトレフト」の文化が確立されたため、保守はより容易になり、脆弱性は少なくなっています。Fortify on Demand の使用を開始したときと比べて、ソースコードに含まれる脆弱性の数量と重大度が確実に低下傾向にあることが分かります。」と、語っています。コードを作成して最終的にデプロイするソフトウェア開発ライフサイクルにおいて、「シフトレフト」とは、あらゆる取り組みを前倒しすることにより、コストが低下し、ビジネスの効率を高められることを意味します。Phillips 氏にとって、Fortify on Demand は、British Gas における時間・コスト・品質の三角形のすべてのポイントを押さえています。「我々には、非常に大規模な変更プランがありーそれは、予算編成メカニズムとして知られておりーコードの行数の観点からそれは大きな財産です。」と、彼は語ります。

「我々は、リスクの理解と低減に役立つと同時に、コスト面とプロジェクトスケジュール面で妥協しないサービスの提供を確約する必要がありました。デリバリーライフサイクルを大幅に延長したり、導入に多額のコストがかかったりするものは望ましくありませんでした。Fortify on Demand は現在、広範囲で使用されており、変更プランの重要な一部として広く受け入れられています」。

Micro Focus とは密接に連携しています。「実際の Fortify on Demand のスタッフは、ここ British Gas で、当社のアプリケーションセキュリティチームと開発コミュニティの両方と強固で良好な業務関係を築いています」と、Phillips 氏は語ります。「安全なコーディングについて、理に適った実用的な話し合いができ、その結果、我々は大きな経験と理解を得ることができました。これは、British Gas におけるアプリケーションセキュリティの継続的な改善につながります。」

今後、Phillips 氏は同社の増加しているモバイルフットプリントと、脅威の新たな経路であるソーシャルエンジニアリングへの漏洩を厳重に監視していきます。スマートメーターが、新たな攻撃のターゲットとなる可能性があるのです。「我々は、アーキテクチャと実践可能なアプローチを理解することで、初期段階から安全な設計を期し、プロセスの早い段階でできる限り多くの脆弱性を排除することに

取り組んでいます」と、Phillips 氏は語っています。

彼は、この取り組みに最適なソリューションを手にしています。「我々は、リスクを理解して低減し、安全で目的に合った製品を提供し、お客様の機密データを保護する必要があります。」Phillips 氏は締めくくります。「Fortify on Demand は、これらすべてを実現するための鍵です。」

詳細情報はこちら：
www.microfocus.com/fod

「2 年間にわたり、現場常駐コンサルタントの専門知識に大いに助けられました。ツールだけでなく、プロセスの側面からも、チームが Fortify ソフトウェアを理解できるように教えてくれました。」

UWE SODAN氏
TIP Security, Engineering Excellence and Education, Code Analysis Team Manager
SAP

お問い合わせ先：
www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp