お客様成功事例

セキュリティ

ServiceMaster

ServiceMaster は、Micro Focus® のセキュリティテクノロジーによりアプリケーションを変革することで、サイバー対策を整備し、DevOps のスピードを実現しています。

概要

ServiceMaster Global Holdings, Inc. は、85 年以上にわたり、北米全域で 75,000 の家庭と企業に毎日サービスを提供しています。Terminix、Merry Maids、American Home Shield を含む同社の 7 つのブランドを通じて、ハウスクリーニング、害虫駆除、災害後の修復などのサービスを提供しています。ServiceMaster は、2016 年、世界で最も評価の高い企業の 1 つとして Fortune 誌に掲載されました。

課題

お客様や競合他社のビジネスが次第にオンラインに移行しつつあったため、ServiceMaster は、ソーシャルメディア、モバイル、および Web を活用した大規模なデジタルトランスフォーメーションにより、ビジネスを再活性化しようと考えていました。しかしサイバーセキュリティ侵害が増加していたため、経営陣は、企業の評判を守るためにさらなる投資を行うことを決定しました。セキュリティ製品はこれらのリスクを軽減することはできますが、コストが高く、運用業務計画に悪影響を及ぼす可能性があります。

「このような保護機能がなければ、ソフトウェアを確信を持って迅速にリリースすることはできません。」

DENNIS HURST氏
Founder
Saltworks

ServiceMaster は、サイバーセキュリティにおけるデジタルトランスフォーメーションの一環として、運用方法とアプリケーション開発方法の見直しも行っています。経営効率と運用効率を高めるため、開発者チームを、オンライン予約、モバイルアプリなどの機能への取り組みや、多様なバックエンドシステムの連携に注力させました。セキュリティは開発ライフサイクルに組み込まれているため、社内常駐のセキュリティテストチームを持つ必要がありません。

同社がこれらを実現できたのは、Micro Focus Fortify on Demand および Micro Focus Application Defender の導入と使用によるものです。これらは業務のペースを落とさずにコードを保護する製品です。

ソリューション

ServiceMaster の「デジタルファースト」戦略によって、同社のビジネスが変化しています。お客様は、希望の時間、場所、方法で同社とやり取りができるようになりました。これには、新たなオンラインビジネスの手法をサポートし、効率を向上させるようにレガシーシステムをリエンジニアリン

ServiceMaster

概要

- **業界**
  生活産業
- **所在地**
  米国
- **課題**
  毎日新しいアプリケーション機能をデプロイしながら、サイバーセキュリティ侵害のリスクを軽減して企業の評判を守る。
- **製品とサービス**
  Fortify on Demand
  Application Defender
- **成果**
  + DevOps による迅速なソフトウェア開発とデプロイを実現することで、ビジネスのスピードを高めることが可能に
  + 従業員を増やさずにセキュリティを向上
  + 開発者のプログラミング技術が向上し、会社の評判に関するリスクが低減

グする大幅な変化が必要でした。たとえば、モバイルアプリは販売担当者の効率性の向上に役立ちます。改善されたバックオフィスシステムにより、プロジェクトの承認と資金供給を迅速に行うことができます。また、オンライン予約により、ServiceMasterは同社のさまざまなブランドのサービスをクロスセルできます。

「私たちは、家庭向けサービスのリーダーとして認められたいと思っています。」と話すのは、SercicеMastar の Director of Information Security、Thomas Davis 氏です。

この目標に向けて、新しいビジネスチャンスに迅速に対応できるよう、同社は DevOps 手法を取り入れ、ソフトウェアの開発とデプロイをはるかに迅速に行える方式にシフトしました。たとえば、ServiceMaster の Terminix は、新たな害虫駆除問題の対応に早急に取り組むことができます。

デジタルトランスフォーメーションの過程にある ServiceMaster には、アプリケーションがセキュリティリスクにさらされる可能性があります。専門家は、かなりの割合のビジネスソフトウェアにセキュリティ上の脆弱性があり、数週間、さらには数か月もの間、パッチが適用されていない状態であると推定しています。また、ネットワークのファイアウォールと侵入検知システムは企業のネットワークの境界を防御しますが、アプリケーションに脆弱性がある場合にはセキュリティ防御が不足する可能性があります。SQL インジェクションなどのサイバー攻撃テクニックが標的にするのは、このようなセキュリティの盲点です。

脆弱性をリアルタイムに特定して修正できるように、ServiceMaster の IT プロジェクトチームは「ウォーターフォール」アプローチ (プログラミングでコードを作成してからテストするまでに長時間かかる) からアジャイルおよび DevOps へと移行しました。この移行により、チームは段階的にソフトウェアを開発し、毎日リリースを行う短期間の開発「スプリント」を実施することになります。DevOps アプローチでは、リリース前の開発ライフサイクルで、欠陥、バグ、および脆弱性が検証されるため、リスクを最小限にすることができます。プロセスの有効化、コードの検証、本番環境へのリリースにおいて、自動化が重要な役割を果たします。

成果

迅速な脆弱性の発見

ServiceMaster は、アプリケーションのセキュリティへの包括的な取り組みを行い、企業のソフトウェア開発ライフサイクル (SDLC) に必ずセキュリティ対策を組み込むようにしました。開発者がより安全なアプリケーションを構築できるように、開発者を正しくトレーニングすること、そして開発者に適切なアーキテクチャ標準とテクノロジーを提供することに注意が払われています。こうした取り組みには、設計段階でのアプリケーションのセキュリティの分析、開発中に脆弱性を最小化するための静的コードの分析が含まれます。アプリケーションがデプロイされた後は、動的な分析、侵入テスト、およびランタイムアプリケーション自己保護 (RASP) で脆弱性の特定や脅威の防御を行い、侵害のリスクを軽減することができます。

侵入防止システム (IPS)、侵入検知システム (IDS)、およびセキュリティ情報 / イベント管理 (SIEM) などのその他のセキュリティツールと、アプリケーションのセキュリティツールを組み合わせると、リスクを軽減しやすくなります。

ServiceMaster は、コードを非常に高速にテストするオンラインサービスである Fortify on Demand を使用しているため、ServiceMaster のセキュリティチームは、他の主要なセキュリティ機能に集中して取り組むことができます。これにより、ServiceMaster は、脆弱性の数も企業の評判を損なうリスクも最小限に抑えながら、365 日 24 時間テストを実行し、DevOps に必要なテストニーズに対応できるようになりました。

成功の理由は、テスト期間の短さでした。ServiceMaster の開発者は 1 日の終わりにコードをアップロードし、脆弱性の詳細情報と修正方法が記載されたレポートを翌日受け取ることができます。

テスト結果は、開発者がコードを記述した直後に届くため、早い段階で容易に脆弱性の対応と修正を行えます。これにより、事業計画の実行に向けて、より迅速な行動を取ることができるようになります。

Micro Focus とそのパートナ企業である Saltworks Security は、ServiceMaster と密接に連携して、アプリケーションのセキュリティプロセスによる開発者への影響を最小限に留めています。Saltworks Security の創設者、Dennis Hurst 氏と Micro Focus の代表は ServiceMaster で行われる開発者の定期ミーティングに参加し、すべての工程が順調に進んでいることを確認します。また Saltworks は、セキュリティのスクラムマスターとしての役割を果たす常勤の人材を提供することで、SDLC を通してアプリケーションのセキュリティ要件が満たされるようにし、再構築と運用の遅延を最小限に抑えています。

「私たちが求めていたのは、ボルトオンソリューションではなく、プログラムでした。」と Davis 氏は言います。「世界にはあらゆるツールがありますが、それ自体が価値を生むわけではありません。必要なのは、そこからビジネス価値を引き出すことです。」

リスクの軽減

開発ライフサイクル中の他のポイントでテストすることにより、セキュリティリスクを事前に特定できます。Fortify on Demand では、開発中に静的コードをテストし、デプロイ後はライブ Web やモバイルアプリケーションを動的にテストします。この継続的なテストとフィードバックにより運用が効率化され、開発者は以前よりもっと速いスピードで対応できるようになります。

お問い合わせ先:
www.microfocus.com

開発者は、テスト結果からも、より安全なコードを記述する方法を学習します。特定される脆弱性が少なくなれば、それだけServiceMasterの評判の保護が強化されます。

ServiceMasterの開発者は、このセキュリティに特化した考え方を取り入れています。ServiceMasterは、Fortify on Demandの重要性メトリクスをゲームのように利用し、開発者は5つ星の評価を得ようと競い合っています。「それが開発者に受けました。開発者は今では「どうやったら5つ星を取れるだろう」と話しています。開発者は、コードと問題を完全に自分のものとしてとらえています。」とDavis氏は述べています。.

アプリケーション内からの保護

ServiceMasterは、プログラミング段階で脆弱性を削減する以外にも、もう1つの重要な対策を取っています。つまりセキュリティオペレーションセンター(SOC)を可視化することで、アプリケーションを標的とする攻撃の可能性を認識し、アプリケーション自体が攻撃をブロックできるようにしています。

Application Defenderを使用すると、開発者はアプリケーションのランタイム環境にセキュリティの計測ツールを簡単に追加できます。つまりServiceMasterの防御では、デプロイ前にソフトウェアのすべての脆弱性を排除する必要がありません。本番環境に脆弱性が存在しても、Application Defenderが脆弱性の悪用の可能性を検出し、SOCに警告するため、SOCは悪用の試みをブロックすることができます。

ServiceMasterの開発者は、Application Defenderが全面的にデプロイされていない場合でも、セキュリティ対策を数秒でランタイム環境に追加できることを認識しつつあります。

「このような保護機能がなければ、ソフトウェアを自信を持って迅速にリリースすることはできません。」とSaltworkのHurst氏は話します。

この信頼性と高度な可視性により、ServiceMasterはコードを再デプロイして時間を節約できます。「これにより、多種多様な方法でWebサービスを利用できるようになります。」とHurst氏は言います。「このサービスには脆弱性がなく、攻撃に対して強靭です。そうでなければ、余計な懸念、コスト、ストレス、時間が増えることになります。」

ビジネスを再活性化する

ServiceMasterの開発者がすばやく行動できるようになったことで、同社のデジタルトランスフォーメーションは加速しています。ServiceMasterのデジタルトランスフォーメーションを率いているのは、American Home Shieldです。American Home Shieldのeコマースチャネルでの売上は、2015年におよそ45%アップし、セールスリードの数も増加しました。新しいリードを創出し、お客様からの信頼を高める主要な要因は、デジタルエンゲージメントでした。
ServiceMasterの新しい開発およびデプロイ方法は、同社のIT採用戦略においても大きな役割を果たすようになりつつあります。ServiceMasterは、同社が活力に満ちた職場であることを宣伝するビデオをリリースしました。.

Davis氏は、セキュリティ製品を提供するだけでなく、作業の迅速化をサポートする点において、Micro Focusの功績を認めています。「良いパートナーシップを築けたと思っています…」とDavis氏は話します。

結果として、開発者はServiceMasterのブランド価値を守ることができます。「私たちは、私たちのブランドを価値あるものにしたいと考えています。強力なブランドを確立したいのです。強靭でなければ、デジタルファースト戦略は取れないのです。」

詳細情報はこちら:
www.microfocus.com/appsecurity

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