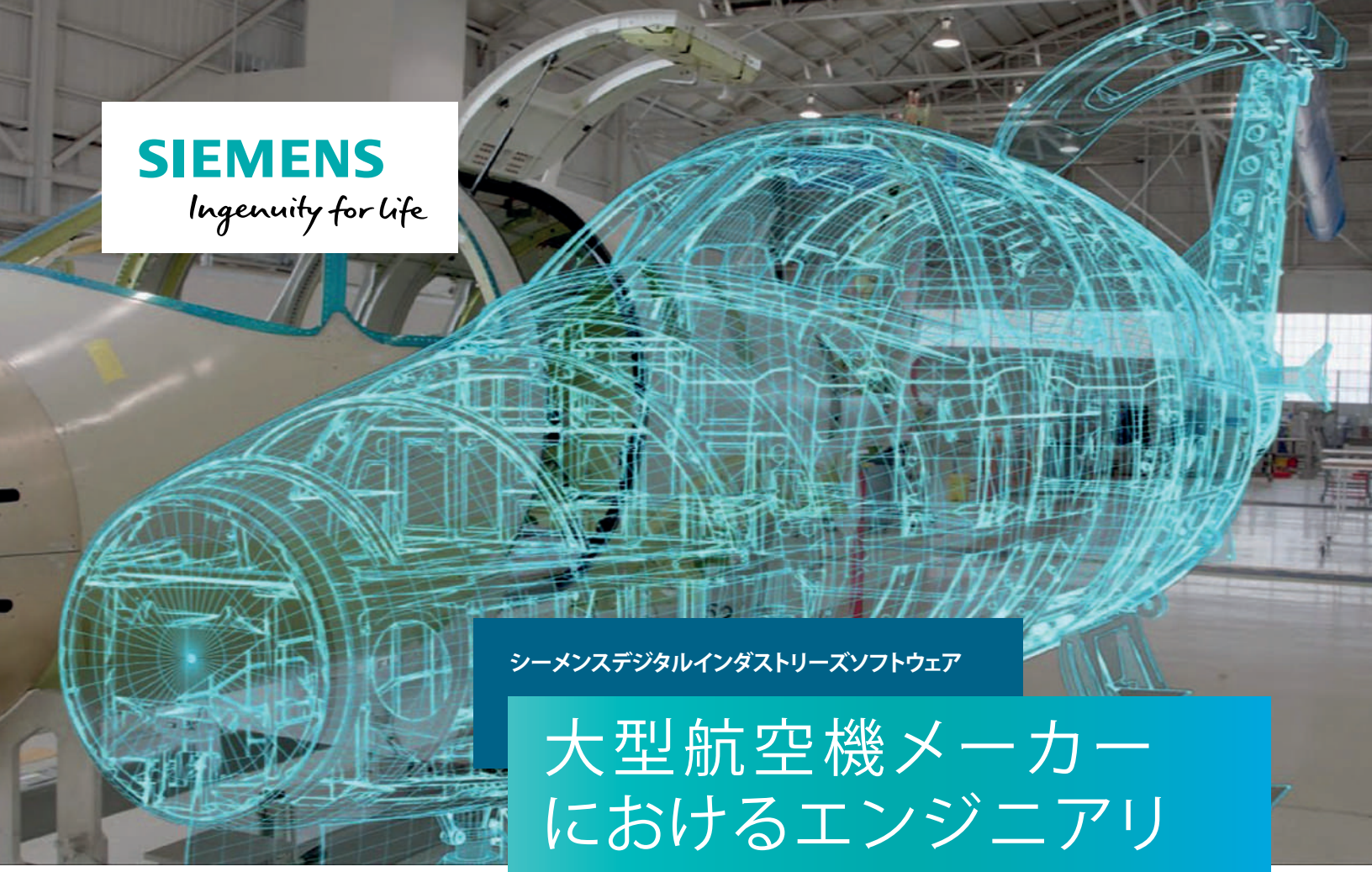

SIEMENS
Ingenuity for life

シーメンスデジタルインダストリーズソフトウェア

大型航空機メーカーにおけるエンジニアリング・ソフトウェアのセキュリティー

エグゼクティブ・サマリー

世界中の企業が、サイバー犯罪、サイバースパイ行為、サイバーテロの絶え間ない増加に悩まされています。セキュリティー・システムへの侵害は、企業の信用を著しく損なうだけでなく、顧客のプライバシー、安全、安心も脅かします。報告される事例は、毎日発生する攻撃のごく一部にすぎません。Online Trust Allianceの集計によると、2016年だけでも、82,000件のサイバー「インシデント」が発生しています (Online Trust Alliance、2017年)。ただし、報告されないサイバー攻撃もあるため、実際のインシデントの数は250,000件を超えると推定されています (Online Trust Alliance、2017年)。サイバー犯罪の発生は年々増加しており、攻撃の範囲と被害も広がっています。

シーメンスデジタルインダストリーズソフトウェア
テクニカル・ディレクター
Artem Kornilov

サイバー犯罪: 標的と影響

図1: サイバーセキュリティー侵害を受けたとして大きな注目を集めたF-35戦闘機

政府と取引関係にある民間企業や政府機関は、所有している情報の重要性から、サイバー攻撃の標的にされやすいといえます。一例を挙げると、2016年11月にF-35統合打撃戦闘機、P-8ポセイドン哨戒機、C-130ハーキュリーズ輸送機、統合直接攻撃弾 (JDAM)、およびオーストラリア海軍の次期戦闘機に関する情報がオーストラリア国防軍から流出した事件が印象的です (図1、Ars Technica、2017)。

サイバー犯罪者が企業を攻撃するときの動機はさまざまです。知的財産を盗む目的で、機密情報にアクセスすることもあれば、新製品やプロジェクトの設計プロセスを中断あるいは遅延させることが目的の場合もあります。設計の重要な領域を改ざんすることにより、製品の機能自体を損なうことを目的として攻撃する場合もあり得ます。例えば、設計中に特定のワイヤーの周囲の絶縁材料を変更することにより、第三者が電磁放射を介して最終製品の動作を簡単に傍受できたり、設計データが完全に破壊され、数か月または数年の設計作業を台無しにしたりする可能性もあります。

サイバーセキュリティー侵害の頻度の増加と深刻化に、世界の大企業が警戒感を強めており、サプライチェーン全体の情報保護に向け、より大がかりな対策を講じています。

このホワイトペーパーでは、シーメンスデジタルインダストリーズソフトウェアのようなベンダーが、新しいより厳格なセキュリティー要求にどのように応えているのかをご紹介します。

エンタープライズ・ソフトウェア・ソリューションのセキュリティー保護

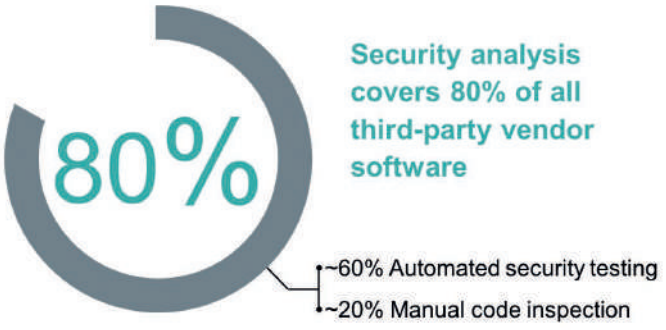

図2: 企業は、ベンダーのソフトウェアを保護する均一な手順を確立しようと模索している

サイバーセキュリティー侵害を防ぐことは、企業の信用の向上や事業の繁栄と成長を実現させるために不可欠です。セキュリティー侵害は、企業に多大な金銭的損失をもたらし、機密情報の漏えいにつながる可能性があるため、何も対策を取らないことで払う代償はあまりに高額なものになります。 そのため、世界中のメーカーが、多面的で安全なソフトウェア開発プログラムを考案して実装し、使用するすべてのソフトウェアのサイバーセキュリティーを強化しています。

こうしたプログラムは、テストおよびセキュリティー開発の実施を通じて、第３者のソフトウェアのセキュリティー上の脆弱性によってもたらされるリスクとコストの低減に重点を置いています。セキュリティーの専門家チームは、頻繁にソフトウェアのサプライヤーと直接協力し、ソフトウェア・セキュリティーを開発プロセスに統合することによる利点の実現に向けたサポートを行います。ソフトウェア・ベンダーとの協力は、メーカーのシステムを強化するための基本的な要素です。

セキュリティー対策は、社内のソフトウェア・ソリューションとネットワークから始まります。一方、セキュリティーを強化すると、それに応じてハッキング技術も進化することは明らかです。自社のネットワークとソフトウェアを強化する企業が増えたことから、ハッカーの標的はサプライチェーンに移りつつあります。

大企業のサプライチェーンは第３者や提供する多くのソフトウェアを使用しているため、ハッカーの攻撃対象領域が非常に大きくなる傾向にあります。 ソフトウェア製品の開発プロセスとセキュリティー投資はベンダーによってまちまちであり、その分、ハッカーが企業のデータにアクセスできる機会も増加します。あるセキュリティー専門家が最近述べたように、「セキュリティーの保護は、サプライヤー次第なのです」。

この状況に対応するために、企業はセキュリティー・プログラムを拡張し、ソフトウェア・ベンダーと緊密に協力してソフトウェア・セキュリティーの均一な手順を確立しています(図2)。一般的な最初のステップは、ベンダーの製品に対するセキュリティー評価を調達プロセスに組み込むことです。この評価結果をまとめて、調達プロセスでどの製品を選んだかを企業の経営陣に示します。

ソフトウェアのセキュリティー評価には、独立の第三者機関による脆弱性調査も含めることができます。セキュリティー調査の結果に関する完全かつ詳細なレポートはベンダーに提供され、購入を検討しているメーカーには大まかな概要が提示されます。この方法により、ベンダーは自社の知的財産を保護しながら、ソリューションに関心のある企業に必要な情報を提供することができます。ベンダーが独自の運用手順を選択しつつ、顧客もベンダーと同程度の均一なセキュリティー評価を行えます。

ベンダーとその顧客は、クリーンなセキュリティー・レポートの記録方法を作成した後、 ベンダーのセキュアなソフトウェア開発ライフサイクル (S-SDLC) プロセス全体を共同で評価します。開発プロセスが十分な堅牢性を持ち、セキュリティー要件を満たす製品を常に提供できるということをベンダー自身が実証することもあります。そのベンダーは確実なS-SDLCを適用している信頼できるプロバイダーとみなされ、継続的な監視や継続的な評価を必要としません。

ベンダーの視点

今日の市場で最先端のエンジニアリング・ソフトウェアに必要とされる機能が、高度なセキュリティー機能です。ソフトウェア・ベンダーに、ソフトウェアのセキュリティーの体系的な検証を行うように求める企業が増えています。しかし、ベンダーが製品セキュリティーの強化に投資する際に考慮すべき重要な要素もあります。

セキュリティーは従来、ソフトウェア開発チームではなく、ITまたは専任のセキュリティー部門が担ってきた事項です。また、セキュリティーは人事上の問題でもあります。つまり、データの適切な取り扱いに関するトレーニングの計画と実施には、人事部門が関与することになります。よりセキュアなソフトウェアが求められるようになると、これまで行ったことのない共同作業が必要となり、新しいプロセスを策定する必要性が生じます。

さらに、高機能ソフトウェアのセキュリティーの強化には、包括的なアプローチが必要です。ベンダーは、データの暗号化や監査証跡などのセキュリティー機能を追加し、コードの弱点を特定して解決することでソフトウェアを強化する必要があります。ベンダーのソフトウェアに存在する第３者のコンテンツも保護しなければ、真にセキュアなソフトウェアとは言えません。コードの重要かつ詳細な分析の結果に基づく機能強化は、ソフトウェアのセキュリティーと品質の両方の向上という点で、市場での差別化要因となるのです。

つまり、製品セキュリティーへの投資に関するベンダーの決定は、ビジネスの持続的な成長に与える影響を考慮して行われます。一方、顧客は、製品のセキュリティー向上が購買の判断、あるいは宣伝などにどのように影響するかを明確かつ説得力をもって伝えることが重要となります。ベンダーが満たさなければならない業界のセキュリティー標準を確立することで、達成すべき最小限のセキュリティーをどれだけ上回っているかという視点で判断できるため、購買の判断が非常に簡単になります。製品のセキュリティー保護への投資をベンダーが決定した場合は、ビジネスへのプラスの影響を最大化するために、最も効果的かつ効率的な方法でこれを達成しようとすることが重要となります。

Capital製品群のセキュリティー保護

図3: 電装システムとワイヤーハーネスのライフサイクル全体をサポートするシーメンスのCapitalソフトウェア製品群

2011年以来、シーメンスはお客様と共にセキュリティーに取り組んできました。シーメンスデジタルインダストリーズソフトウェアのセキュリティー強化は、IT部門が中心となって進めています。シーメンスのIT部門は、セキュリティーに関する全社的な取り組みを主導し、ベンダー選定プロセスを牽引し、セキュリティーに関するトレーニングや調査ツールの予算を確保するとともに、複数部門に渡るセキュリティーの取り組みを推進しています。シーメンスはこの一環として、電装システムの設計および統合ソフトウェア製品群であるCapitalを高度なセキュリティー・プログラムに含める決定を下しました。

シーメンスのCapitalは、電気および電子アーキテクチャーの初期探索から、生産設計、製造準備および現場でのメンテナンスに至るまで、電装システムおよびワイヤーハーネスのライフサイクル全体をサポートしています(図3)。オンプレミスおよびクラウドのどちらにも導入でき、多層型でデータ中心のソリューションであるCapitalは、シッククライアントとWebベースのクライアントを備えています。Capitalは、一般的に使用されているソフトウェア・テクノロジーと設計手法を幅広くカバーしており、ソフトウェア・ソリューションを保護するアプローチの好例といえます。

セキュリティー強化の第一歩として、Capitalチームはプロセスの目標を明確に定め、シーメンス経営陣の支持を得るよう努めました。電装設計の統合型スイートであるCapitalのセキュリティーは、1つの部門で完結するものではありません。シーメンスの経営陣の理解を得るには、ITと営業が協力して連携する必要がありました。経営陣の承認を得て、Capitalソフトウェア開発部門は、Capitalで以下の3つの目標を達成するため、セキュリティー・プロジェクト・チームを編成しました。

1. 既存のセキュリティーの弱点に対処すること
2. 新しいセキュリティーの弱点の発生を防ぐこと
3. トレーニングとベストプラクティスの共有を通じて、セキュリティーの文化を確立すること

既存のセキュリティーの弱点に対処するため、Capitalソフトウェア・チームはクラウドベースのソリューションを使用して、静的アプリケーション・セキュリティー・テスト (SAST) を行いました。SAST技術が選ばれた理由は、Capitalソフトウェア・チームがS-SDLCの一部として既に使用していた動的アプリケーション・セキュリティー・テスト (DAST) を補完するコード・カバレッジが大きいためです。クラウドベースのSASTソリューションは、Capitalのコードを調査し、

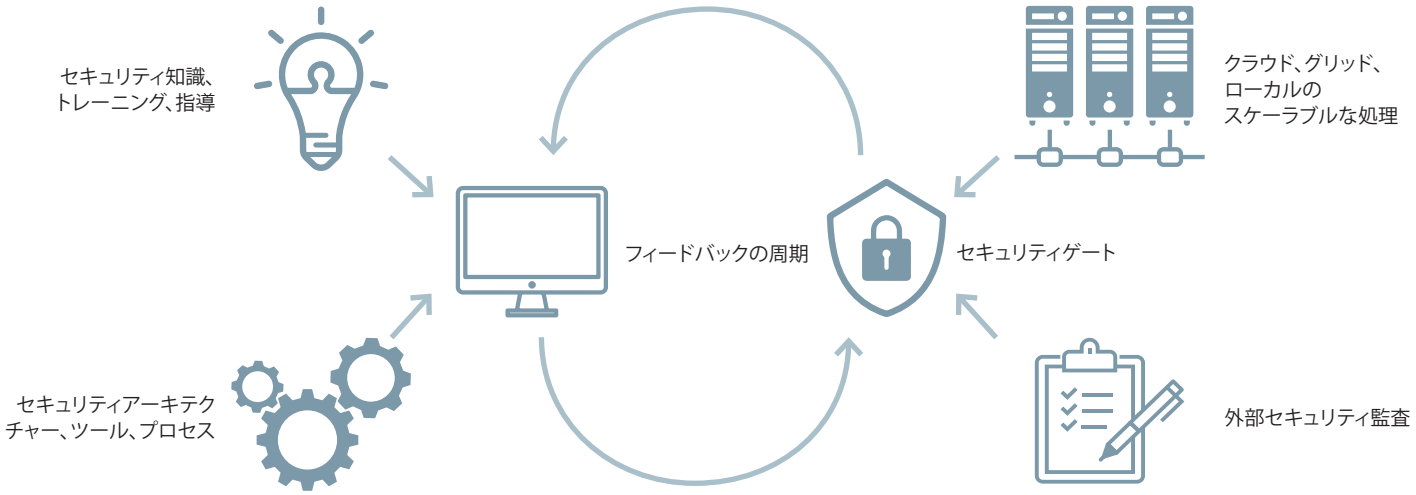

図4: フィードバック周期の短縮により、不具合のより迅速な特定と修復が可能

既存のセキュリティー上の弱点リストを作成しました。このリストを使用して、それぞれの不具合を解決するために必要な工数を試算しました。その後、弱点をグループ化して、効率的な改善が行えるよう優先順位を付けました。影響の最も大きい弱点を最初に解消することに決め、それと同時に、関連する弱点に対処しました。このプロセスにおいて、Capitalを構成する無数のコード行のすべての弱点が修正されました。

次に、チームは一般的なパターンを特定し、Capitalのコードベース、ツール、プロセスに合わせたベストプラクティスを策定しました。重要なポイントの1つは、SAST評価で検出された弱点の多くが誤検出であり、セキュリティーの弱点として特定されたものがなかったことです。クラウドベースのSASTソリューションで、これらの誤検出の多くは除外されますが、それであってもシーメンスデジタルインダストリーズソフトウェアのエンジニアが対処しなければならないものも少なくありません。そのため、誤検出を特定し、正しく除外するための一連のベストプラクティスが作成されました。これには、特定された誤検出の真正性を判断するためのレビューおよび承認プロセスが含まれます。これらのベストプラクティスは、最初に部門エンジニアリング・ブログで公開され、その後、定期的なエンジニアリング・チーム会議で議論されました。

クラウドベースのソリューションは、ツールが新しいタイプのセキュリティーの弱点を特定できるよう定期的に更新され、さらに役立つようになっていました。その結果、Capitalチームは、以前はクリーンであると判断されていたコードを再調査し、新しいセキュリティーの弱点を見つけ、解決することができました。ただし、これらの定期的な更新の利点を完全に実現するには、既に調査されたコードであってもセキュリティーの弱点を見つけて対処するための堅牢な調査プロセスと継続的な投資が必要でした。

弱点の修正は、コードの変更を継続的に配信し、SAST調査を再度行うことで追跡されました。Capitalチームは、SAST調査用のコードのパッケージ化や、統一されたコード・メトリクス・プラットフォームへの調査結果の読み込みなどのタスクを実行する自動スクリプトを開発しました。 より大規模なシーメンスのセキュリティー・イニシアチブの一環として、シーメンスデジタルインダストリーズソフトウェアでは、 コードのアーキテクチャーと設計を進化させることにより、 セキュアなソフトウェアの開発を容易にすることに重点を置いています。これは、アプリケーションの攻撃対象領域を日常的に最小化および保護し、セキュリティー・リスクを予防的に管理することで実現されます。

SAST技術が複雑で、かつCapitalソリューションのコードベースのサイズが大きいため、各調査にかなりの時間を要し、結果としてソフトウェア・エンジニアのフィードバックの周期が比較的長くなっていました。これを軽減するために、 Capitalチームは、SAST調査のカバレッジを狭める代わりに、フィードバック周期を短くする補完的なツールを採用しました (図4)。ソフトウェア・エンジニアが使用する統合開発環境のバックグラウンドで継続的に 実行されるセキュリティー重視の静的コード分析により、最短のフィードバック周期が実現しました。これには、JetBrains™ IntelliJ コード検査静的コード分析エンジンと、オープンソースの

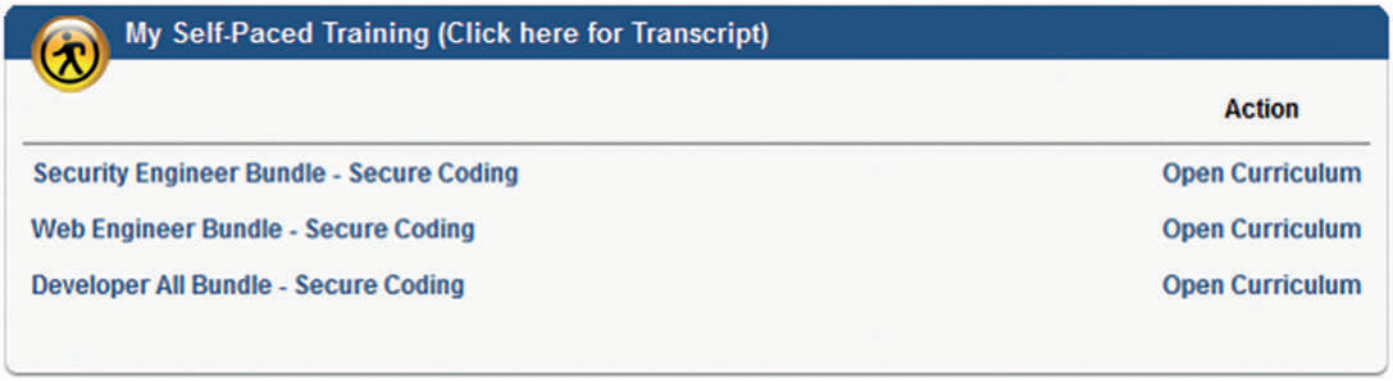

図5: セキュリティの知識を深めるコンピューターベースのトレーニング

Find Security Bugs SASTソリューションの組み合わせを選択しました。

これらのツールは、フィードバック周期の短縮に加えて、セキュリティーを自動品質ゲートに統合し、ユニット・テストの完了とカバレッジ、コードの重複をチェックすることで、コードとテストの配信を管理します。コード配信は、エンジニアとチームの間、およびチームとリリースの間でゲートされます。結果として、ソフトウェア開発のプロセスにセキュリティーが組み込まれ、個々のソフトウェア・エンジニアがさらなる労力を費やすことなく保護を強化し、セキュリティーの2番目の目標を実現しました。

セキュリティーの文化を確立するという3番目の目標に対して、CapitalチームはIT部門およびHR部門と協力して、ソフトウェア・エンジニアおよび品質保証エンジニア向けのコンピューターベースのセキュリティー・トレーニングを準備しました。トレーニング・プロバイダーとしてSecurity Innovations™ を選びました。Capitalソリューションのテクノロジー・スタックと多様なチームそれぞれのニーズに最も合うようにカリキュラムを組み立てました。トレーニングの早期受講を部門単位で働きかけ、トレーニング完了期限を定めて、進捗を追跡します。セキュリティー・トレーニングは、新人研修にも組み入れられました。

Capitalチームは、セキュリティー・トレーニングに3つの主要なアプローチを採用しました。1つ目は、セキュリティー・テストを目的とした、インストラクターによる品質保証のトレーニングです。これらのセッションでは、セキュリティーを重視するお客様とのエンゲージメントを2011年に開始して以来、Capital開発チームが適用してきた技術の強化と改良に焦点を当てました。例えば、シーメンスデジタルインダストリーズソフトウェアは、ハッカーのように攻撃して結果を観察することでアプリケーションを評価するDASTを使用しています。 2つ目は、セキュアなソフトウェア開発に関するコンピューターベースのトレーニングです。これは、第３者のプロバイダーであるSecurity Innovations を通じて実施します。このトレーニングは、開発者用、Webエンジニア用、セキュリティー・エンジニア用の3つのコースで構成されています。各コースは、各ジョブに固有であるセキュリティー上の問題のみを対象としました (図5)。例えば、開発者向けコースには、「セキュアなJavaコード基盤の作成」、「セキュアなJavaコードの作成」、「Open Web Application Security Projectのトップ10の脅威と緩和策」などのトピックがあります。3つ目は、シーメンスのソフトウェア全体で共有されるベストプラクティスをまとめてリスト化する作業です。このリストは、シーメンスデジタルインダストリーズソフトウェアでセキュリティーの中心的な役割を果たしているIT組織より共有されます。

オープンソースのセキュリティーへの対処

設計ツール・ベンダーにとってのもう1つの大きな懸念が、第３者の開発者によるオープンソース・ソフトウェア (OSS) の使用です。OSSは、Capitalを含む多くの強力なソフトウェア・ソリューションで広く採用されています。 実際にOSS は、開発時間を数か月または数日間短縮することができる、企業にとっては価値のあるツールですが、他の安全なソフトウェア・ソリューションに不具合を起こす恐れがあります。 OSSをソフトウェア・ソリューションに使用することを検討する際に、OSSの安全性を確保するのはベンダーの責任です。

ベンダー製品にオープンソース・ソフトウェアを組み込んで出荷する前に、SAST調査で個別に分析し、使用するコードのコンテキストで分析する必要があります。問題が見つかった場合、問題を解決するか、OSS開発者に問題を解決するよう働きかけることが重要です。このプロセスでは、公開されているセキュリティー脆弱性データベースも重要なリソースです。これらのデータベースは、ソフトウェアの既知の脆弱性を追跡し、検索可能な形式で公開するものであり、代表的なものとしてはNational Vulnerability Database (NVD) があります (National Institute of Standards and Technology、2018)。

ただし、OSSのセキュリティーに細心の注意を払うだけでは不十分です。OSSの用途を減らすことはできないか、慎重に検討する必要があります。ソフトウェア開発チームは、OSSの使用状況を確認して、その機能をアップグレード、削除、または置換できるかどうかを判断する必要があります。OSSのセキュリティー上の弱点の軽減は、ベンダーのコードでOSSが実行する機能を置き換えるかラップする回避策を実行するか、検出された問題を解決するようOSS開発者に働きかけるか、セキュリティの高い別のソリューションに切り替えることで達成できます。OSSの使用に関するセキュリティーのベストプラクティスのリストも作成して共有するのも良いでしょう。 OSSの使用の最終的な承認には、セキュリティーへの影響のレビューを含める必要があります。

主な教訓と達成内容

セキュリティーのベストプラクティスを体系的にトレーニング、開発、共有することにより、シーメンスデジタルインダストリーズソフトウェアは、セキュアなソフトウェア製品の開発プロセスを体系化することができました。このプロセスは開発ライフサイクルに深く根付き、安全なベストプラクティスの持続につながっています。

また、セキュリティー重視のお客様との長期にわたる関係を通じ、優れたセキュリティー標準を達成しました。こうしたお客様のS-SDLC開発へのコミットメントが、より高いセキュリティーにシーメンスが投資することの価値を表しています。シーメンスデジタルインダストリーズソフトウェアは、セキュリティーを確保するプラクティスを強化することでより多くの利点を実現してきました。またセキュリティーに対する取り組みで学んだベストプラクティスに基づいて、製品開発インフラストラクチャーを改善し、生産性を向上させています。統合型電装設計ソリューションCapitalは、セキュリティーと品質の両面でコードを強化することで、より競争力の高い製品に進化してきました。最後に、セキュリティーのトレーニングによって社員が重要かつ市場性のあるスキルを習得する時間を設けることにより、社員の満足度を向上させました。

安全なソフトウェア開発プロセスを確立する道のりのなかで、次に示す複数の重要なステップを経ていくつもの成果を達成しました。まず、シーメンスデジタルインダストリーズソフトウェアはセキュリティー調査とトレーニングを体系的に採用して、Capitalの弱点を特定して修正し、OWASP (Open Web Application Security Peoject)、およびそ の他の規格に至るまでの一貫した明確な概要レポートにつ なげました (OWASP, 2018)。複数の異なったセキュリティー用調査 ツールを使用することにより、フィードバック周期の短 縮を達成でき、脆弱性を迅速に特定して解決することも可能となりました。これが、シーメンスのS-SDLCを実装するための鍵となりました。次にシーメンスは、企業全体の セキュリティー向上に関する知識やスキルを共有する仕組みを確立しました。

企業の未来を守る

今日の企業は、現代社会に無数に存在するサイバーセキュリティーの脅威に対する堅牢で包括的、かつ強力な保護手段の開発に投資しています。これは、大企業だけでなく、そのサプライチェーンもサイバー攻撃の標的になりつつあることを警戒しています。企業にとって、安全なソフトウェア開発プログラムには2つの重要な要素があります。まず、会社全体で体制を整備することです。すべての部門においてソフトウェアのセキュリティーを確保する均一なプロセスが、企業全 体のセキュリティーにとって重要です。第2に、ベンダーと企 業管理者の両方がセキュリティー・プログラムに対して一 貫して関与し続けることです。これによって、すべてのベンダーが一様に基準を満たすので、それらを等しく扱うことができます。

シーメンスのCapitalチームは、ソフトウェアのセキュリティー強化の過程で、 最新の規格に合わせて、応答性と安全な製品とプロセスの配信についてのベンチマークを設定しました。その際、Capitalチームは、Capitalのような大規模で強力なソフトウェア・ソリューションでも、その複雑さにもかかわらず厳しいセキュリティー要件に適合できることを実証しました。

一方、製品セキュリティーについてソフトウェア・ベンダーが単独で責任を負うことはありません。顧客自身の購買決定とRFIとRFPに含まれる情報も、製品のセキュリティー確保に大きな影響を及ぼします。顧客は、堅牢なS-SDLCプロセスを実装し、セキュアな開発文化が確立されたベンダーを探すことを求められます。そのために、RFIとRFPのなかで強調しておくべきことがあります。それは、ベンダーが自社製品に含まれる第 3 者のコンテンツのセキュリティーに責任を持つこと、DASTおよびSASTセキュリティー・テストを実行すること、クリーンなセキュリティー・レポートを定期的に作成しなければならないということです。顧客とベンダーの双方にとって、ソフトウェアのセキュリティーを重視するということが、製品とプロセスのより効果的な保護につながるのです。

参考文献

1. Gallagher, S. (2017年10月13日)。オーストラリアの防衛企業がハッキングされ、F-35のデータが盗まれたことをDODが確認。Ars Technica。https://arstechnica.com/information-technology/2017/10/australian-defense-firm-was-hacked-and-f-35-data-stolen-dod-confirms/より引用。
2. 国立標準技術研究所 (2018)。全国の脆弱性情報データベース。https://nvd.nist.gov/から引用。
3. Online Trust Alliance (2017年1月25日)。消費者データの侵害は横ばいとなるも、他のインシデントは急増。Online Trust Alliance。https://otalliance.org/news-events/press-releases/consumer-data-breaches-level-while-other-incidents-skyrocketから引用。
4. Open Web Application Security Project (2018)。OWASPへようこそ。Open Web Application Security Project。https://www.owasp.org/index.php/Main_Pageから引用。

シーメンスデジタルインダストリーズソフトウェア

本社
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

アメリカ
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

ヨーロッパ
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

アジア／太平洋
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

日本
〒151-8583 東京都渋谷区代々木 2-2-1
小田急サザンタワー
TEL: 03-5354-6700 (代)

シーメンスデジタルインダストリーズソフトウェアについて

シーメンスデジタルインダストリーズソフトウェアは、シーメンスのデジタルインダストリーズのビジネス・ユニットです。製造業がイノベーションを実現するための新たな機会を創出し、産業のデジタル・トランスフォーメーションを牽引するソフトウェア・ソリューションの提供において、世界をリードするグローバル・プロバイダーです。米国テキサス州プラノを本拠地とし、これまで世界140,000社以上のお客様にサービスを提供しています。シーメンスデジタルインダストリーズソフトウェアは、あらゆる規模のお客様と協働して、アイデアの実現方法、製品の実現方法、稼働中の製品および設備資産の活用や状況把握の方法を変革できるよう支援しています。
シーメンスの製品およびサービスについての詳細は、siemens.com/plmをご覧ください。

siemens.com/plm

77783-81721-C4-JA 3/20 LOC