テクニカルレビュー

HCL AppScanを使用した継続的アプリケーションセキュリティ

日付：2020年8月 **筆者：**Jack Poller シニアアナリスト

要約

本ESGテクニカルレビューは、セキュリティの専門家によって定義されたポリシーを使用してアプリケーションの安全性を継続的に確保するために、HCL AppScanがどのように開発者を補助するかについてのESGの評価と分析を文書化したものです。また、AppScanがCI/CDパイプラインに容易に統合され、スケールで継続的なアプリケーションセキュリティを提供するためのDevSecOpsイニシアチブにおける他の側面をサポートする方法も評価しています。

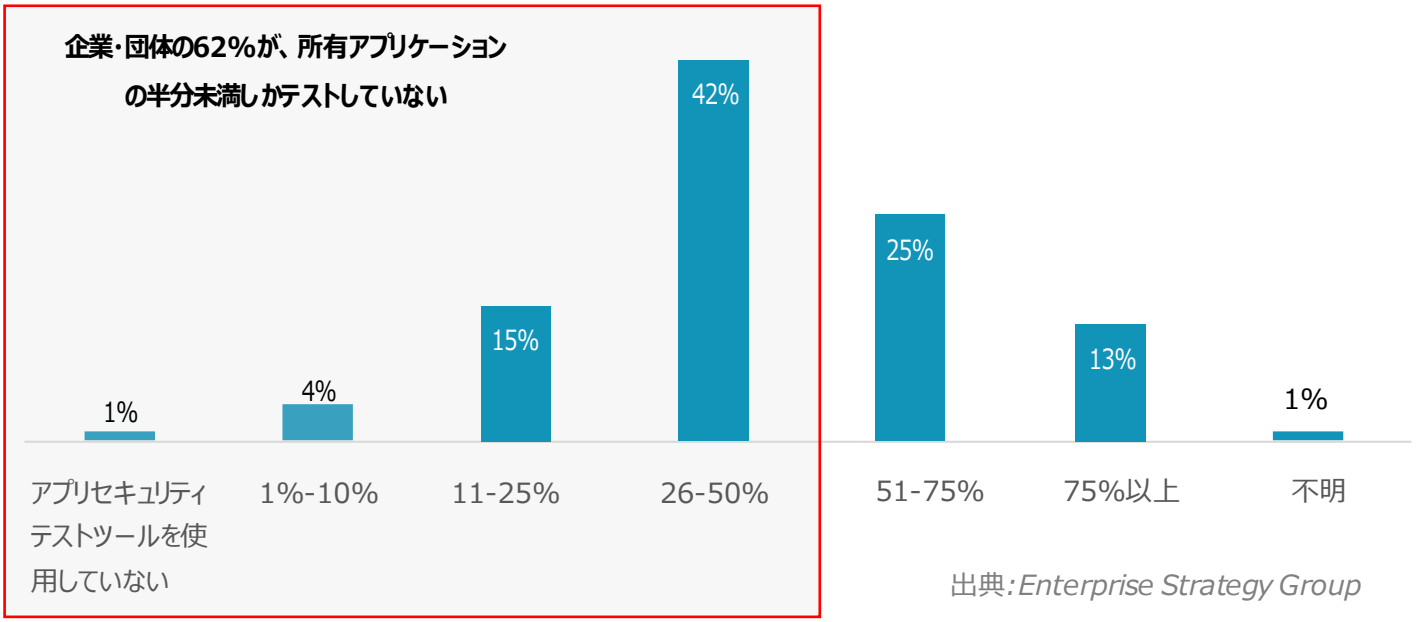
課題

ESGの調査によると、ITはまだ手軽になったとは言えません。全体の3分の2(64%)近い組織が、2年前と比較してITがより複雑になっていると回答しています。これは、データ量の増加、新しいセキュリティとプライバシーの規制、最新のアーキテクチャを活用するアプリケーションの増加によって引き起こされています。また、それと同時に、悪意をもった者の攻撃がより洗練され、標的を絞った攻撃の開発に力を注いでいるため、脅威の状況はますます危険なものになっています[1]。

組織がサイバーセキュリティの脅威に警戒を示すようになり、一般的なセキュリティにおけるベストプラクティスがAppDevコミュニティー内で十分に理解されると同時に文書化されるようになると、組織はサイバーセキュリティの原則やツールをDevOpsパイプラインや手法に組み込むようになってきています。アプリケーションセキュリティ（AppSec）ツールの使用率は過去5年間で着実に増加していますが、62%の組織では、いまだに半分以下のアプリにしか活用されていません（図1を参照）[2]。

図1.アプリケーションセキュリティテストツールの使用

社内開発あるいはサードパーティー製かを問わず、組織におけるすべてのアプリケーションについて考えた場合、動的アプリケーション セキュリティ テスト、静的アプリケーション セキュリティ テストなど、何らかのアプリケーション セキュリティ テストツールによって保護されているおよその割合をご回答ください。(回答者の割合、N=220)



出典:*Enterprise Strategy Group*

ソリューション：AppScan

HCLは、開発者が開発ライフサイクルのあらゆる段階でアプリケーションの脆弱性を迅速に特定し、修復できるようにすることで、組織的なリスクを軽減することを目的にAppScanを設計しました。AppScanは、オンプレミスまたはクラウド上のSaaSとして展開でき、静的テスト（SAST）、動的テスト（DAST）、インタラクティブテスト（IAST）、およびオープンソーステストを含む一連のテスト技術を提供し、スタンドアロン、Web、モバイルアプリケーションのセキュリティを向上させます。

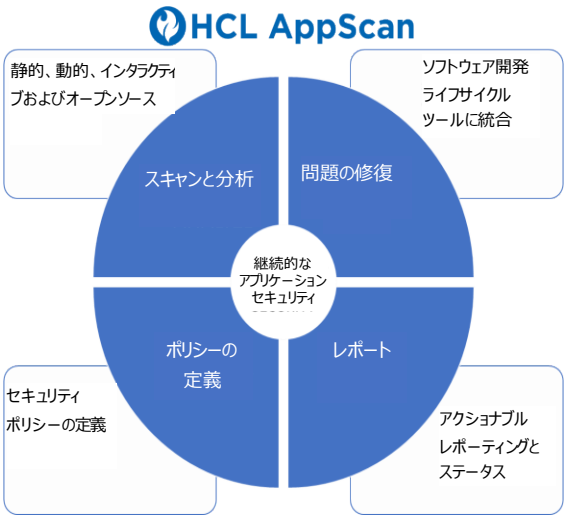
AppScanは、自動化されたビルドや展開パイプライン中のインライン実行、統合開発環境（IDE）内でのフィードバックや修復など、ソフトウェア開発ライフサイクルに直接統合することでDevSecOpsをサポートしています。このソリューションには、規制、コンプライアンス、およびセキュリティの専門家らがアプリケーションのセキュリティ体制やコンプライアンスを継続的に監視および維持するための管理機能も含まれています。

AppScanをDevSecOpsモデルに組み込むメリットとしては、以下のようなものがあります。

- **アクショナブルレポーティング** - 特定された脆弱性には、修正の推奨事項が含まれており、アプリケーションの安全性を確保するための開発者の労力を簡略化します。
- **ノイズの低減** - 機械学習分析は、精度を向上させ、誤検出を減らし、脆弱性と修正に優先順位を付けてROIの最大化をサポートします。
- **現在の脆弱性の知識** - 継続的なアップデートにより、AppScanは最新の攻撃に関連する脆弱性を確実に特定できます。
- **ガバナンスの向上** - 定義済みのセキュリティテストポリシーは、PCI DSS、HIPAA、GDPRに加え、業界標準やベンチマークであるOWASP Top10、SANS25などの規制へのコンプライアンスを達成するのに役立ちます。
- **オープンソースリスクの低減** - アプリケーションに統合されたオープンソースコンポーネントに関連するリスクを特定し、管理します。

AppScanは以下の4つのDevSecOpsの主要な側面に統合されています。

- **ポリシーの定義**—セキュリティと規制の専門家らが、ポリシーを定義し、アプリケーションに関連付けることができます。
- **スキャンと分析**—開発者は静的分析を使って「セキュリティをシフト・レフト」し、CI/CDパイプラインの早期段階でコードの脆弱性を特定します。動的およびインタラクティブ テストも同様に、実行中のアプリケーションの脆弱性を特定するのに役立ちます。
- **脆弱性の修復**—開発者は、脆弱性のレビューと修正を行います。AppScanの機械学習は、関連する脆弱性をグループ化して優先順位を付け、ソースコード内の潜在的に修正が必要な箇所および修正箇所を特定することで、修復速度を向上させます。
- **レポート**—セキュリティおよび規制の専門家らと組織管理者は、アプリケーションのセキュリティとコンプライアンス状況を継続的に監視できます。



ESGによる検証

ESGの評価は、セキュリティ ポリシーをアプリケーションに定義および関連付けることから始まり、最新DevSecOps CI/CDパイプラインにおける、上記4つの側面からなるAppScanの活動を通して進められました。まず、ESGでは、クラウドのユーザーインターフェース上にあるAppScanを利用したセキュリティテスト用のアプリケーションを定義しました。アプリケーション定義プロセスでは、ESGはアプリケーションを資産グループに割り当て、アクセス制御の手段を提供しています。また、ESGはビジネスへの影響を定義し、クリティカル、高、中、低のカテゴリーから選択しています。AppScanはこの情報を使用して、セキュリティ担当者が脆弱性を深く理解し、優先順位を付けられるようにします。

高度なオプション部分により、ESGは、ビジネスユニット、アプリのURL、説明、技術に加え、テスター、ビジネスオーナー、開発者などの関係者や管理者のためにより多くの情報を提供できるようになりました。

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

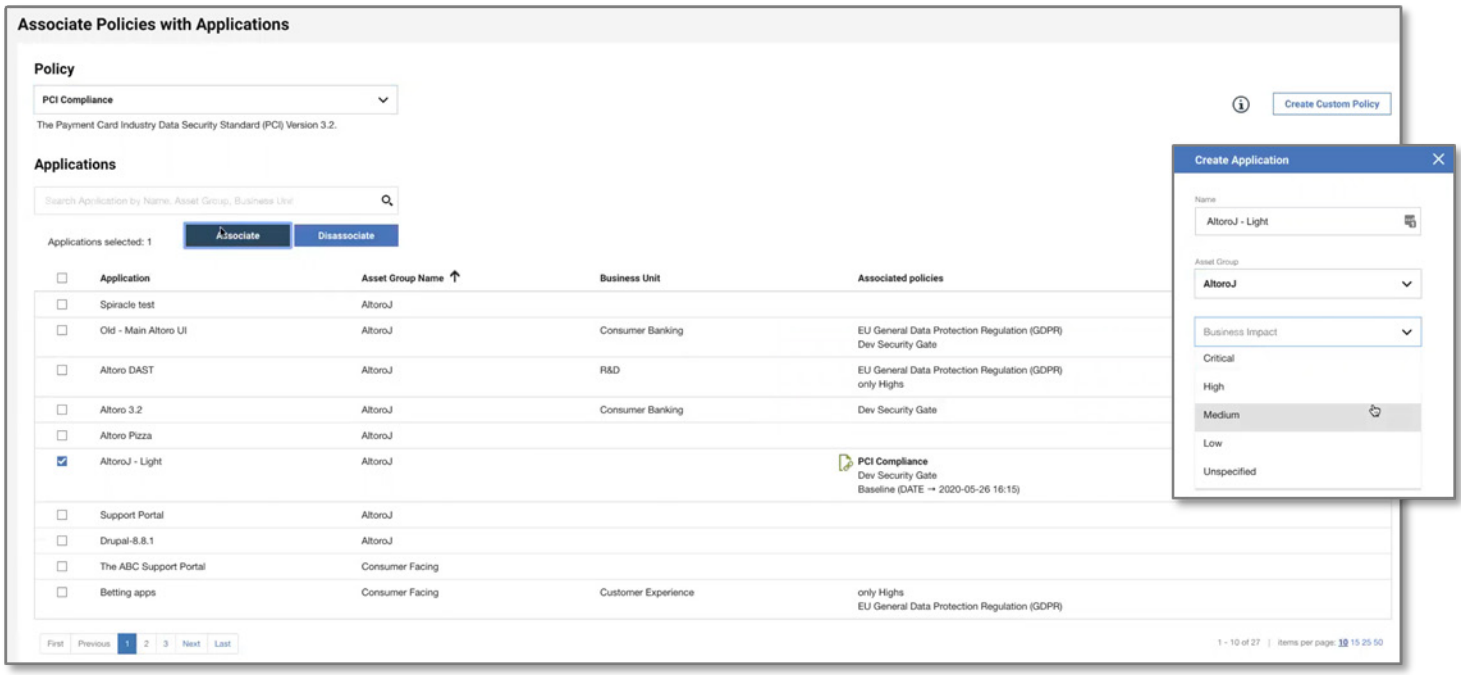
次に、図2に示すように、ESGはアプリケーションにセキュリティポリシーを関連付けました。AppScanのセキュリティポリシーは、開発者が注意すべきセキュリティ問題を指定する方法で、ポリシーには規定の定義や潜在的な脆弱性が記載されています。AppScanには、HIPAA、PCI DSS、GDPRなどの業界標準のベンチマークや規制のための多数の事前定義済みポリシーが含まれており、ユーザーは独自のポリシーを定義できます。

HCLは、アプリケーションセキュリティの現在の状態を特定し、ベースラインを作成するために、適用可能なすべてのポリシーに適用する手動スキャンから始めることを推奨しています。ベースラインスキャンにより、組織はスキャンした日付以降に新たに導入された脆弱性を特定し管理できます。

セキュリティの専門家（または開発者）は、セキュリティの専門知識とアプリケーションのビジネスへの影響の理解と共に、どのようなセキュリティにおける脆弱性が懸念されるかを定義します。例えば、企業内の人事アプリケーションであれば、サービス拒否攻撃される脆弱性の心配は必要はないかもしれませんが、SQLインジェクションやGDPRの脆弱性をテストする必要があるかもしれません。

ポリシーは、開発者とセキュリティ専門家における役割と責任を切り離し、コラボレーションと効率性を高めるのに役立ちます。開発者はアプリケーションの開発と脆弱性の修復に集中できる一方で、セキュリティ専門家は脆弱性を評価し、予め修正すべき最も重要なものを決定する責任を保持します。

図2セキュリティポリシーのアプリケーションへの関連付け



出典：*Enterprise Strategy Group*

次に、ESGは、AppScanをDevSecOpsツールチェーンに統合することで、スキャンと分析の側面を評価しました。ESGではAppScanのJenkinsオートメーション サーバー プラグインを使用しました。図3に示すように、ESGはクレデンシャルとアプリケーションの両方を指定しました。ESGはテストの名前を決定し、静的テストと動的テストの間で選択しました。

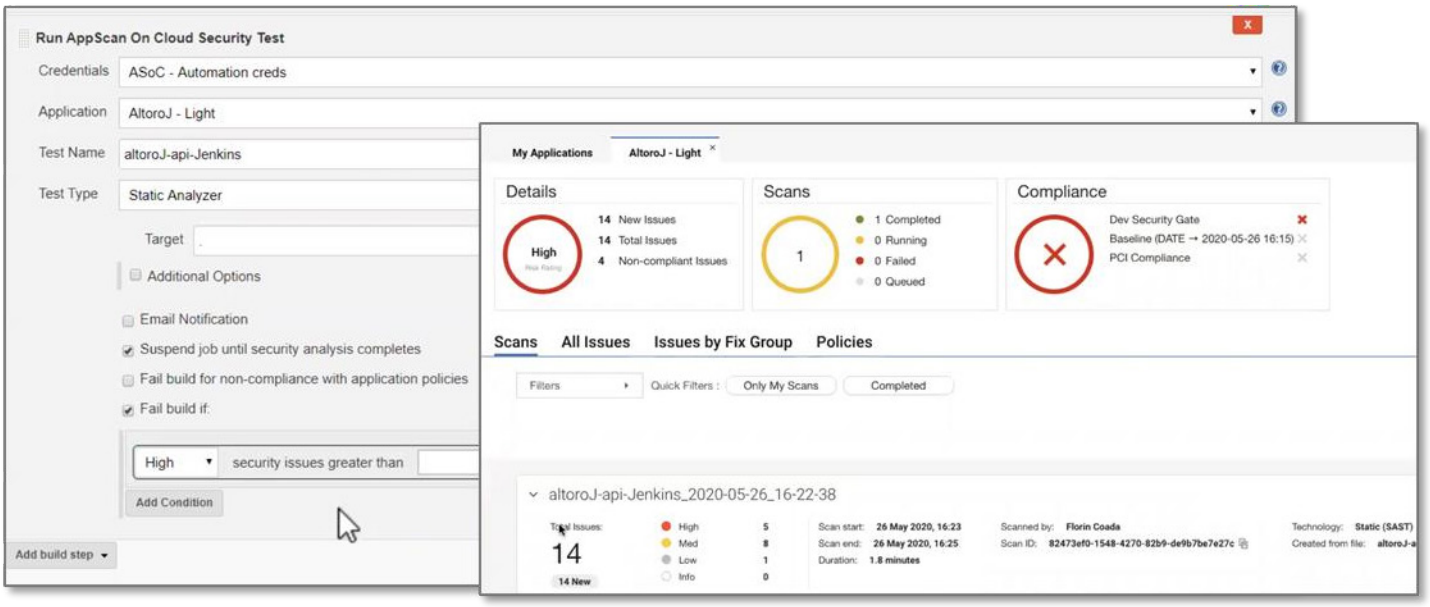
また、ESGでは、静的スキャンと動的スキャンのパラメータを追加で指定しました。静的スキャンでは、ESGはアプリケーションコードとサードパーティーおよびオープンソースコンポーネントの両方をスキャンしたり、アプリケーションコードのみにスキャンを制限したりすることができます。

自動化することで、ESG は、アプリケーション ポリシーへのコンプライアンス違反や、深刻度の高い脆弱性の閾値を超えるなど、ビルドの合否を判断するにあたって、複雑なルールを作成することができます。これらのルールにより、アプリケーション開発をセキュリティ脆弱性の修復と並行して進めることができ、セキュリティの専門家がビルドの自動化を編集することなくセキュリティポリシーを定義できるようになります。

AppScanダッシュボードを使用して、自動ビルド処理中のスキャンの状態を観察しました。ダッシュボードには、特定された問題、セキュリティスキャン、コンプライアンスに加え、スキャン内容と問題のリストが一目でわかるようにまとめられていました。ダッシュボードを使用することで、ESGはアプリケーションのセキュリティの現状を素早く把握できました。

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

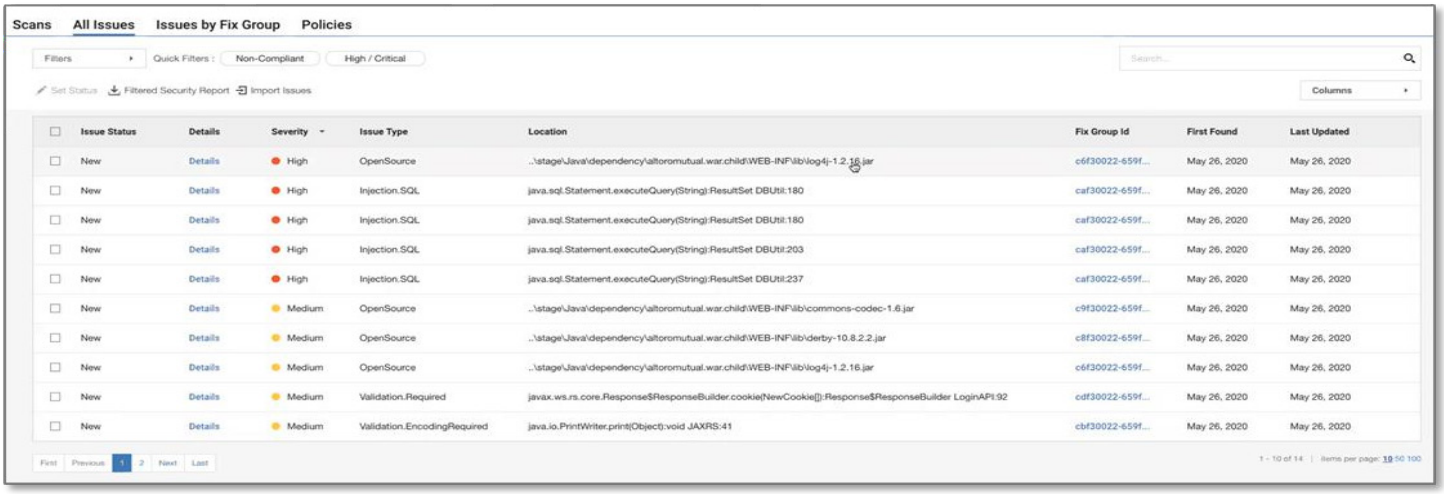
図3AppScanをJenkinsでDevSecOpsパイプラインに統合



出典:*Enterprise Strategy Group*

スキャンが完了すると共に、ESGは脆弱性の修復における側面を評価しました。HCLは、セキュリティの専門家とコード開発者双方のためにAppScanのダッシュボードを設計しました。図4に示すように、ダッシュボードの「All Issues」タブを使用すると、セキュリティの専門家は、アプリケーションのソースコードを見なくても、問題のリストをレビュー、トリアージ、優先順位付けすることができます。ダッシュボードには、コンプライアンスに準拠していない問題や危険度がクリティカルあるいは高い問題のためのクイック フィルタ ボタンがあり、ユーザーは独自のフィルタをカスタマイズすることができます。

図4スキャン結果



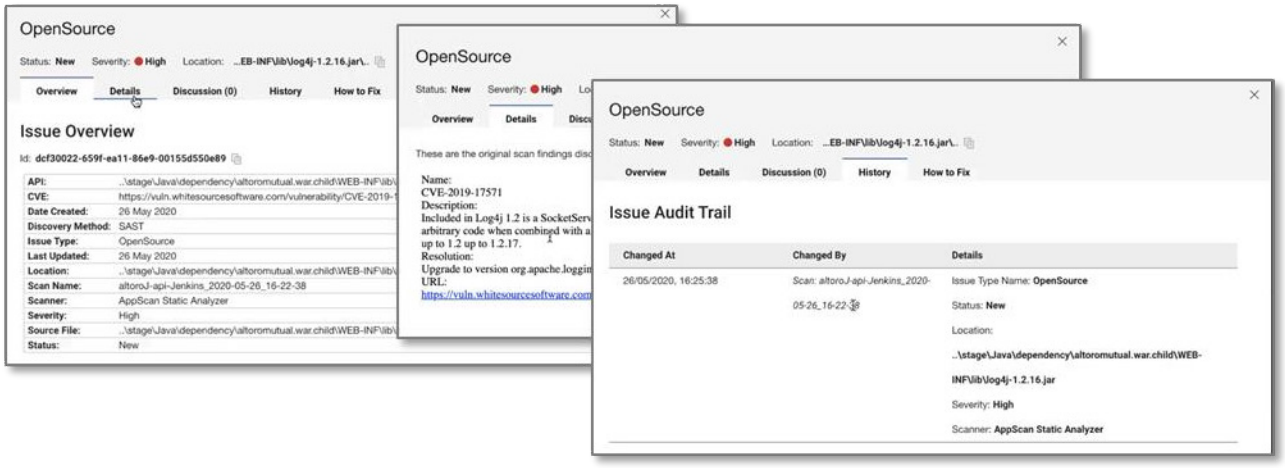
出典:*Enterprise Strategy Group*

「Details」リンクをクリックすると、図5に示すように、特定の問題における詳細が表示されます。「Issue Details」ポップアップ ウィンドウには、概要、詳細、開発者によるディスカッション、問題の履歴、および推奨される修正方法を提供するタブがあります。

開発者は「Discussion」タブでコメントを追加したり、監査証跡として機能する「History」タブでステータスを更新したりすることができます。ステータスを「noise」に変更することで、問題をオープンにしておくことができ、以後のスキャンでは問題を無視するため、スキャン処理を速く行えます。

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

図5問題の詳細



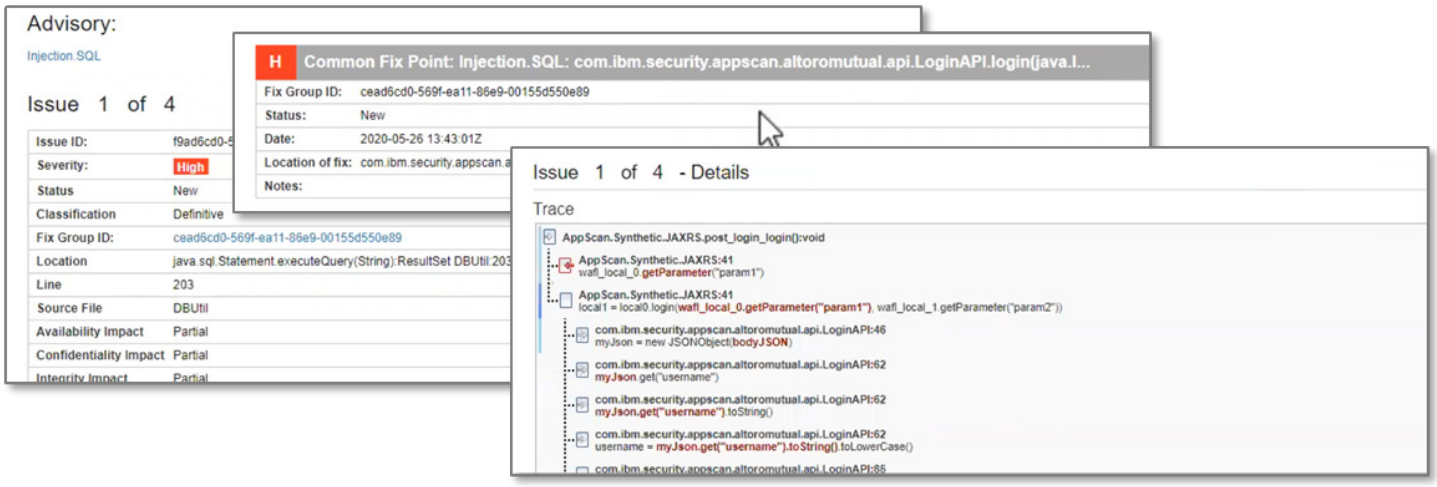
出典:*Enterprise Strategy Group*

HCLでは、AppScan結果のダッシュボードを利用する開発者には、「Issues by Fix Groups」タブを使用して問題のレビューを行うことを推奨しています。AppScanでは、機械学習技術を使用して、ソースコード内の修正箇所が同じであったり、異なる箇所で同じ修正技術が適用されていたりする関連する問題を特定、分類、グループ化します。フィックスグループを使用することで、余計な情報を取り除くことで開発者が集中しやすくなり、開発効率が向上します。

最初のフィックスグループを選択して、詳細を表示しました。図6に示すように、AppScanは4つの関連するSQLインジェクションの問題を特定し、グループ化しました。このフィックスグループは、各問題の場所を特定し、スタックトレースを提供しました。これにより、開発者は問題が発生した箇所とその修正方法をよりよく理解できるようなりました。

また、AppScanの機械学習エンジンは、修正が必要な可能性のある場所を特定し、迅速な修復に最適な箇所を開発者に示すことで、開発者の効率を向上させました。開発者をさらに支援するために、MLのコードでは、フィックスグループ内の複数の問題を一度に修正できるよう、問題共通の修正点を見つけようとしています。

図6フィックスグループ



出典:*Enterprise Strategy Group*

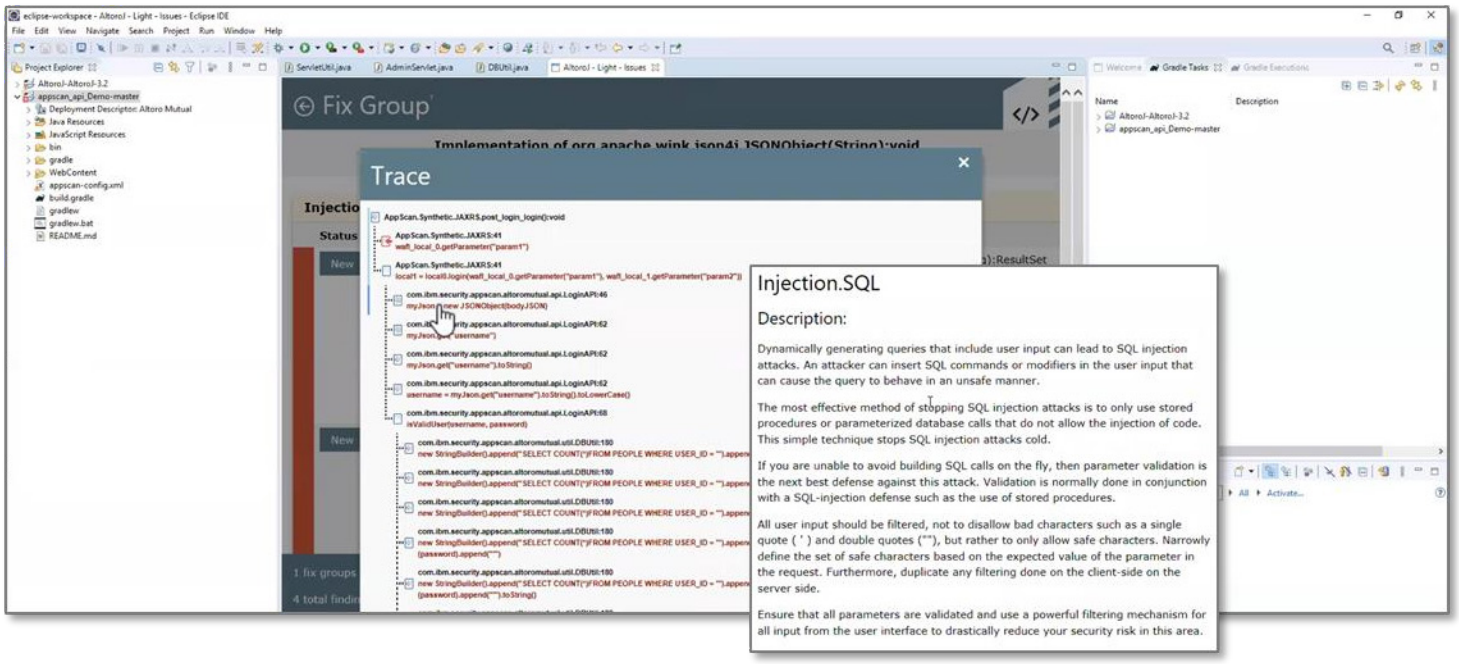
© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

開発者の効率をさらに高めるために、開発者はAppScanの結果を統合開発環境（IDE）から直接処理することができます。ESGはEclipseプラグインを使用して、前回のスキャンから問題のリストを取得しました。その後、ESGは、図7に示すように、SQL Injectionのフィックスグループをクリックして、この問題を確認しました。

AppScanコンソールで利用できるすべての情報とアクションは、IDEプラグインからも利用できます。ステータスの更新はAppScan on Cloud に自動的に伝わり、一貫性を維持しつつ、セキュリティの専門家、開発者、および管理者がアプリケーションのセキュリティについて同じ見解を持つことを保証します。

HCL は、コーディング言語の広範なリストと Java、.NET、および C/C++ の問題の詳細を提供するだけでなく、開発者に最適な修正箇所を提供します。問題の詳細にあるコード行への参照をクリックすると、ソースファイルが自動的にエディタに読み込まれ、カーソルがその行に移動するため、開発者の生産性が向上し、問題の修復を迅速に行うことができます。

図7 IDEにおけるAppScan



出典：*Enterprise Strategy Group*

次に、図8に示すように、AppScanコンソールを使用して、ESGは手動のダイナミックスキャンを作成し、結果のレビューを行いました。手動スキャン作成ウィザードを使用して、ESGはテストするURLとテスト環境を指定し、テストの攻撃性を制御しました。ステージング環境やテスト環境では、AppScanは自動的にフォームに記入し、JavaScriptコードを実行して可能な限り多くのコンテンツを発見しようとしますが、本番環境のサイトでは、実行中のアプリケーションへの影響を最小限に抑えるために、より繊細なアプローチが使用されます。また、ESGでは、スキャンの深さと幅、つまり持続時間を制御するために、テストの最適化設定を行いました。

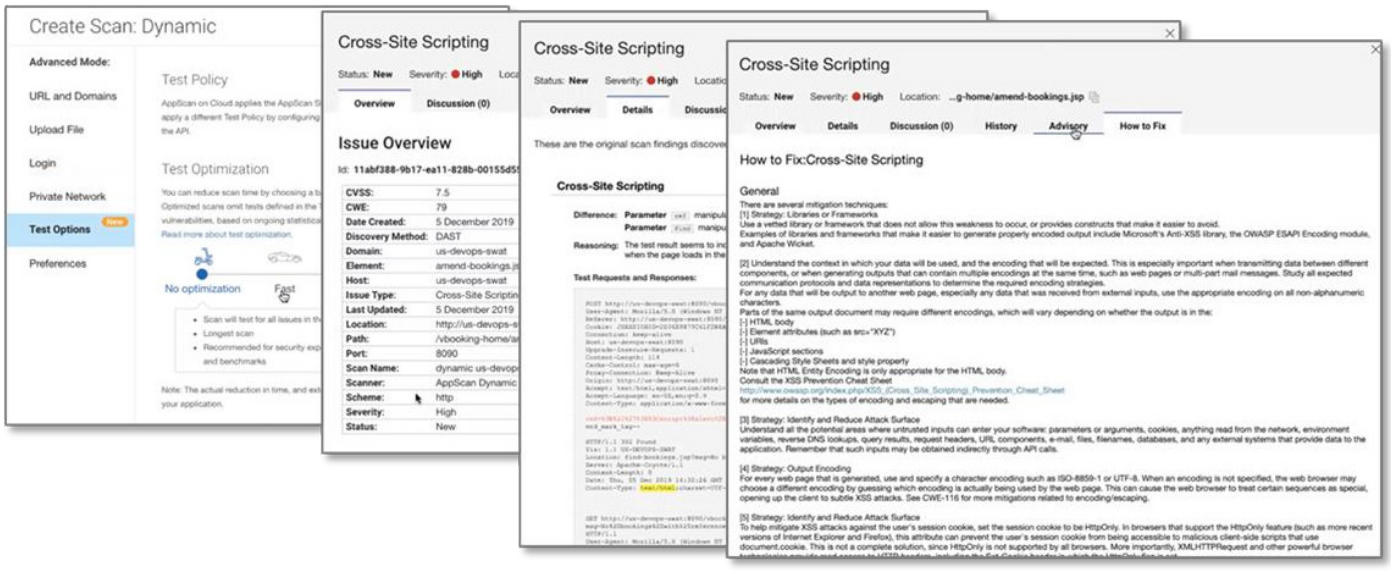
ESGは、テストを推進するためにWebサイトとの手動のインタラクションをキャプチャーすることで、焦点を絞った動的分析を作成しました。ESGは、ChromeブラウザーのHCLプラグインを使用して、サイトとのインタラクションを記録しました。ESGはその後、ダイナミックスキャンの設定の一部として、記録をAppScanにアップロードしました。

また、ESG は、アプリケーションがプライベートネットワークあるいはパブリックなインターネット上でホストされているかを特定しました。パブリックネットワーク上のアプリケーションに対して、HCLは署名ファイルを提供し、権限のある開発者によるスキャンを可能にすると共に、権限のないユーザーによるサイトの悪用を防いでいます。

スキャンが完了すると、ESGは結果のレビューを行いました。動的および静的スキャンとその結果は、AppScanコンソール、IDEプラグイン、AppScan Standardツールなど、さまざまな場所で確認できました。ESGがそのアプリケーションをスキャンしたところ、AppScanはクロスサイトスクリプティングの問題を確認しました。詳細なポップアップには、Webサイトにおけるコミュニケーションを捕捉したものや、問題の修正に使用するさまざまなテクニックの総合的な考察が含まれていました。

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

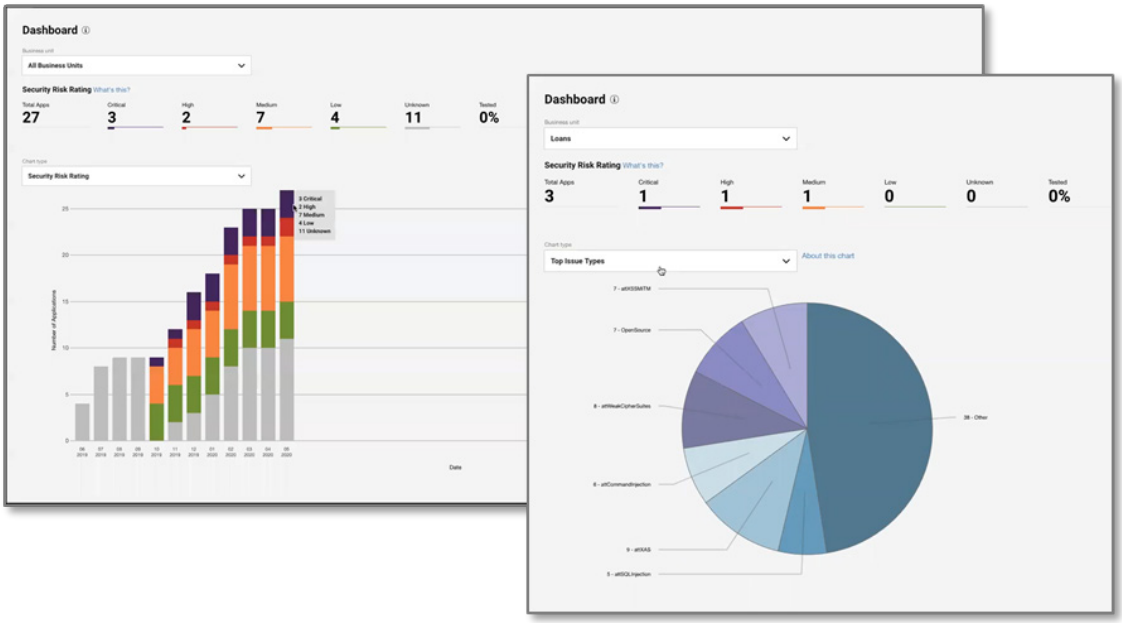
図8動的スキャンとその結果



出典:*Enterprise Strategy Group*

次に、ESGは報告フェーズを評価しました。AppScanは、さまざまなメトリクスを備えた多数のレポートやダッシュボードを提供しています。ESGは、ビジネスユニットや問題の深刻度などの重要な情報をフィルタリングしてグラフを構成することができます。図9は、ESGが特に有用と判断した2つのダッシュボードグラフを示しています。セキュリティリスクの評価を時間経過と共にグラフ化することで、ESGはアプリケーション全体のセキュリティ向上に向けた進捗状況を把握できました。主要な課題をタイプ別にグラフ化することで、現在最大のセキュリティリスクとなっている問題のタイプをESG側で把握できるようになりました。

図9レポートダッシュボード



出典:*Enterprise Strategy Group*

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

なぜ重要か？

アプリケーションのセキュリティ テストをDevSecOpsの手法に統合して自動化することで、アプリケーション開発ライフサイクルの早い段階でサイバーセキュリティの脆弱性を特定して修正することが可能になり、セキュリティの強化と効率性の向上につながります。また、熟練したサイバーセキュリティチームが直面している課題を軽減するのにも役立ちます。これらサイバーセキュリティチームは、往々にして、開発チームよりも小規模なもので、高まるDevSecOpsの要求に対応する努力を続けています。

ESGは、HCL AppScanが簡略化され、アプリケーションのセキュリティ テストが高速化されていることを検証しました。ESGは、わずか数回のクリックで、セキュリティポリシーの定義、AppScanの設定、そして一連のセキュリティ脆弱性とベンチマークや規制へのコンプライアンスのテストを行いました。ESGは、オンデマンドスキャンの設定と実行が迅速かつ容易であることに加え、静的分析と動的分析の結果が簡潔かつ一貫性のあるインターフェースで迅速に表示されることを確認しました。

ESGは、AppScanの機械学習エンジンが、関連する問題を特定してグループ化し、複数の問題に対して共通の修正ポイントを特定することで、脆弱性の修復プロセスを加速できることを検証しました。各問題に対する修正案を提案することで、開発者の生産性を向上させました。

ESGは、AppScanのJenkinsとEclipseのプラグインを介して、DevOps CI/CDプロセスの一部としてAppScanを自動化することが容易であり、開発者やセキュリティ専門家が通常の開発プロセスの一部としてアプリケーションのセキュリティテストを含めやすくなったことを確認しました。

重要な真実

悪意のもとに攻撃するハッカーは、常に新しいアプリケーションを探し求めており、未知の脆弱性を標的とした新たな攻撃を常に生み出し続けています。この現実に対処することはビジネスの成功に不可欠ですが、セキュリティは機能性よりも後回しにされがちです。開発者は、セキュリティを障害物とみなすこともあり、アプリケーションの機能をエンドユーザーに提供するスピードを第一に考えています。配信速度を阻害することなく、より優れたセキュリティを組み込むニーズは、アプリケーションのセキュリティ テストをDevOpsに統合し、自動化するニーズの高まりに繋がっています。これは、主にDevSecOpsと呼ばれています。

ESGは、HCL AppScanのDevSecOps機能を評価するために、HCL AppScanの技術レビューを実施しました。当該評価によって、以下のことが判明しました。

- AppScanは、セキュリティ専門家と開発者の協力関係を促進します。セキュリティ専門家は、DevOpsのビルドプロセスを変更することなく、セキュリティ問題の修正が必要な箇所を定義することができ、開発者は、セキュリティの専門知識を必要とせずに、これらの定義をビルドプロセスに組み込むことができます。
- AppScanは、セキュリティ専門家や開発者が脆弱性にトリアージおよび優先順位付けを行い、ノイズを最小限に抑えるのに役立ちます。
- AppScanは、関連する問題をグループ化し、共通の修正箇所を特定し、修正案を提供することで、開発者の生産性を向上させ、脆弱性の修復を促進します。
- AppScanは、共通の自動化サーバーやIDE用のプラグインを使用することで、容易にDevSecOpsパイプラインへ統合できます。開発者は、通常の開発ワークフローを変更することなく、AppScanを使用できます。

ESGは、管理された環境でのテストを通じて、AppScanが継続的なアプリケーションセキュリティに使用できることを確認しています。しかし、AppScanが特定のビジネス要件や目的を満たしているかどうかを判断するために、お客様自身で評価を行うことを推奨しています。

継続的なアプリケーションセキュリティを、組織内アプリケーションの攻撃の対象となりかねない範囲を縮小し、セキュリティ侵害の可能性を低減するための中核的な要素としたい場合、ESGは、AppScanをDevSecOpsおよびCI/CDの手法に組み込む方法を評価することをお勧めしています。

1 出典: ESG Master Survey Results, 2020 Technology Spending Intentions Survey, January 2020.

2 出典: ESG Master Survey Results, Application and Email Security Trends, September 2019.

ESGテクニカルレビューは、HCLが委託したもので、ESGのライセンスに基づいて配布されています。

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

すべての商標名は各社に帰属します。本書に含まれる情報は、Enterprise Strategy Group (ESG)が信頼できると判断した情報源から入手したものですが、同社が保証するものではありません。本資料にはESGによる意見が含まれている場合があり、予告なく変更される場合があります。本書の著作権はThe Enterprise Strategy Group, Inc.に帰属します。Enterprise Strategy Group, Inc.の明示的な同意なしに、ハードコピー形式、電子的、またはその他の方法で、それを受け取ることを許可されていない人にこの出版物の全部または一部を複製または再配布することは、米国著作権法に違反しており、民事損害賠償請求訴訟の対象となり、該当する場合は刑事訴追の対象となります。ご不明点等ございましたら、ESG Client Relations 508.482.0188までご連絡ください。

ESG Validationレポートの目的は、あらゆる種類と規模の企業に向けた情報技術ソリューションについてのIT専門家を教育することです。ESG Validationレポートは、購入を決定する前に実施すべき評価プロセスに代わるものではなく、これらの新興技術へのインサイトを提供することを目的としています。私たちの目的は、ITソリューションのより価値のある特徴や機能を求め、顧客が現実に直面している問題を解決するためにどのように使用できるかを示し、改善が必要な分野を特定することです。ESG Validation Teamの専門家による第三者視点は、当社独自の実地試験や、本番環境でこれらの製品を使用しているお客様へのインタビューに基づいています。