

HCL AppScan

継続的なセキュリティを包括的に提供



執筆者

Colin Bell,
HCL AppScan CTO

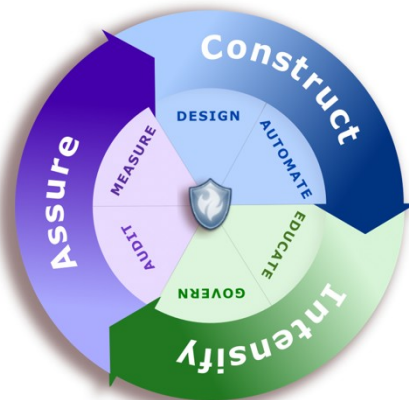
セキュリティ成熟度モデルのこれまで

世の中には多くのセキュリティ成熟度モデルの例があります。私は、2007年にWatchfire社に勤務していた時に、あるモデルを共同で作成したことを覚えています。このモデルでは、アプリケーション・セキュリティについて無知な状態から始まり、5つの改善段階を経て、アプリケーション・セキュリティが最適化された状態であるユートピアに到達するとしています。

このモデルは、私たちのチームがAppScanとともにIBMに吸収される際に再利用されました。公平に見て、このセキュリティモデルは他の多くの組織でも使用されました。セキュリティの成熟度で検索すると、このアプローチを描いた図がたくさん出てきます。同じ5つのステップを概説した派手な図もたくさんあります。

要するに、これは何のオリジナルでもなく、モデルはすべて、5段階の成熟度を持つソフトウェア工学研究所の能力成熟度モデル（SEI-CMM）と同様のアウトラインを提供しています。これは確かにセキュリティプログラムに多大なメリットをもたらす姿勢ではあるものの、一面的であり、改善を完全に強制するものではないことがわかりました。

なぜなら、これらの成熟度モデルはすべて、レベル5に到達した時点で作業が「完了」することを示唆しているからです。残念ながらこれは真実から大きく外れています。これは継続的なサイクル/モデルである必要があります。



Compliance
Security Requirements

どこから始めるべきか？

継続的なセキュリティサイクルを見た時に、最初にはっきりと考えられることは、正確な出発点がないということです。アプリケーション・セキュリティが、何も知らない、あるいは全く意識していないという状態から始まることはほとんどありません。ありがたいことに、組織（少なくとも私が出会った組織）はみな、アプリケーション・セキュリティに真剣に取り組まなければならないことを知っています。苦労しているのは、その方法です。多くの企業は、リリース前にアプリケーションをテストするための強力なセキュリティ対策を実施しており、自動化によって開発者を巻き込み、開発プロセスの早い段階で変更を行う「シフトレフト」という強い動きがあります。

少し調べてみると、多くのアプリケーション・セキュリティ・プログラムの根底にあるのは、セキュリティ・ガバナンスです。私にとっては、ここからが本番です。これは、セキュリティ要件であったり、外部のコンプライアンス優先事項（PCI-DSSやSOXなど）であったりします。問題は、これが出発点であって、終着点ではないということです。コンプライアンスの必要性を満たすためにアプリケーションをスキャンしても、問題解決に目を向けなかったり、問題を修正しなかったりしたら、何の意味があるのでしょうか。驚くべきことに、多くの組織がスキャンのためにスキャンを行い、スキャンしたアプリケーションの数で成功を測っています。



最も重要なコンストラクトフェーズ

コンストラクトフェーズ、特にコーディング時は、アプリケーションセキュリティが適用される最後の領域であることが多いです（結局、SDLCの中では非常に残された領域です）。しかし、私は次にこの領域を見ていきます。「シフトレフト」ではなく「シフトライト」しましょう。

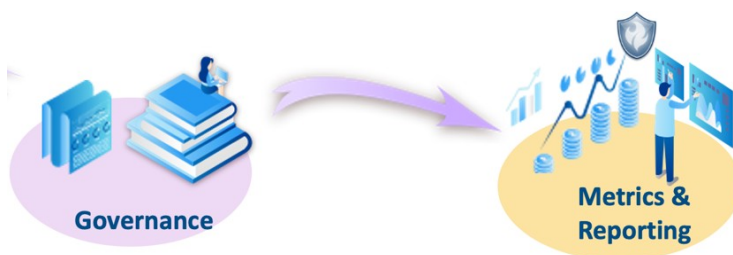
今日、開発者が開発中のアプリケーションをテストするためのツールやテクニックがたくさんあります。HCL AppScan CodeSweep のように、コードを書いている最中に検査して不正なコーディング手法を判断するツールから、ファイルやプロジェクトの静的解析スキャンを可能にするIDEプラグインまで、さまざまなものがあります。

開発プロセスのこの部分での成功は、これらのツールが使いやすく、意味のある結果を提供し、遠くから分析されるようなものではないことにあります。開発者は、入力のスニタイズを何回忘れたかというメトリクスを、ある種のリーグ戦のように見せられたいとは思いません。成功するためには、ライフサイクルのこの部分のツールは、開発者のためだけのものである必要があり、そのためには正確で明確に理解されている必要があります。

メトリクスが重要でないと言っているわけではありません。そうではありません。指標は、プロセスの成熟と進歩に合わせて正しく適用する必要があります。この点でも、多くの組織でアプローチが異なっています。私は、リリース前にすべてのアプリケーションがスキャンされていることが最も重要な測定基準であるケースを見てきました。通常、発見された結果はほとんど、あるいは全く重視されていません。通常、このようなアプローチの根本的な理由は、PCI-DSSなどのコンプライアンスの必要性からプログラムが推進されていることにあります。

また、テストするアプリケーションの数を重視する人もいます。多くの場合、「王冠の宝石」や最も重要な重要アプリケーションから始めて、そのアプリケーションがある程度の基本的なセキュリティ・ポリシーを満たしていることを確認します。例えば、アプリケーションが次のフェーズに移行する前に、すべての高リスクの問題が緩和されているかどうかを確認します。

より成熟した組織では、脆弱性の修正に要する時間を測定し、チームベースの測定基準を活用して、どこに脆弱性が発生したか、あるいは作られたかを判断します。



どのようなアプローチであっても、セキュリティガバナンスの観点から測定基準を設定することが重要です。これには、ビジネスリスクに基づいたアプリケーションのテストプロセスの概要が含まれる場合もあれば、スキャンにどのような種類のポリシーを適用するか、どのようなリスクを許容し、どのようなリスクを修正する必要があるかを決定するセキュアコーディングガイドラインが含まれる場合もあります。

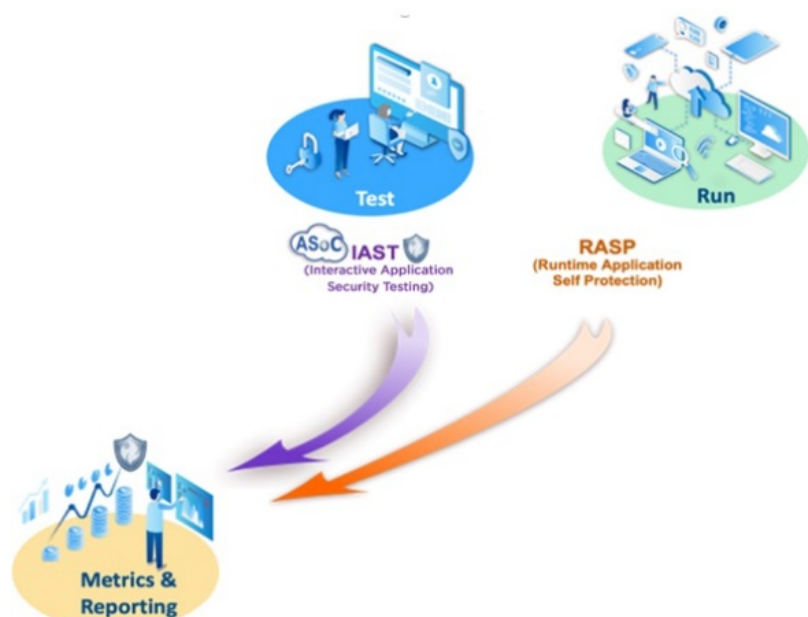
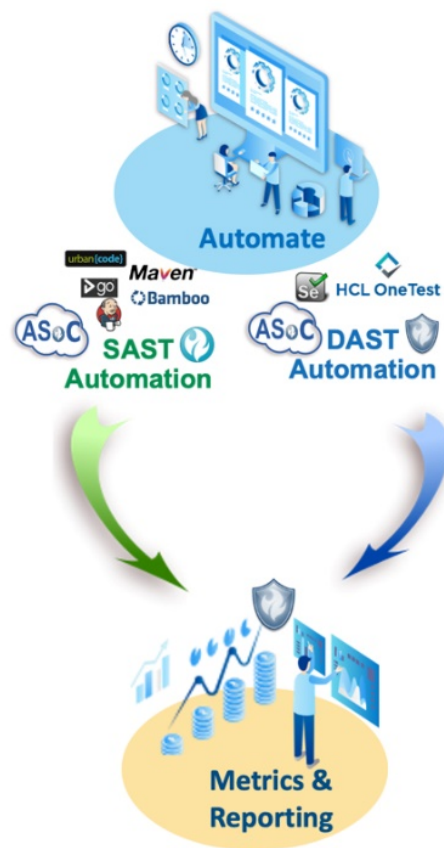
自動化の段階は、ほとんどの組織がアプリケーション・セキュリティに注目するところです。これは、継続的インテグレーション（CI）パイプラインの一部として自動的に実行される静的テストおよび動的テストで形成されます。HCL AppScanソリューションは、さまざまなプラットフォームに対応し、オンプレミスまたはクラウドベースのソリューション、あるいはその両方を組み合わせて提供できます。ここでの目的は、CIプロセスを妨げずにセキュリティ評価を行うことです。

多くの人にとって、これはDevSecOpsプログラムを成功させるための鍵となります。これは事実ですが、アプリケーション・セキュリティ・プログラムの開始と停止は、しばしばここで見られます。時には、開発チームがセキュリティチームから切り離されて作業していることがあります。また、コンプライアンス上の必要性を満たすために自動化を行うこともあります。

確立された測定基準があれば、開発チームをアプリケーション・セキュリティの目標に結びつけることができるだけでなく、セキュリティ改善のための手順を確実に実行できます。

私が継続的なセキュリティについて話したい理由の1つは、この重要なフェーズを超えて議論を進めるためです。DevSecOps は、スキャンを自動化するだけでなく、それを超えて議論する必要があります。

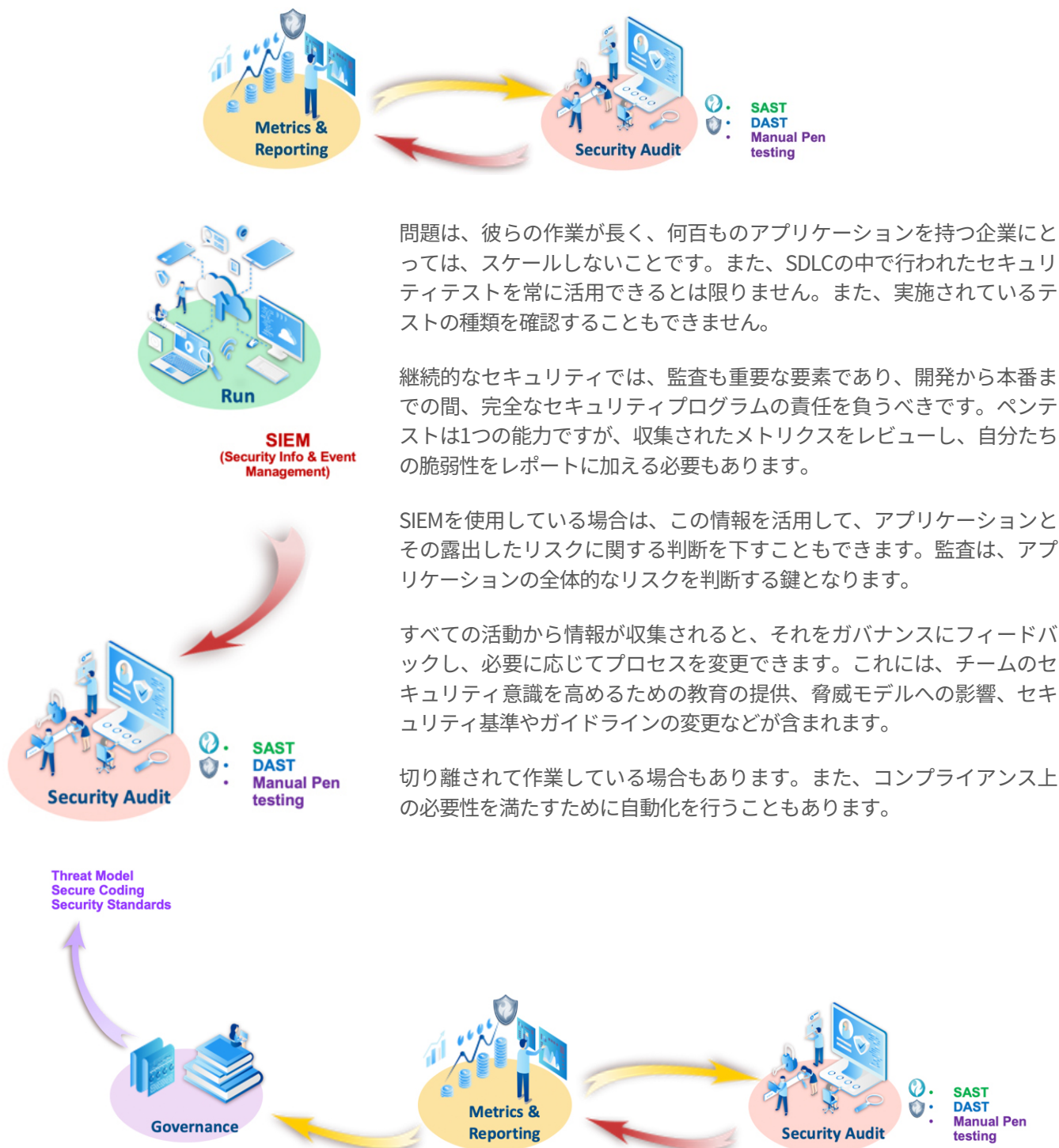
そのためには、機能テストが行われるライフサイクルのフェーズで、セキュリティ・テストを行わせることが課題となります。また、機能テストをチームで実施する場合、チームメンバーには、機能テストを必要なレベルで実施するためのセキュリティ・スキルがないことが多いのです。そこで、インタラクティブ・アプリケーション・セキュリティ・テスト（IAST）のような機能が役立ちます。



HCLのIASTソリューションは、テストチームがテスト環境にIASTエージェントまたはモニターを展開すると、テストチームが通常の機能テストやQAテストを行っている間に発見された問題や脆弱性を報告してくれます。スキャンを実行する必要はなく、これらが同じ報告ポイントにプッシュされていれば、セキュリティチームが監査やレビューを行う際に情報を利用できます。

同じことが、ランタイム・アプリケーション・セルフプロテクション（RASP）ソリューションにも当てはまります。このような情報は、セキュリティの状況を判断し、改善するために不可欠なものとなります。

このことが、セキュリティ監査の活動にうまくつながっています。多くの組織では、これは独立した機能であり、重要なアプリケーションのセキュリティテストやアプリケーションのペネテストを担当しているかもしれません。私は過去にこの業務に携わったことがあります。これらのチームは非常に高い技術を持ち、脆弱性を探す際には絶対に漏れがないようにする能力に誇りを持っています。



問題は、彼らの作業が長く、何百ものアプリケーションを持つ企業にとっては、スケールしないことです。また、SDLCの中で行われたセキュリティテストを常に活用できるとは限りません。また、実施されているテストの種類を確認することもできません。

継続的なセキュリティでは、監査も重要な要素であり、開発から本番までの間、完全なセキュリティプログラムの責任を負うべきです。ペネテストは1つの能力ですが、収集されたメトリクスをレビューし、自分たちの脆弱性をレポートに加える必要もあります。

SIEMを使用している場合は、この情報を活用して、アプリケーションとその露出したリスクに関する判断を下すこともできます。監査は、アプリケーションの全体的なリスクを判断する鍵となります。

すべての活動から情報が収集されると、それをガバナンスにフィードバックし、必要に応じてプロセスを変更できます。これには、チームのセキュリティ意識を高めるための教育の提供、脅威モデルへの影響、セキュリティ基準やガイドラインの変更などが含まれます。

切り離されて作業している場合もあります。また、コンプライアンス上の必要性を満たすために自動化を行うこともあります。

継続的なセキュリティ 成功の柱

継続的セキュリティを成功させるための柱は、監査、測定基準、ガバナンスが連携していることです。要するに、ガバナンスは、なぜ、どのようにしてセキュリティテストを行うのかを示し、メトリクスはテストに関する事実を示し、監査はテストが望ましいレベルで機能していることを確認することです。



これらすべてをまとめると、セキュリティがSDLC全体に組み込まれていることを確認するためのフローができあがります。

また、教育が成功への基本的な鍵であることも言及する価値があるでしょう。これは、ツール、セキュリティ意識、プロセス、さらには安全なコーディング技術に関するものです。継続的なセキュリティの目標は、チームが最適なレベルで作業していること、そして重要なのは、プロセスが必要に応じてレビューされ、改善されていることを確認することです。

詳細情報

このテーマについてもっと知りたいという方は、オンデマンドのウェビナーで、私と同僚が「継続的なセキュリティ」についてさらに詳しく説明していますのでご覧ください。

著者について



Colin Bell,
AppScan CTO

Colinは30年以上のIT経験を持つ。過去18年間、アプリケーション・セキュリティに特化し、AppScanポートフォリオを世界中の顧客に展開してきました。現在は、HCLソフトウェアチームでAppScanのCTOを務めています。

Way Forward

Expected Value To Customers

Customer hyper-care – Nurture and strengthen existing customer relationships. Engage in closer, meaningful discussions on product direction. Customer-centric roadmaps – Apart from addressing key customer requirements, HCL is also investing in product modernization and TCO reduction for customers.

Expected Value To Partners

HCL Software has a robust Partner ecosystem to design, deliver and support our offerings. Whether you are a developer, consultant or partner, Partner Connect will provide you with insight on how you can build value in your go to market with HCL Software. Partner Connect - One-stop-shop for software-based offerings to enable growth and scale:

<https://www.hcltechsw.com/wps/portal/resources/partner-connect/>

Resell and Build With Us | Provide Services around our Products.

Please reach out to Geo Partner heads for more information. You can find your geo head at:

<https://www.hcltechsw.com/wps/portal/resources/partner-connect/partner-resources/partner-team>

製品ポートフォリオの詳細については、www.hcltechsw.comをご覧ください。



HCL Software について

HCL Software は、HCL Technologies (HCL) の一部門であり、主要なソフトウェア事業を展開しています。HCLソフトウェアは、DevOps、自動化、デジタルソリューション、データ管理、メインフレームの分野で、20以上の製品ファミリーを開発、マーケティング、販売、サポートしています。HCLソフトウェアは、世界中に事業所や研究所を持ち、何千ものお客様にサービスを提供しています。HCLソフトウェアの使命は、製品の絶え間ない革新により、IT投資で顧客を成功に導くことです。詳細については、www.hcltechsw.com

Copyright © 2021 HCL Technologies Limited.