SYNOPSYS®

集約して簡素化する：アプリケーション・セキュリティ・ツールを合理化し、ソフトウェア・リスクを管理

なぜ今、集約の重要性が叫ばれているのか

「ソフトウェアが世界を飲み込もうとしている」と Marc Andreessen 氏が発言したのは今から 10 年以上前のことです。そしてその予測のとおり、小売から自動車、農業から防衛まで、既存のあらゆる産業がソフトウェアによって根底から変革されました。ただし、それに伴って世界中のソフトウェア・セキュリティ・チームの活動が激変することまでは同氏も予測しませんでした。事実、自前コードであれ商用などの再利用コードであれ、ソフトウェアのコード**量**がこれほどまでに増大すること、そしてそれに伴う攻撃対象領域（アタック・サーフェス）の指数関数的な拡大によりアプリケーション・セキュリティ（AppSec）の必要性がここまで高まることは当時誰も予測できなかったはずです。

あらゆる業界でソフトウェアが増え続けている今、急速な技術革新のペースに合わせてセキュアなソフトウェアを本番環境へ投入することを義務付けられているチームは、大きな課題に直面しています。こうした課題に対し、多くの組織はソフトウェア開発ライフサイクル（SDLC）にいくつものポイントツール（特定の機能を提供することに特化したツール）を追加するというアプローチで対処してきました。しかし、開発者とセキュリティ・ツールチェーンの組み合わせは、ソフトウェアのセキュリティを強化しながら開発の速度と俊敏性を高めることを約束してくれたはずでしたが、逆にソフトウェアの出荷スピードを低下させているケースがほとんどです。この結果、チームがソフトウェアを本番環境への迅速なリリースを最優先させてしまい、セキュリティの検証や確認の手順を省いてしまう事態が生じ、リスクの全体像が把握しにくくなっています。

こうした現状と、慎重な予算管理が求められる現在の経済状況があいまって、多くのビジネスおよびソフトウェア・アナリストたちが今、セキュリティ・ツールチェーンの集約を強く提唱しています。ベンダーとセキュリティ・ツールを集約することは、業界を問わずすべての組織が直面している 3 つの深刻な問題、すなわち複雑化の進行、リスク管理能力の低下、そしてこれらツールの TCO（総保有コスト）を押し上げる要因となっているリソース効率の低下を解決する手段となります。

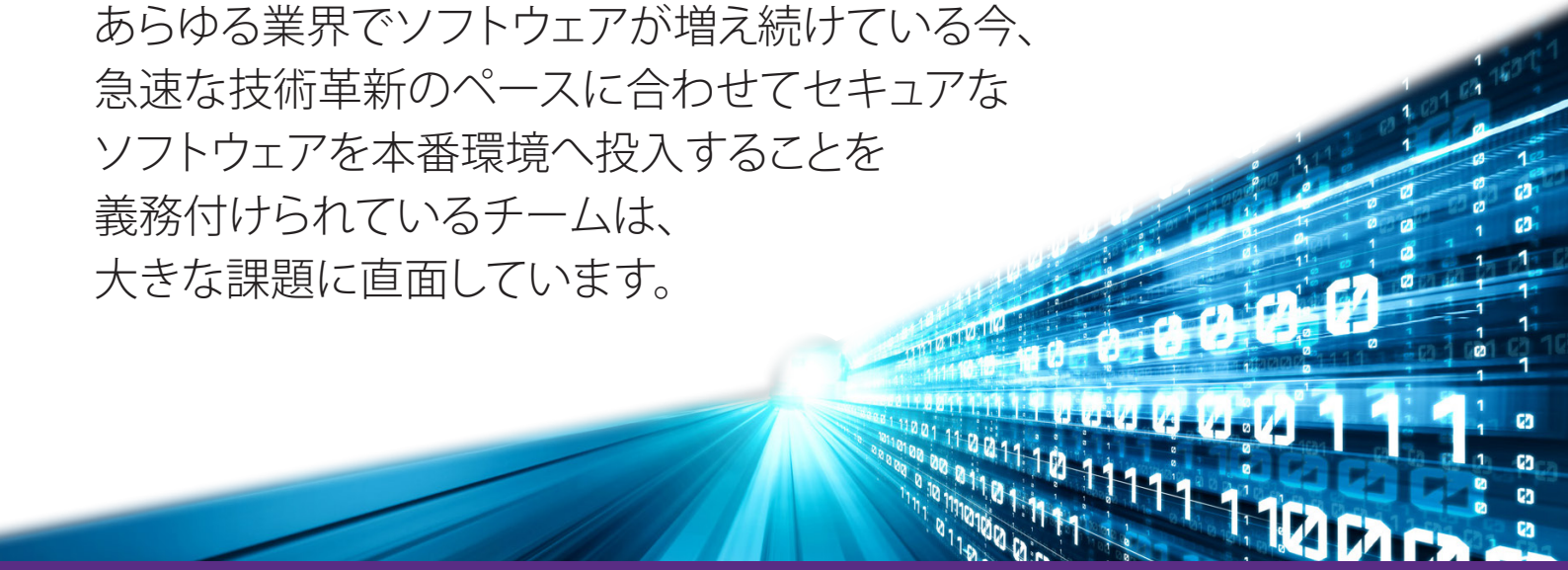
ツールの増加が複雑さの要因に

セキュア開発を支援するツールを多く導入しすぎると、開発およびセキュリティ環境は複雑で入り組んだものとなります。こうした環境を維持管理しようとすると、SDLC の摩擦とそれによる開発サイクルの長期化、エラーや脆弱性のリスクの増大、そして新しいテクノロジーの拡張と統合の難しさなど、さまざまな問題が発生します。特に、開発パイプラインが停滞すると開発チームは開発マイルストーンの達成を優先させてセキュリティ・ゲートをスキップしたり無視したりするようになります。こうして、SDLC を強化するために導入したはずのツールチェーンが摩擦を引き起こして SDLC が破綻し、リスクが軽減するどころかむしろ増大する結果となっています。

先ごろシノプシスと Enterprise Strategy Group が共同スポンサーとなって作成した調査レポート「DevSecOps の難題を解く」でも、現在使用している AST ツールが 10 種類を超えていると答えた組織が全体の 70% 以上を占めていました。しかも大規模な組織はサイロ化されていることが多く、複数の開発チームがそれぞれ 10 種類のツールを使用していると、複雑さは掛け算方式で増大します。多くの場合、ツールの選定と実装はそれぞれの開発チームに委ねられています。このため、セキュリティ・ポリシーの実装がツールごと、あるいは組織内のチームごとに異なり、一貫性が失われます。するとアプリケーション・セキュリティ・プログラムの実装にも一貫性がなくなり、セキュリティ・チームがリスクを一貫した方法で評価することができなくなります。ポリシーの実装に一貫性がなくなると、すべてのアプリケーションまたは組織全体のリスクの測定や報告、ポリシーの適用ができなくなります。

集約とは、なるべく少ないベンダーから必要不可欠なツールのみを絞り込んで調達し、使用することを言います。また、組織全体で一貫性のあるポリシーとワークフローを実装および拡張していくのに必要な工数を集約することも意味します。これにより、開発環境の複雑さが最小に抑えられ、チームはビジネスで要求されるスピードで作業できるようになります。

あらゆる業界でソフトウェアが増え続けている今、
急速な技術革新のペースに合わせてセキュアな
ソフトウェアを本番環境へ投入することを
義務付けられているチームは、
大きな課題に直面しています。



現在使用している AST ツールが
10 種類を超えていると答えた組織が
全体の 70% 以上を占めています。

リソース効率の低下により AppSec の ROI が低下する

ソフトウェアの複雑さはリスクを高めるばかりでなく、管理、メンテナンス、およびサポート面での課題も引き起こし、セキュリティ・ツールの TCO に甚大な影響を与えることがあります。AppSec プログラムの投資収益率（ROI）に悪影響を与える主な要因には、(1) 開発リソースの浪費、(2) 複数のベンダーから多くのツールを調達して実装、管理するのに必要な運用リソースの増大、(3) ツールのライセンス・コストの増大があります。これらの要因により、組織はチーム間、ベンダー間でスケールメリットを享受できなくなります。

ツールが増え続けると、開発チームはたくさんの UI を習得して使いこなす必要があります。これは貴重なコーディング時間を奪うだけでなく、複数のツールを行き来する際の障壁を大きくもします。さらに、重複する問題が課題追跡システムにプッシュされたり、コンテキストや優先順位の情報がないまま問題が提示されたりすると、開発者はトリアージに忙殺されることになります。開発者を取り巻くセキュリティ環境が複雑になると、重要な開発活動から貴重なリソースが奪われるだけでなく、俊敏性が低下して市場や顧客ニーズの変化への迅速な対応が困難になります。

また、開発チームにプレッシャーがかかるとセキュリティ手順をスキップし、問題があることを知りながらソフトウェアを出荷するようになるため、ミスやセキュリティ侵害の可能性が高まります。また、修正作業に膨大なコストが発生するばかりでなく、法規制への違反により重大な影響を被ることにもなります。

増えすぎるツールの重荷に耐えかねているのは開発チームだけではありません。調達チームも多くのベンダーや契約を管理し、これらツールの実装、メンテナンス、サポートに必要なリソースを見つける作業で手一杯な状況です。予算をいかに有効活用するかが組織の重要課題となっている今、このような運用コストの増大は正当化が難しくなっています。

そして最後に、複数のベンダーからポイントツールを購入することは、間違いなくセキュリティ・スタックのライセンス・コストを押し上げます。多くの契約を個別に管理していると、調達チームの購買力が低下します。さまざまなセキュリティ・ニーズを 1 社のベンダーとの契約で満たすようにすれば、大口割引や長期割引などのメリットを受けやすくなります。

リスクの全体像を把握できない

Enterprise Strategy Group の調査では、10 種類以上の AST ツールを使用した場合にセキュリティ・リスクがどのように高まるのかについてのデータも示されています。セキュリティ・ツールの数が増えるとテストの数が増え、その結果、テスト結果と問題の数も増えます。この調査でも明らかにされているように、たくさんのポイントツールから返される結果には多くのノイズが含まれ、開発者には脈絡のない検出結果が山のように押し寄せます。その中には重複した結果も含まれるほか、コンテキストを考慮した効率的な修正ガイダンスが提示されることもほとんどありません。このため、開発者はセキュリティ問題のトリアージに貴重な時間とリソースを奪われ、問題の修正に取りかかることさえできずにいます。このように、コンテキストを考慮して優先順位を付けた問題を一元的に把握する仕組みがなければ、開発者は膨大なノイズの除去に時間を奪われるばかりで、重大な問題だけを修正して次の作業に移るといったことは実現不可能です。ほとんどの開発者にとって、最大の職務はソフトウェアを出荷することであり、それは必ずしもセキュアなソフトウェアを出荷することを意味しません。このため、セキュアでない、あるいは脆弱性があると知りながらソフトウェアをリリースしてしまうこともあります。

1 つの開発チームが 1 つのアプリケーションのリスクを理解するだけでも大変だと言うのに、ツールとその検出結果があまりにも多いと、ポートフォリオ全体のリスクを理解するのがますます難しくなります。さまざまなチームにポイントツールが散在し、その中にリスク・データが格納されていると、監査のたびに無駄な労力を費やすことになります。ソフトウェアのリスクを迅速かつ正確に報告するには、一元的な記録システム（SoR）を構築して、何がテスト済みなのか、何が検出されたのか、何が修正済みなのかをいつでも確認できるようにする必要があります。

経済的要因と現場の要望の両面から AppSec イニシアティブの合理化が強く求められている今、TCO を改善するだけでなく、複雑さを抑えて真のリスク管理を達成するための実践的なソリューションとして「集約」が叫ばれるようになっています。

最近の調査で、Gartner は次のように指摘しています。「需要側の事情として、最高級のセキュリティ製品ポートフォリオを組み込むのに必要なテクニカル・セキュリティ・スタッフの数がほとんどの組織で不足しています。この結果、セキュリティおよびリスク管理のリーダーたちの 80% が今、ベンダーの数を絞り込んでセキュリティ支出を集約しようと考えています。これにより、エンタープライズのリスク態勢およびセキュリティ・スタッフの効率を向上させようという狙いがあります。」

次のページからは、ベンダーとツール、セキュリティ対策の工数、およびセキュリティ分析情報を集約する手順について説明します。

ベンダーとツールを集約する

多くの組織が 10 種類以上の AST ツールを使用している現状では、これ以上ツールを増やすのではなく、既に所有しているツールをいかに最適化するかを考えることが問題解決への第一歩となります。そのためには、まず自社のビジネスに必要不可欠なセキュリティ・テストを特定し、そのテストがきちんとカバーされていることを確認します。そして非効率性と複雑さの要因となっている重複機能を取り除きます。次に必要なのが、リソース効率の改善です。これにはいくつかの方法があります。

まず、チームが管理しているベンダーの数を減らします。自社が必要とする複数の重要なテスト領域に対して強力なソリューションを 1 社で提供できるアプリケーション・セキュリティ・パートナーを見つけることにより、調達、実装、サポートの各チームにかかる運用上の負担を軽減できます。

複数のツールを単一のベンダーから調達することで問題はある程度解決しますが、連携のとれていない実装では集約がもたらすメリットを最大限には享受できません。複数のカテゴリで最高級のソリューションを提供しているベンダーなら、ツール間の強力な統合ポイントも用意されているはずで、全体的なエクスペリエンスがよりシームレスなものになります。

開発チームがいくつもの UI を習得し、複数のツールから報告される問題をトリアージせざるを得ない状況を解消するには、開発チームとセキュリティ・ツールの間に抽象化レイヤーを挟むようにします。この役割を果たすのが、アプリケーション・セキュリティ態勢管理（ASPM）ソリューションです。ASPM ソリューションを使用すると、チームは 1 つの UI を覚えるだけでよいため効率が向上するほか、テストに影響を与えることなく新しいツールをプラグイン方式で追加したり、不要なツールを除去したりできます。

連携のとれていない実装では集約がもたらすメリットを最大限には享受できません。

Gartner は次のように述べています。「アプリケーション・セキュリティ態勢管理はソフトウェアの開発からデプロイ、運用にわたってすべてのセキュリティ信号を解析することにより、可視性の向上、脆弱性管理の改善、セキュリティ対策の適用を可能にします。ASPM を使用することで、セキュリティ・リーダーはアプリケーション・セキュリティの効果を高め、リスク管理を改善できます。」

セキュリティ・ベンダーを精査する

集約を決断したら、その実行方法を検討する必要があります。まず考えるべきは、セキュリティ・ベンダーの精査方法です。1 つの判断材料となるのが、そのベンダーのポートフォリオが自社のセキュリティ・ニーズを完全にカバーできるかどうかです。

自動ツールの「三種の神器」、すなわち静的アプリケーション・セキュリティ・テスト（SAST）、ソフトウェア・コンポジション解析（SCA）、動的アプリケーション・セキュリティ・テスト（DAST）のいずれか 1 つしか提供していないベンダーでは不十分です。これら 3 つすべてに対して堅牢性と精度と効率を兼ね備えたクラス最高のツールを提供しているベンダーが必要です。このうち 1 つでも欠けていると、セキュリティの鎖に弱い環ができてしまいます。セキュリティの鎖の強度は最も弱い環によって決まるため、このようなベンダーを利用していてはアプリケーションのセキュリティを確保できません。

もう 1 つの判断材料として、そのベンダーがオープンなプラットフォームを提供しており、自社で導入済みのツールを活用できるかどうかを確認します。集約は一朝一夕にできることではなく、ほとんどの組織は既にいくつものセキュリティ・ツールを導入しています。そこで、これらすべてを連携動作させ、適切なタイミングで適切なテストを適切な深さで実行できるようにすることが鍵となります。このため、既存のセキュリティ・テスト・ツールを活用しながらベンダー集約を可能にする統合機能を備えたプラットフォームが必要となります。

最後に、そのベンダーに長期的な安定性があるかどうかを確認する必要があります。集約とは、そのベンダーと長期的な関係を結ぶことを意味します。そのベンダーには、急速に進化する開発手法や脅威に合わせてポートフォリオを発展させてきた実績があるでしょうか。集約の目標を達成できるかどうかは、どのように集約を進めるかにかかっています。したがって、ソフトウェアに信頼を組み込めるように時間をかけて集約を進めることが重要です。

集約はツールとベンダーの数を減らすことから始まりますが、それで終わりではありません。ポリシーを一元化し、すべてのセキュリティ・ツールから結果を取り込むこと。そしてこれらに優先順位を付けてコンテキスト化し、管理とレポート作成を中央から実行できるようにすること。これらを可能にする仕組みがチームには必要です。集約の一環としてこのような仕組みを構築することで、リソースが最適化されるだけでなく、実際の結果としてリスク態勢が改善します。

工数を集約して複雑さを抑える

1 つのチーム内でいくつものポイントツールを実装すると、工数の重複が大量に発生します。そればかりか、アプリケーション・セキュリティ・プログラムの実装にも一貫性がなくなります。

ツールとベンダーを整理統合し、ASPM ツールを実装してチームが単一の UI を使用できるようにしたら、次にその管理に必要な工数を集約することで、AppSec プログラムの複雑さをさらに緩和できます。これにはいくつかの方法があります。

ポリシー管理を一元化する

10 種類を超える AST ツールを使用していると、ポリシーの実装に一貫性がなくなり、AppSec チームには余分な作業が大量に発生します。ASPM ツールでポリシー管理を一元化すると、現在どのようなセキュリティ・ツールを使用中であっても、セキュリティ・ポリシーを 1 回設定しておくだけであらゆるアプリケーションとチームに対して一貫性のあるポリシーを適用できます。これによりポリシー適用が合理化され、工数の重複が減り、組織全体でセキュリティへのアプローチを標準化できるようになります。

テストを自動化する

ポリシー管理が一元化されると、チームは問題の修正に関する SLA を設定および適用し、個々のリスク許容度に基づいてテストを自動でオーケストレーションできるようになります。一部の ASPM ソリューションには、コンテキストを考慮したテストをタイムリーに実行できる自動化機能を備えたものもあり、開発マイルストーンに合わせてスキャン・スケジュールを最適化できます。このようにインテリジェントな自動化を導入することにより、必要なタイミングでセキュリティ・テストを実行できるようになり、不要なスキャンを減らして開発プロセスのボトルネックを解消できます。

開発環境に統合する

セキュリティ対策の工数を集約するには、ASPM ツールと既存の開発環境の統合が不可欠です。開発者は、いくつものスタンドアロン・セキュリティ・ツールの習得と管理に時間を奪われるのではなく、使い慣れたツールチェーンの中でセキュリティ・ツールやセキュリティ分析情報にシームレスにアクセスできるようにする必要があります。セキュリティを開発プロセスの一部に組み込むことで、セキュア・コーディング・プラクティスが可能になり、開発ワークフローを邪魔することなく全体的なソフトウェア・セキュリティが強化されます。例えば、問題のトリアージと修正、およびそのステータス更新を開発者が課題追跡システムの中で直接行えるようになれば、生産性が向上し、システム同期の問題は発生の余地がなくなります。

このようにしてセキュリティ対策の工数を集約することは、複雑さを抑えて TCO を改善する最も効果的な手段の 1 つです。ASPM を導入すると、サイロ化の解消とコラボレーションの促進、ポリシー管理の一元化、テストの自動化、既存の開発環境への統合が可能になり、その結果、セキュリティ・プラクティスの最適化、運用コストの削減、強力なアプリケーション・セキュリティ態勢の確立を効率的かつ効果的に実現できます。

セキュリティ分析情報を集約してリスク管理を強化する

組織が依存するベンダーとツールを集約し、AppSec プログラムの実装と管理に関する工数を集約したら、次にツールから得られるセキュリティ分析情報の集約に取りかかります。

セキュリティ分析情報を集約すると、信頼できる唯一の情報源（SSOT）が構築され、リスクの全体像を把握できるようになり、組織のセキュリティ態勢の可視性が向上します。こうした分析情報を一元的に閲覧できるようになれば、意思決定担当者は潜在的な脅威の軽減、監査までの時間の短縮、新しい脅威の迅速な解決が容易になります。

セキュリティ分析情報を集約するには、まずすべてのセキュリティ・ツールで検出された結果を中央に集め、正規化して優先順位を付ける仕組みが必要となります。これにより開発チームにとってのノイズが減少し、どの問題をどの優先順位でいつまでに修正すればよいかが明確になり、開発プロセスが円滑に進むようになります。アプリケーション、コンポーネント、および関連するセキュリティ・データをビジネスの文脈に正確に位置付けて重大な問題を特定し、優先順位を付けることにより、チームはいつでもソフトウェアの全体的なリスクを実用的な観点から把握できます。

これを実現する上で中心的な役割を果たすのが、ASPM ソリューションです。ASPM を使用して AppSec プログラムを管理すると、開発者にとってのセキュリティが簡素化され、一貫性のある AppSec ポリシーの実装に必要な工数が削減されるほか、すべてのセキュリティ・データを 1 か所にまとめて問題に正確な優先順位を付けることや、信頼できる唯一の情報源（SSOT）を構築して組織のリスクを一元的に把握することができます。

まとめ

あらゆる業界でソフトウェア革命が続く中、自前コードであれ商用などの再利用コードであれ、コード量は今も増え続けており、ソフトウェア・セキュリティ・チームはかつてない課題に直面しています。セキュリティ・ツールの複雑さはリスクを高めるだけでなく、運用コストの増大、俊敏性の阻害、リソースの逼迫を招きます。こうした問題を受けて、アプリケーション・セキュリティ対策の合理化、組織の TCO 改善、およびリスク管理の強化に向けた戦略的アプローチとして「集約」が提唱されるようになっています。

集約による成果を確実に手に入れるには、以下に示す 3 つの手順に従うことを推奨します。

- ベンダーとツールを集約して TCO を改善する
- セキュリティ対策の工数を集約して AppSec プログラムを簡素化する
- セキュリティ分析情報を集約してリスク管理を強化する

自社にとって重要なセキュリティ・テストのニーズを強力なソリューション群で完全にカバーしてくれるベンダーとパートナーシップを結び、ASPM ソリューションを実装することによりツール、工数、セキュリティ分析情報を集約することで、より費用対効果に優れた堅牢なセキュリティ・プログラムを実施できるようになります。

シノプシスのソリューション

シノプシスは業界をリードするアプリケーション・セキュリティ・テスト（AST）ソリューションのポートフォリオを提供しており、組織における集約の取り組みを強力に支援します。シノプシスは SAST、DAST、SCA というテスト・ツールの「三種の神器」に加え、IAST、ファジング、モバイル・ペネトレーション・ソフトウェアなど幅広い種類のテスト・ツールを提供しています。シノプシスの AST ソリューションはオープンなエコシステムを提供し、135 種類を超える統合をサポートしているため、既に組織で導入済みのツールもより効率的に活用できます。シノプシスのセキュリティ・テスト・ソリューションは極めて柔軟性が高く、オンプレミス、SaaS、ヘッドレス API 環境のいずれにおいても高い効果を発揮します。現在使用しているソリューションは、シノプシス製であるかサードパーティ製、オープンソース、あるいは手動テスト・ソリューションであるかを問わず、すべてをシノプシスの ASPM ソリューションである Software Risk Manager に統合できます。シノプシスは、SDLC のあらゆるステージでプログラムを集約の成功に導く戦略的ソリューションを低コストで提供しています。

SYNOPSYS®

シノプシスの特色

シノプシスがご提供する統合型ソリューションは、ソフトウェア開発とデリバリのあり方を根底から変革し、ビジネス・リスクに対処しながらイノベーションを加速することを可能にします。シノプシスのソリューションにより、開発者はスピードを落とすことなくセキュアなコードを作成することができます。開発およびDevSecOps チームはスピードを犠牲にすることなく、開発パイプライン内でテストを自動化できます。セキュリティ・チームは先手を打ったリスク管理が可能となり、組織にとって最も重要な問題の修正に集中できます。シノプシスは業界随一のノウハウを活かし、最適なセキュリティ・イニシアティブの立案と実行をご支援します。信頼性の高いソフトウェアの構築に必要なものをワンストップでご提供できるのは、シノプシスだけです。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社
ソフトウェア インテグリティ グループ
〒158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス
TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software