DevSecOps

成功のための6つの柱

splunk>
turn data into doing®

今日のDevOpsの急速な広がりは驚くことではありません。DevOpsには、ソフトウェア開発ライフサイクル(SDLC)の短縮や、高品質なソフトウェアの継続的デリバリーなど、さまざまなメリットがあります。企業はクラウド利用を進め、DevOpsの導入は、成長と進化を加速させ、市場投入までの期間を短縮し、顧客の価値実現を早期化するための重要な手段です。

クラウドコンピューティングリソースが手軽に利用できるようになり、オープンソースのソフトウェアやコードリポジトリが普及したことで、企業のソフトウェア生産能力が向上し、多数の多様なプロジェクトの同時進行に対応できるDevOpsが魅力的なオプションとなりました。かつては、その本質がわからず敬遠されがちであったDevOpsは、今日広く理解され、主流の開発手法の1つになっています。独立系戦略コンサルティング/世論調査会社のClearPath Strategies社が2021年に米国と英国のクラウド購入意思決定者を対象に行った調査によると、62%の企業が全社的またはチーム単位でDevOpsを標準手法として導入しています。さらに28%の企業が、特定のチームでDevOpsを導入しています。

ただし、DevOpsにはセキュリティ面で課題もあります。それは、急速に進化し拡大し続けるサイバー攻撃に対して、その標的になり得る面が広がるなど、弱点が増えることです。この課題に対処するには、DevOpsプロセスの初期段階からより包括的にセキュリティを統合する必要があります。しかし問題は、従来のセキュリティ手法とDevOpsは互いに相いれないことです。この問題をきっかけに、セキュリティをDevOps手法の必須要素として組み込もうという機運が高まり、開発、セキュリティ、運用を連携させる新しい手法「DevSecOps」が誕生しました。

DevSecOpsの目標は、DevOpsのペースを落とすことなくセキュアなソフトウェアを提供することです。しかし、まだ発展途上の手法であり、組織の間で理解が進まず、実践に何が必要でどのように導入するのが効果的かに多くの組織が頭を悩ませています。このガイドでは、あらゆる規模の組織を対象に、DevSecOpsを定着させるために有効な戦略と戦術について説明します。ここで紹介する6つの柱を実践すれば、DevSecOps戦略を成功させ、早期に成果を出すための基盤を築くことができます。

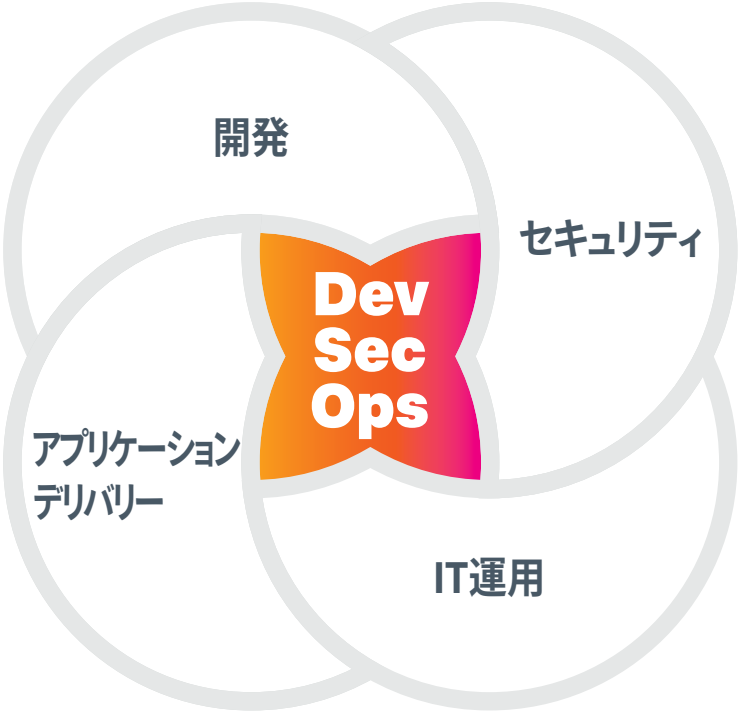
DevSecOps：
セキュリティを初期段階から組み込む

従来、セキュリティの責任は専門のチームが担い、開発サイクルの開始、終了、またはその両方のタイミングでアプリケーションの検査やストレステストを行ってきました。しかし、このようなセキュリティを後回しにするアプローチは、今日のDevOpsの足を引っ張ることになります。

DevSecOpsの基本的な考え方は、初期設計から、コーディング、テスト、デプロイ、稼働まで、DevOpsの開発サイクルのすべてのフェーズにセキュリティを組み込むことです。これにより、セキュリティの脆弱性をDevOpsサイクルの早い段階で発見して修正できるため、コードの品質向上と後段階での手戻りの削減につながります。

DevSecOpsの効果を高めるには、アプリケーションとその実行環境のセキュリティに対する責任を、セキュリティチームだけでなく、開発チームや運用チームを含むすべてのチームで分け合い、同じ目標に向かって協力し合うことが大切です。もちろんこれは口で言うほど簡単ではありません。何を最優先にするかはチームによって異なります。たとえば、開発チームにとってはコードのスピードと品質、運用チームにとってはアーキテクチャの安定性とレジリエンス(回復力)、セキュリティチームにとっては脆弱性対策の徹底、カバー範囲の広さ、保証が重要でしょう。DevSecOpsの成功とは、すべてのチームの目標を整合させて、これまでと同じかさらに速いペースで、かつセキュリティをより深く組み込みながら、アプリケーションを開発できるようにすることです。

今日、企業が競争力を維持するにはスピードが求められます。その点で、DevSecOpsの導入に最初に躊躇するのはおそらく開発者でしょう。理由は、DevOpsのペースを落としたくないか、セキュア開発の手法に慣れていないためです。しかし、正しく実践すれば、DevSecOpsはセキュリティチームだけでなく開発者にとっても、生産性の向上や高品質なプロダクトのオンタイムデリバリーなど、さまざまなメリットがあります。さらに組織全体にとっても、開発の迅速化と同時にリスクの軽減やセキュリティ態勢の強化を実現できるメリットがあるのです。



DevSecOps成功の6の柱

DevSecOpsのメリットは明らかですが、DevSecOpsを成功させることは容易ではありません。基本的にDevSecOpsは、専用の製品を導入すればできるというものではありません。新しいアプローチやツールセットを採用すると同時に、組織の文化やマインドセットを変えることが求められます。その中で、これまで独自のツールとワークフローを使用し、ときには独自のKPIを設定してきたチーム間のギャップを埋める必要があります。

DevSecOps戦略を効果的に実践するには、既存のシステムを利用しながら、古いプロセスやテクノロジーを排除し、必要に応じて新しいプロセスやテクノロジーを取り込んでいくことが欠かせません。さらに、開発チーム、運用チーム、セキュリティチームのニーズに配慮しながら、SDLCのすべての段階、そしてテクノロジースタックとアプリケーション自体のすべての層を見直す必要があります。

DevSecOps戦略の導入と定着を成功させるための6つの柱と、その実践を促進、加速するためのSplunkのアプローチを以下にご紹介します。

1 **組織の縦割り構造を見直す：**DevSecOpsを効果的に実践するには、まず、開発チーム、運用チーム、サイトリライアビリティエンジニアリング(SRE)チーム、セキュリティチーム間の壁を取り払い、セキュリティを共同責任として位置付ける必要があります。そして、すべてのチームに共通の目標とKPIを設定することが重要です。その際には、どのチームもある程度の妥協は避けられませんが、目標に優先順位を付け、セキュリティ的な「負債」を増やさないようにしながら優先度の高い目標の実現を目指すことで、新しい体制を受け入れられやすくなります。このような共同作業には、情報源を共有できるツールが欠かせません。

Splunkのアプローチ：Splunkは、すべてのチームに共通のプラットフォームと、セキュリティ、IT、DevOpsに特化したソリューションを提供して、縦割り構造の打破とコラボレーションの促進を後押しします。組織の規模を問わず、テクノロジー環境全体とそこで使用されるすべてのツールからデータを完全な忠実度で収集して統合します。データやレポートを共有することにより、重要なタスクの洗い出しと優先順位付け、共通のKPIの設定、進捗状況の追跡、DevOpsライフサイクルで反復すべきタスクの判断が容易になります。

2 **DevOpsチームやセキュリティチームの負担にならないように新しいセキュリティツールとプロセスを導入する：**DevSecOpsを導入するために既存の作業環境に新しいツールやプロセスを追加する際は、既存のワークフローに適合させる必要があります。セキュリティに携わってこなかった開発者が開発スピードを維持できるようにするには、セキュリティツールやプロセスを既存のDevOpsツールチェーンにシームレスに組み込んで、使い慣れた統合開発環境内ですべての作業ができるようにすることが大切です。同様に、既存のセキュリティワークフローやSOC業務にも新しいツールやプロセスを組み込んで、セキュリティチームとDevOpsチームが積極的に協力し合えるようにします。

Splunkのアプローチ：Splunkでは、規模を問わずテクノロジースタック全体のあらゆるソースのデータを統合することにより、開発チーム、セキュリティチーム、運用チームの既存のプロセスとワークフローで、コンテキストに即して状況を可視化できます。個々のチームに合わせた専用のデータ表示が用意されているだけでなく、チーム間で共有したい情報を集めたダッシュボードを作成することもできるため、リーダーは必要なメトリクスを包括的に把握できます。

3 自動化に重点を置く：

従来のアプリケーションセキュリティのアプローチでは、セキュリティ専門の担当者が開発プロセスの前後に重点的に検査を行うのが普通でした。こうしたアプローチは、俊敏性が高く継続的なフィードバックが必要なDevSecOpsプロセスには適しません。DevOpsと同様にDevSecOpsでも、スピードと精度を上げるため、そして合意された手順とベストプラクティスをすべてのチームが負担なく守れるようにするために、自動化を取り入れる必要があります。問題の発生時に状況を把握して迅速に修復を行うためにも自動化は欠かせません。自動化を導入する際は、正確で実用的な結果が得られるよう入念に計画することが大切です。システムに余計な負担をかけたり開発者が誤検知のアラートに煩わされることのないように注意が必要です。

不定期に行う必要があり、DevSecOpsプロセスの中で自動化できない作業については、反復可能なタスクを別個に作成し、結果をDevSecOpsプロセスと連携させるようなシステムを構築する必要があります。

Splunkのアプローチ：Splunkでは2つの方法で自動化ができます。1つ目は、SDLCで使用するさまざまなツールのデータをシームレスに関連付ける方法です。主要なツールに対応した事前構築済みのインテグレーションを利用できるほか、SplunkのAPIドリブンのアーキテクチャによってベンダー固有の特殊なツールとも接続できるため、連携は簡単です。この方法で自動化すれば、手動作業を減らし、同じ作業を繰り返し行う負担をなくして、新しいユースケースの開拓やイノベーションの促進に集中できます。

2つ目は、DevSecOpsに関連するより包括的な自動化機能を利用する方法です。問題を未然に通知する予測分析など、自動化機能の健全性や運用状況を可視化することで、ブラックボックス化したプロセスで生じる問題を緩和することもできます。

4 状況を継続的に可視化し、情報を共有する：

可視化とフィードバックは、機能の定義から本稼働までエンドツーエンドで、プロセスの進行に合わせたスピードでコンテキストに即して提供することが重要です。さらに、開発チームも運用チームも、チケットシステムやSlack通知など、それぞれ使用するツールチェーンと既存のプロセス内でこれらの情報を確認できるようにする必要があります。もちろん、セキュリティチームも独自のプロセスとツールチェーン内で、必要なすべてのメトリクスを把握できるようにします。これにより、本番環境でセキュリティの問題が発生したときに、必要なすべての情報にアクセスし、開発チームや運用チームと協力して対応できます。

Splunkのアプローチ：Splunkでは、すべてのツールとテクノロジースタックからデータを収集できるため、アプリケーションやその実行基盤をコンテキストに即して可視化できます。また、プロセスの個々のステージがパイプライン全体の中でどのようにつながっているかを可視化することもできます。さらに、内蔵のAI/機械学習によって実用的なインサイトを導出して、開発、運用、セキュリティのワークフローを効率化できます。リスクベースのアラートなどの機能を利用してインシデントに優先順位を付け、アラート数を抑制すれば、セキュリティ対応に関する開発者の負担を軽減できます。

5 **セキュリティ上のすべての脆弱性を品質欠陥として扱う：**多くの組織は、セキュリティに関するデータと品質に関するデータを別々に管理しています。この方法では全体の可視性が低下するだけでなく、セキュリティに関する欠陥に開発者が無関心になりがちです。この問題を解決するには、セキュリティデータと品質データを1カ所で管理する必要があります。これにより、セキュリティに関する状況を正確に把握して情報を共有できるようになり、開発チームが品質の問題とセキュリティの問題を同等に扱うように促すことができます。

Splunkのアプローチ：Splunkでは、DevOpsとセキュリティのツールチェーン全体からデータを収集し、統合的な共有ダッシュボードで情報を可視化できます。これにより、共通リポジトリにアクセスして、セキュリティや品質に関する欠陥をリアルタイムで正確に把握できます。このように情報を共有することにより、関係チームすべての意見を基にセキュリティ上の重大な欠陥に早期に対処して、コストのかかる本稼働直前での手戻りを避けることができます。

6 **インシデント後対応の戦略を拡大/強化する：**本番環境でセキュリティの問題が発生するのは避けられませんが、機能の定義時点からコンテキストに即して状況を可視化できれば、原因を迅速に特定できます。また、クラウドアーキテクチャはエフェメラル(短命)な性質があるため、すべてのサービス間のすべてのやり取りを完全な忠実度で追跡できるようにすることも重要です。インシデントの対応と解決を特定のチームに割り当てる場合でも、他のチームとの協力は必要になるでしょう。共通のツールを使用し、可視化した情報を共有していれば、より適切かつ迅速に問題を解決できます。

Splunkのアプローチ：Splunkでは、開発プロセスのデータだけでなく、すべてのインシデントデータを可視化し、内蔵のツールでインシデント対応を効率的に行うことができます。これにより、最前線で対応に当たるSREは、セキュリティインシデントの分析に必要なすべてのデータにアクセスできます。また、適切な担当者にアラートを転送し、対応の担当者を割り当てて、ケースの状態と進捗を追跡することもできます。セキュリティ担当者にケースが割り当てられると、SREが実行したフォレンジック調査のすべてのデータが担当者に自動的に引き継がれるため、同じ作業の繰り返しを避けることができます。さらにSplunkでは、プロセスを機能の定義時点からエンドツーエンドで可視化できるため、セキュリティ担当者は開発者の手を煩わせることなくインシデントの詳細を把握できます。開発者は、解決に直接かかわっていなくてもその状況を把握できるため、自身が書いたコードが本番環境のセキュリティにどのような影響を与えているかを理解し、今後のプロジェクトでのセキュリティ要件の定義と優先順位付けに活かすことができます。

DevSecOpsのユースケース

DevSecOpsの活用方法は幅広く、業界や業種によってもさまざまです。とはいえ、主なユースケースは、開発環境の保護、よりセキュアなアプリケーションの開発、本番環境でのアプリケーションの保護の3つに絞り込むことができます。

1 **開発環境の保護：**DevOpsのツールチェーンで安心して作業を行うには、開発環境のセキュリティとレジリエンスを確保する必要があります。しかし、DevOpsのツールチェーンには、固有の機能を提供するさまざまなポイント型製品が含まれます。さらに、オープンソースの開発ソフトウェアを使用する機会や、疎結合かつエフェメラルなアーキテクチャパターンを採用する例が増えているため、環境の複雑化が進んでいます。

Splunkがもたらすメリット：Splunkなら、異なる多数のツールのテレメトリを相関付けて、AI/機械学習を使用してデータパターンを分析し、リスクベースの理解しやすいアラートを生成できます。これにより、開発者がどのツールを使用していてもセキュリティポリシーに準拠していることを確認できるとともに、誤検知アラートのノイズを最小限に抑えることができます。また、Splunkではインシデント対応を自動化することもできるので、修復作業を効率化できます。

2 **よりセキュアなアプリケーションの開発：**よりセキュアなアプリケーションを開発するには、アプリケーションのコンポーネントだけでなく、アプリケーションが依存するクラウドサービスやOSSライブラリを含むすべての層でセキュリティに配慮する必要があります。その対象には、アプリケーションのカスタムコード、サービス間のAPIインテグレーション、開発/デプロイイメージ、コードを実行するインフラ(最近ではますます多くの場合クラウドやコンテナ)なども含まれます。

Splunkがもたらすメリット：Splunkなら、すべての層のログをリアルタイムで収集して、機能の定義からリリース、さらには本番環境のセキュリティインシデントまで、アクティビティパイプライン全体を追跡できます。コンテキストに即した詳細な可視化によって得られる情報は、リアルタイムの共有ダッシュボードでも既存のツールからでも確認できます。そのため、開発者は、よりセキュアなコードを書くだけでなく、開発中にポリシー違反やセキュリティ違反を検出してすばやく対応することもできます。また、チーム間で共通の認識を持つことにより、最適なコーディング規約を作成し、SDLC全体でその準拠状況を追跡、測定できます。

3 **本番環境でのアプリケーションの保護：**デプロイ後にセキュリティインシデントが発生したときは、通常、SREとセキュリティチームが修復の責任を担います。ただし、開発ペースが速いことに加えて、開発者が開発サイクルと本稼働サイクルの両方のステージを広範に理解する必要があるため、問題を効果的に修復するのは困難になりがちです。

Splunkがもたらすメリット：Splunkなら、アクティビティパイプライン全体を追跡して、セキュリティ調査とインシデント解決の両方を迅速に行うことができます。これらのプロセスを効率化すると同時に、開発チーム、SREチーム、セキュリティチーム間の無駄なやり取りをなくすことができます。

データの時代の成功に不可欠なDevSecOps

サイバー脅威が進化し続ける中、企業の間でセキュリティに対する関心がますます高まっています。さらに企業は、アプリケーションの開発とリリースのペースを上げなければ、適応力や俊敏性の高い企業に後れを取り、競争から取り残されるという重圧にさらされています。

DevOpsのペースを落とすことなくソフトウェア開発ライフサイクルにセキュリティテストを組み込むDevSecOpsは、その両方の課題に対する答えをもたらします。DevSecOpsでは開発の初期段階からセキュリティのリスクと脆弱性に対応するため、発見や修復が遅れるほどダメージやコストが増す問題を早期に緩和したり、場合によっては完全に回避することができます。また、DevSecOpsで「継続的セキュリティ」を実現することで、資産を24時間365日、常に保護できます。

Splunkは、エンドツーエンドの可視化、ワークフローに沿った適切なデータの提供、セキュリティとDevOpsのワークフローへの新しいツールやプロセスの適合を通じて、この新しいDevSecOpsアプローチの導入と定着を支援します。包括的なアプローチにより、既存のDevOpsプロセスだけでなくセキュリティチームやSOCでのセキュリティ業務とも適切に連携します。

将来的には、DevSecOpsは開発プロセスで存在感を増すだけでなく、組織全体の能力を高めてデータの時代に成功を勝ち取るために欠かせないプラクティスになる可能性があります。DevSecOps文化の構築と定着は一夜にして成し遂げることはできませんが、DevSecOpsを前提に開発パイプラインを見直すことは、生産性の向上、リスクの軽減、全体的なセキュリティ態勢の強化につながります。

DevSecOpsの導入におけるSplunkのメリットについて
詳しくは、Splunkまでお問い合わせください。

詳細はこちら

splunk> turn data into doing®

21-21001-Splunk-6 Pillars of a Successful DevSecOps Practice-LS-JA-202204