SYNOPSYS®

世界の DevSecOps の現状 2023

ソフトウェア・セキュリティに影響を及ぼす戦略、ツール、プラクティス

概要
2023 年シノプシス DevSecOps レポートについて
DevOps と DevSecOps について
自動化によるメリット
DevSecOps における ASOC/ASPM 使用の増加
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

概要

シノプシス DevSecOps レポートについて

2023 年前半、シノプシス Cybersecurity Research Center (CyRC) と国際的な市場調査会社 Censuswide は、セキュリティを職務または職責に含む 1,000 人の IT 専門家を対象にした調査を実施しました。調査対象のグループには、開発者、アプリケーション・セキュリティ専門家、DevOps エンジニア、CISO に加え、テクノロジー、サイバーセキュリティ、アプリケーション / ソフトウェア開発でさまざまな職務に携わるエキスパートが含まれました。また、米国、イギリス、フランス、フィンランド、ドイツ、中国、シンガポール、日本から回答が得られました。

業種と規模を問わず、あらゆる企業に属する回答者が調査対象となりました。調査開発時に直面した課題の 1 つは、「DevSecOps」という用語にはさまざまな領域が含まれ、その多くが独自のペルソナを含むことでした。この調査では、コードを作成する「実践的な」開発者や CISO レベルの個人などを含む幅広い専門家を含め、業務上何らかの観点でソフトウェア・セキュリティにかかわる個人を対象とすることを目指しました。

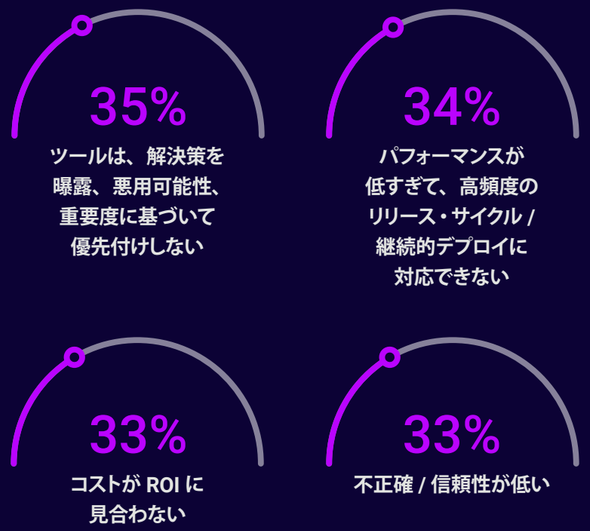
DevOps と DevSecOps について

DevOps の主な原則 (開発の加速、継続的デリバリー、パイプラインのレジリエンス、スケーラビリティ、エンドツーエンドの透明性) を達成するには、開発、セキュリティ、運用分野の専門家による協調的な取り組みが必要です。

DevOps の拡張版である DevSecOps は、チーム全体にセキュリティ文化を浸透させて、DevOps 環境内で早い段階から一貫してセキュリティに対処するためのメソドロジーです。DevSecOps の目的は、ソフトウェア開発ライフサイクル (SDLC) と CI パイプラインにセキュリティ・プラクティスを組み込むことにより、セキュリティを、切り離され、独立したフェーズから開発ライフサイクルの不可欠な要素へとシフトすることです。

DevSecOps はこれまでに、ソフトウェア開発関連のあらゆる組織で大きな支持を獲得しています。SANS 2023 DevSecOps survey によると、現在、DevSecOps は間違いなくビジネスに不可欠なプラクティスであり、リスク管理上の考慮事項であると見なされています。しかし、開発プロセスへのセキュリティ導入を試みると、多くの場合、従来のアプリケーション・セキュリティ・テスト (AST) を SDLC に持ち込んだ結果ですが、歴史的に、多くの場合セキュリティ・チームと開発チームは意見が一致しませんでした。また、よく聞かれる不満には、AST ツールは複雑で習得すべき事項が多く、パフォーマンスも不十分だというものや、結果に「ノイズが多い」ために DevOps の「摩擦」(ソフトウェア作成プロセスで、開発者が素早く簡単にコードを作成するのを妨げるすべての要素) が引き起こされるというものがあります。

回答者の大部分が、使用中の AST ツールに関する一般的な不満として以下を回答



概要

2023 年シノプシス DevSecOps レポートについて

DevOps と DevSecOps について

自動化によるメリット

DevSecOps における ASOC/ASPM 使用の増加

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

調査結果からの学び

調査対象者の属性

付録

自動化によるメリット

DevOps の核となる原則は、SDLC の各段階で手動プロセスを自動化することです。自動化は、どのような組織にとっても、継続的インテグレーションまたは継続的デプロイを実装してコードの開発とデリバリーを迅速化するための基本要件となります。

DevOps を成功させるには、統合と自動化の相互作用が必要であり、これらは標準とポリシーによって管理されなければなりません。こうすることで、セキュリティ・チームはセキュリティ面が考慮されていると信用でき、DevOps チームは業務を継続し、開発パイプラインに想定外の中断が生じないと確信を持てます。

手動でのテストとは異なり、自動化されたセキュリティ・テストは一貫性をもって素早く実行できるため、開発者はデリバリー・スケジュールや生産性に影響を与えることなく、開発プロセスの早い段階で課題を特定できます。

一貫性

自動テストにより、すべてのビルドとデプロイにセキュリティ・チェックが常に適用されます。手動テストでは、テストの手順と範囲にばらつきが生じる可能性があります。

スケーラビリティ

ソフトウェアが複雑になるにつれて、手動テストは現実的ではなくなりますが、自動テストは、さまざまなコンポーネントにわたる多数のテストを処理するために容易に拡張できます。

継続的インテグレーションと継続的デプロイ (CI/CD)

自動テストは、コードの変更が迅速かつ頻繁にデプロイされる CI/CD パイプラインにおいては非常に重要です。自動テストにより素早く変更を検証することで、不完全なコードが本番環境に移行されることを防止できます。

継続的改善

自動テストにより、チームが時間をかけてセキュリティ・プラクティスの改善に役立つデータと知見が得られ、脆弱性のパターンを体系的に分析して対処できます。

文書化

自動テストはテスト手順を文書化するため、セキュリティ対策とコンプライアンス要件の追跡および監査が容易になります。

人的ミスの削減

手動テストでは、疲れや見落としによってエラーが発生しやすくなります。自動テストは事前定義されたスクリプトに従って実行されるため、人的ミスのリスクが軽減されます。

時間とコストの節約

開発プロセスの終盤や本番環境に移行してからセキュリティの課題を特定して修正すると、大幅な時間とコストがかかる場合があります。自動テストはこのようなコストを最小限に抑えます。

開発者のエクスペリエンスの改善

自動化されたアプリケーション・セキュリティ・テストでは、セキュリティの考慮事項に対処するための、積極的で統合された教育的なソリューションを提供することで、開発者のエクスペリエンスを向上させます。これは最終的に、よりセキュアなソフトウェアと、より効率的な開発プロセスにつながります。

概要
2023 年シノプシス DevSecOps レポートについて
DevOps と DevSecOps について
自動化によるメリット
DevSecOps における ASOC/ASPM 使用の増加
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

DevSecOps における ASOC/ASPM 使用の増加

本レポートでは、DevSecOps の成熟度のさまざまな段階にある組織特徴と、組織が使用するセキュリティ・ツール / プラクティスの特性を調査しています。調査結果に基づき、より高いセキュリティ成熟度を達成しようと取り組む組織に対して、規範的な推奨事項を提供します。

調査結果に見られた興味深いデータ・ポイントは、アプリケーション・セキュリティのオーケストレーションと相関付け (ASOC) の使用が増加していることです。これは現在、アプリケーション・セキュリティ態勢管理 (ASPM) と呼ばれることが一般的で、ガートナーは、複数の開発ツールやセキュリティ・ツールを使用する組織にとって、ASPM は優先事項である必要があるとしています。

ASPM ソリューションは、開発からデプロイまでにわたるセキュリティの課題を検出、相関付け、優先順位付けすることで、継続的にアプリケーション・リスクを管理します。ASPM ツールは、さまざまなソースからデータを取り込んで互いに関連付け、結果を分析することで、解釈、トリアージ、修正を容易にします。

ASPM は、セキュリティ・ツールの管理およびオーケストレーション層としての役割も果たし、セキュリティ・ポリシーの制御と適用を可能にします。アプリケーション・セキュリティの検知結果を統合したビューが提供されるため、アプリケーションまたはシステム全体のセキュリティおよびリスク状態を包括的に把握できます。

1,000 人の回答者の大半が、使用中の AST ツールに関する全般的な不満を挙げています。これらのツールは、修正がビジネス・ニーズに基づいて優先付けされない (35%)、課題解決のための結果の統合 / 相関付けができない (29%) といった評価が含まれており、ASOC/ASPM の使用が急速に増えていることも頷けます。

概要

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

調査結果からの学び

調査対象者の属性

付録

2023 年シノプシス DevSecOps 調査からの主な発見事項

DevOps チームの大半が一定レベルの DevSecOps を採用済み

合計で 91% の回答者が、ある程度の DevSecOps アクティビティをソフトウェア開発パイプラインに取り入れていると回答しました。DevSecOps メソドロジーの採用は、ソフトウェア開発の一部として定着したと言って差し支えないでしょう。

成熟度の高いセキュリティ・プログラムの導入組織は、セキュリティに特化した要員を配置

29% の回答者が、セキュリティ・プログラムの成功にとって、部門横断的な DevSecOps チーム (開発、セキュリティ、運用担当者による協調的なグループ) が重要な要因であると回答しました。成熟したセキュリティ・プログラムを持つ組織では、セキュリティに特化した要員が、開発者 / ソフトウェア・エンジニアおよび / または QA およびテスト部門と協力しながら、セキュリティ・テストの最前線に立つと見られます。

DevSecOps の効果的な実装に立ちはだかる多くの障壁

33% を超える回答者が、主な阻害要因としてセキュリティ・トレーニングが不十分であることを挙げました。続いて、セキュリティ要員の不足 (31%)、開発 / 運用作業の透明性の欠如 (31%)、絶えず変化する優先順位 (30%) が挙げられました。

3 分の 1 を超える回答者が、ビルド / デプロイ・ワークフローへの自動セキュリティ・テストの組み込みがセキュリティ・プログラム成功の鍵となると指摘

その他の重要な要因には、インフラストラクチャ・アズ・コードを介したセキュリティ / コンプライアンス・ポリシーの適用、開発および運用チームでのセキュリティ・チャンピオンの育成、開発、運用、セキュリティ・チーム間でのコミュニケーションの改善が含まれました。

SDLC 終盤での重大な脆弱性への対処が収益に大幅な影響

80% を超える回答者が、2022 年から 2023 年にかけて、デプロイ済みソフトウェアに含まれる重大な脆弱性 / セキュリティの課題がデリバリー・スケジュールに何らかの影響を及ぼしたと述べました。

28% の回答者が、デプロイ済みアプリケーションでの重大なセキュリティ・リスク / 脆弱性へのパッチ適用に 3 週間もかかると回答し、他の 20% は最大 1 か月かかると回答

かつてなく短期間で脆弱性が悪用されているため、これらの数字はことさら憂慮すべきです。最新の調査では、報告された脆弱性の半数を大幅に超える脆弱性が公開後 1 週間以内に悪用されています。

70% を超える回答者が、自動スキャンによるコードの脆弱性やコーディングの不具合の検出を有益なセキュリティ対策だと述べ、34% は自動化された AST を「非常に有益」と回答

「ツール / プロセスの有用性」カテゴリで最も多かったのは、自動化されたコード・スキャンによる脆弱性とその他の不具合の検出であり、「SDLC 要件段階の一部としてのセキュリティ要件定義」と「BSIMM および SAMM などのモデルを使用した、ソフトウェア・セキュリティ・プログラムの正式な測定」が続きました。

ほぼすべての回答者が、AST ツールはビジネス・ニーズに適合しないことに同意

1,000 人の回答者の大半が、AST ツールのさまざまな課題を主要な問題として挙げました。挙げられた課題には、修正がビジネス・ニーズに基づいて優先付けされない (35%)、課題解決のための結果の統合 / 相関付けができない (29%) を含みます。

52% のセキュリティ専門家はすでに DevSecOps のプラクティスで AI を積極利用しているが、4 分の 3 を超えるセキュリティ専門家が AI 利用に関する問題を懸念

調査結果は、AI、機械学習、自然言語処理、ニューラル・ネットワークがセキュリティ・チームによって積極的に使用されていることを示しています。しかしながら、AI を利用したコーディング提案などの生成型 AI ツールには、IP 所有権、著作権、AI が生成したコードのライセンス供与に関して疑問が生じ、場合によっては訴訟が引き起こされています。

概要

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

DevSecOps の採用

セキュリティ・プラクティスの実装は成熟度レベルの高さを示す

セキュリティ・プログラムの測定

DevSecOps の成功における部門横断的チームの重要性

最善の結果を得るための手動テストと自動テストの組み合わせ

重要業績評価指標 (KPI)

使用している AST ツールとその有用性

テストおよびパッチのタイミングとスケジュールへの影響

効果的な DevSecOps を妨げる課題

AI への期待と落とし穴

調査結果からの学び

調査対象者の属性

付録

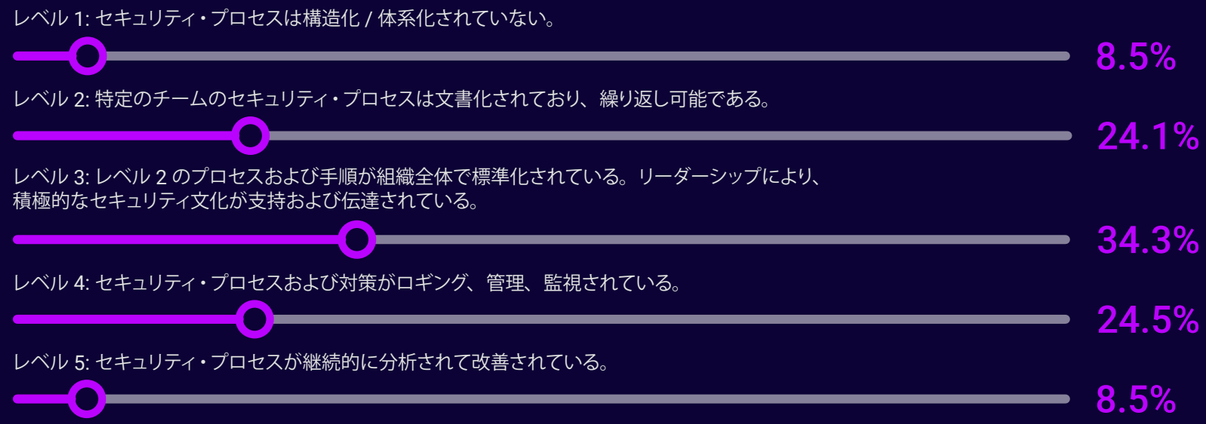
2023 年の DevSecOps の現状

DevSecOps の採用

1,000 人の回答者のうち 3 分の 1 を超える回答者が、自社のセキュリティ・イニシアティブを成熟度段階のレベル 3 であると評価しました。レベル 3 は、セキュリティ・プロセスが文書化され、繰り返し可能であり、組織全体で標準化されています。また、25% はレベル 4 に到達したと認識しています。レベル 4 は、セキュリティ・プロセスがロギングされ、監視しており、評価できている状態です。

合計で 91% の回答者が、ソフトウェア開発パイプラインに何らかの DevSecOps アクティビティを適用したと報告していることから、DevSecOps の採用は、DevOps の一部として定着したと見なされます。

図 A 現在使用しているソフトウェア・セキュリティ・プログラム / イニシアティブに最も当てはまる成熟度はどれですか



概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

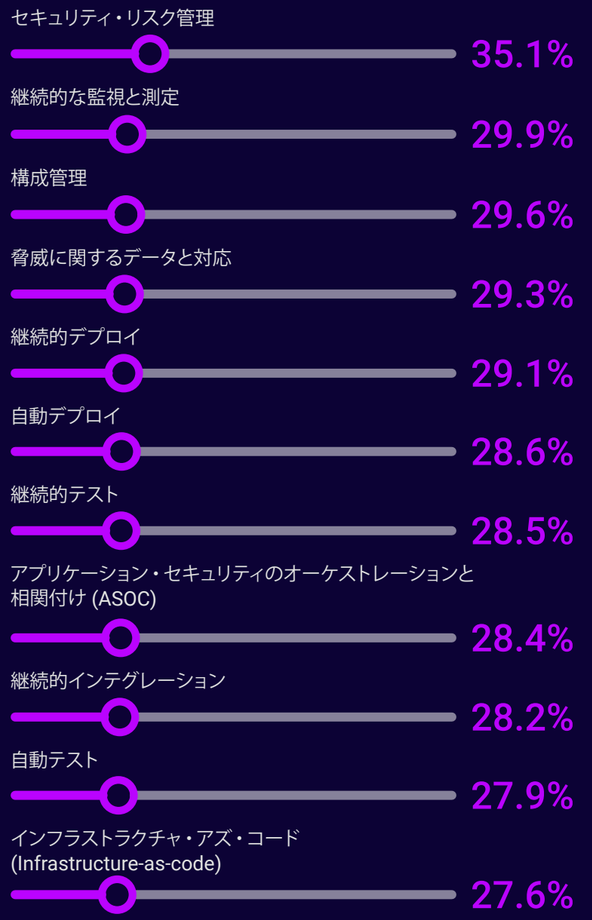
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す

図 B に DevSecOps の成熟度に対する別の測定結果が確認できますが、継続的な監視と測定 (30%) から自動テスト (28%) まで、さまざまなセキュリティ・プラクティスを回答者が採用していることがわかります。

最も採用されているプラクティスとして 358 人の回答者 (35.1%) が挙げたセキュリティ・リスク管理では、開発プロセスのすべての段階でセキュリティ上の考慮事項を統合することで、ソフトウェア・アプリケーションに関連する潜在的なセキュリティ・リスクが特定、評価、軽減されます。SDLC に適用される総合的なセキュリティ・リスク管理には以下が必要です。

- **要件の分析：**SDLC の早期にセキュリティ要件および制約事項を特定し、セキュリティ目標を定義する。
- **設計：**セキュリティ原則をシステム・アーキテクチャおよび設計に取り入れることで、一般的な脆弱性に対する適切な予防措置がアプリケーションの設計に含まれるようにする。
- **開発：**セキュア・コーディング・プラクティスを実装し、セキュリティの考慮事項に対処したコーディング標準に準拠する。静的アプリケーション・セキュリティ・テスト (SAST) やソフトウェア・コンポジション解析 (SCA) などの統合セキュリティ・テスト・ツールを使用して、コードが作成され、オープンソースまたはサードパーティのコンポーネントとの依存関係が取り込まれた時点で脆弱性を検出する。
- **テスト：**SAST や動的アプリケーション・セキュリティ・テスト (DAST)、SCA、ペネトレーション・テストなどの各種セキュリティ・テストを実行し、アプリケーション内の脆弱性を特定する。
- **デプロイ：**アプリケーションが実行される環境をセキュアに構成する。アクセス制御、ネットワーク・セキュリティ、適切な認証および認可メカニズムを実装する。
- **監視と測定：**本番環境のアプリケーションを継続的に監視して、セキュリティ・インシデントと異常を検出する。ロギングおよび監視ソリューションを実装して、潜在的な侵害を検出してこれに対応する。調査回答者の 30% が、組織の主なセキュリティ・プラクティスとしてこれを挙げた。
- **対応と修正：**セキュリティ・インシデントに素早く効果的に対処するためのインシデント対応計画を作成する。テスト・フェーズで検出されたリスクを修正する。
- **透明性とセキュリティの確保：**セキュリティ・リスクおよびリスク許容度の明確な標準、基準、ポリシー、レポートを規定する。
- **トレーニング：**セキュアなコーディング・プラクティス、一般的な脆弱性、セキュリティ・ベスト・プラクティスに関するトレーニングを開発チームに提供する。これにより、開発者がセキュリティの考慮事項に対して積極的に対処できるようになる。残念ながら、34% の調査回答者が、組織での効果的な DevSecOps の実装を妨げる主な要因として「開発者 / エンジニア向けのセキュリティ・トレーニングが不十分 / 非効果的」を挙げた。
- **継続的改善：**SDLC に含まれるセキュリティ・プロセスおよびプラクティスを定期的にレビューして改善する。

図 B 現在使用しているプラクティスはどれですか (当てはまるものをすべて選択)



概要

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

- DevSecOps の採用
- セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
- セキュリティ・プログラムの測定
- DevSecOps の成功における部門横断的チームの重要性
- 最善の結果を得るための手動テストと自動テストの組み合わせ
- 重要業績評価指標 (KPI)
- 使用している AST ツールとその有用性
- テストおよびパッチのタイミングとスケジュールへの影響
- 効果的な DevSecOps を妨げる課題
- AI への期待と落とし穴

調査結果からの学び

調査対象者の属性

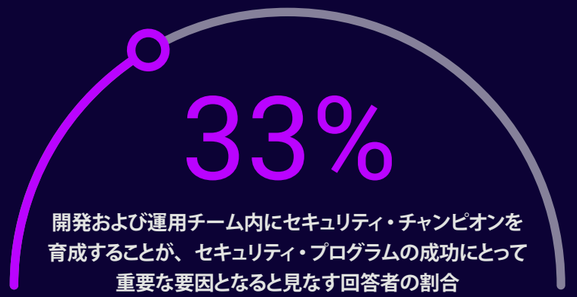
付録

セキュリティ・プログラムの測定

回答者の 70% 近くが、セキュア開発成熟度モデル (BSIMM) などの評価ツールによるセキュリティ・プログラムの測定は有益だとしており、3 分の 1 を超える回答者が「非常に有益」だと述べています。

セキュリティ態勢を外部から評価することで、自組織のソフトウェア・セキュリティ・プログラムを分析し、その他の組織や業界他社と比較しベンチマークを行うことができます。BSIMM などのツールで提供されるのはデータ・ドリブンで客観的な分析であるため、これに基づいて、リソース、時間、予算、優先順位を決定できます。セキュリティ・プログラム実装の早い段階にある場合も、既存のプログラムで変化するビジネス・ニーズとセキュリティ・ニーズに確実に対応できることを確認したい場合も、他のソフトウェア・セキュリティ・プログラムを自社のプログラムと比較することで、取り組みにおける戦略を方向付けることができます。

ソフトウェア・セキュリティ・プログラムの責任を負っている、または構築を開始しようとしている場合、業界のアプリケーション・セキュリティのトレンドを理解しておくことは、自社のセキュリティの取り組みに対する戦略的改善を計画するのに役立つでしょう。セキュリティ・プログラムを技術面から実行している場合は、BSIMM またはソフトウェア保証成熟度モデル (SAMM) の評価によって収集した情報を使用して、セキュリティ・チャンピオン・プログラムの構築などにより、人材とプロセスの戦術的改善を定義できます。

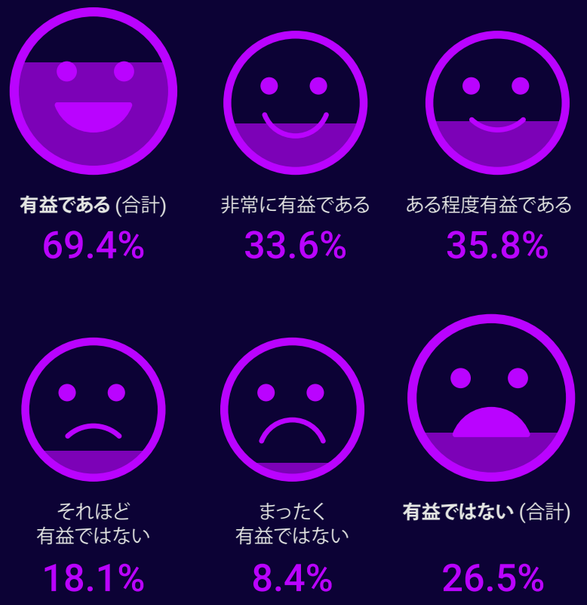


開発および運用チーム内にセキュリティ・チャンピオンを育成することが、セキュリティ・プログラムの成功にとって重要な要因となると見なす回答者の割合

実際、BSIMM レポートによると、多くのソフトウェア・セキュリティ・グループが取り掛かる最初のイニシアティブの 1 つは、ソフトウェア・セキュリティの推進役ではあるが、ソフトウェア・セキュリティ・グループと直接のつながりはない個人を特定することです。総称して「ソフトウェア・セキュリティ・チャンピオン (推進リーダー)」と呼ばれるこれらの人々は、ソフトウェア・セキュリティの取り組みを実現し、関心を集めることのできる人々です。

たとえば、エンジニアリング・チームのセキュリティ・チャンピオンは、ソフトウェア成果物のセキュリティに当事者意識を持つようにエンジニアに促すことができます。セキュリティ・プログラムを成功させるための重要要因としてセキュリティ・チャンピオン・プログラムの開発を挙げた回答者は 33% でした。

図 C BSIMM、SAMM などのモデルによるソフトウェア・セキュリティの正式な測定の有用性



概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

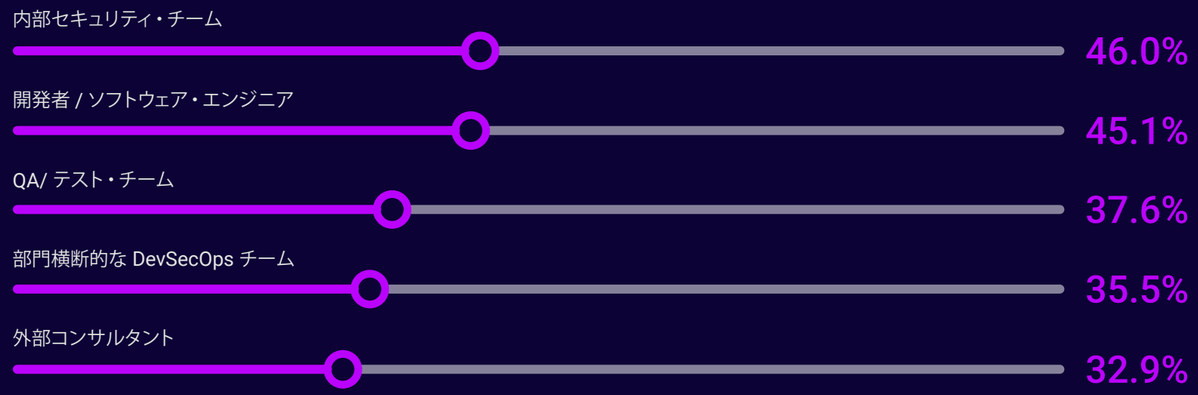
DevSecOps の成功における部門横断的チームの重要性

調査回答者の 29% が、セキュリティ・プログラムの成功にとって、部門横断的な DevSecOps チーム (開発、セキュリティ、運用による協調的グループ) が重要な鍵であると指摘しました (付録 Q16 参照)。より成熟したセキュリティ・プログラムを持つ組織では、セキュリティに特化した要員が、開発者 / ソフトウェア・エンジニアおよび / または QA およびテスト・チームと協力しながら (正式に DevSecOps グループに属するかどうかにかかわらず)、セキュリティ・テストの最前線に立つと見られます。

融通のきかない縦割りのセキュリティ・チームがデプロイ直前 (またはデプロイ後) にテストに介入するというやり方は、すでに廃れています。現在のソフトウェア開発環境では、QA、開発、運用を含むエンジニアリング・チーム全体がセキュリティ・テストの責任を負い、大半のメンバーが、さまざまな SDLC 段階で各自のソフトウェアにセキュリティを取り入れる役割を担います。

回答者の 33% が、組織のセキュリティ・テストは外部コンサルタントによっても実施されていると回答しました。定期的なセキュリティ監査の実施は、ベスト・プラクティスとして推奨されています。こういったテストをサードパーティの監査人やペネトレーション・テスターと契約して実施することは、組織のセキュリティ態勢を先入観抜きで把握するのに大変有益になり得ます。

図 D 組織内でセキュリティ・テストの実施責任を負っているのは誰ですか (当てはまるものをすべて選択)



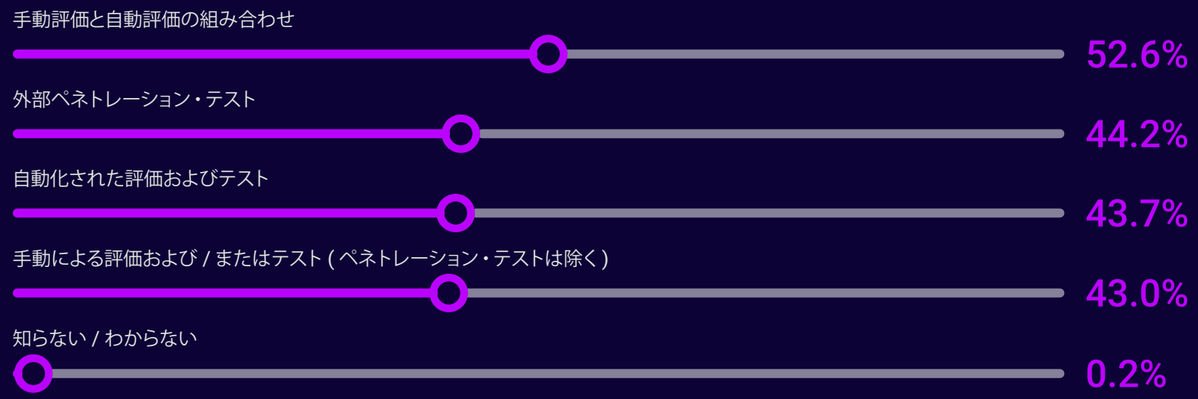
概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

最善の結果を得るための手動テストと自動テストの組み合わせ

調査結果によると、回答者の大半が、ビジネスに不可欠なアプリケーションのセキュリティを評価する際、手動および自動のセキュリティ・テストを組み合わせることでより包括的なアプローチが得られると考えています。一貫性、スケーラビリティ、時間とコストの節約を実現するために自動テストが重要であるのと同様に、複雑でとらえにくいセキュリティ課題を特定するために欠かせない知見と適応性は、人的な要因によってもたらされます。例を挙げると、「ブラック・ボックス」テスト (アプリケーションの内部構造に関する知識なしで実施するテスト) としての DAST の特性を活かすには、開発者とセキュリティ・エキスパートによる検証と結果のトリアージが必要です。

同様に、セキュリティ・テストの重要な要素として、外部ペネトレーション・テストを挙げた回答者が 44% いるという事実から、内部でのテストを補完する役割としてのペネトレーション・テストの重要性が示されています。業界の規制および標準に準拠するために義務付けられることの多い外部ペネトレーション・テストですが、組織のセキュリティ態勢に関して先入観のない観点が得られる、外部攻撃者による悪用の可能性がある潜在的脅威と脆弱性を正確にシミュレートできる、といったメリットもあります。

図 E ビジネスに不可欠なアプリケーションのセキュリティをどのような方法で評価またはテストしていますか (当てはまるものをすべて選択)



概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

重要業績評価指標 (KPI)

今回の調査では、回答者に対して、組織の DevSecOps プログラムの成功を評価するために使用している KPI の上位 3 つを選ぶように依頼しました。非常に重要な KPI として、295 人 (29%) の回答者がオープンな脆弱性の全体的な削減を挙げており、288 人 (28%) の回答者が SDLC 終盤でのセキュリティ関連の発見を僅差で選んでいます。上位 3 つの KPI の最後は課題解決までの時間で、281 人 (28%) の回答者に選ばれています。

調査結果からわかるように、時間、生産性、コストの 3 つが上位 KPI における共通事項であり、セキュアな SDLC の実装時に組織が対処すべき課題でもあります。

別の言い方をすると、DevSecOps 関係者が直面する主な質問は以下の 3 つになります。

- どうすれば、直面する脆弱性 / 課題の数を減らせるか
- SDLC のより早い段階で脆弱性を検出するためには何ができるか
- ビルド遅延を削減し、開発者の生産性を上げるために、どうすれば課題解決までの時間を短縮できるか

図 F DevSecOps アクティビティの成功を評価するために使用している主な KPI はどれですか (最大で 3 つまで選択)

概要

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

DevSecOps の採用

セキュリティ・プラクティスの実装は成熟度レベルの高さを示す

セキュリティ・プログラムの測定

DevSecOps の成功における部門横断的チームの重要性

最善の結果を得るための手動テストと自動テストの組み合わせ

重要業績評価指標 (KPI)

使用している AST ツールとその有用性

テストおよびパッチのタイミングとスケジュールへの影響

効果的な DevSecOps を妨げる課題

AI への期待と落とし穴

調査結果からの学び

調査対象者の属性

付録

使用している AST ツールとその有用性

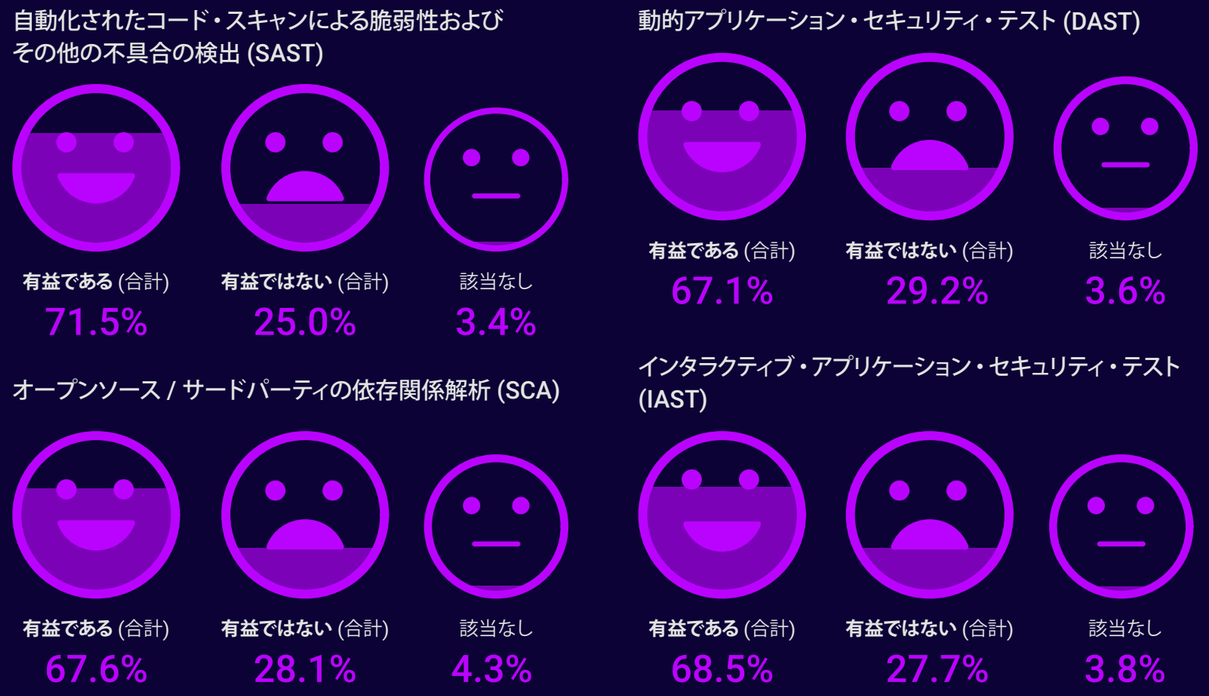
調査結果から、順調な DevSecOps 戦略ではセキュリティ・ツールセット一式が使用されていることが示されました。これには、動的アプリケーション・セキュリティ・テスト (DAST)、インタラクティブ・アプリケーション・セキュリティ・テスト (IAST)、静的アプリケーション・セキュリティ・テスト (SAST)、ソフトウェア・コンポジション解析 (SCA) ツールが含まれ、ソフトウェア開発ライフサイクル全体を通じてコード品質とセキュリティ上の欠陥に対応するために使用されています。

回答者が最もよく使用している AST ツールは SAST で、72% が有益だと感じています。続いて、IAST (69%)、SCA (68%)、DAST (67%) が挙げられています。

SAST と DAST は異なるテスト・アプローチを用いており、それぞれ異なる SDLC フェーズで最大の効果を発揮します。SAST は、アプリケーションがデプロイされる前の SDLC の早い段階で自前のソフトウェアに含まれる脆弱性を発見して解消するために非常に重要です。その一方で、DAST はデプロイ後、認証やネットワーク構成の不備など、実行時に生じる課題を特定するために使用されます。SAST と DAST の両方の機能の一部を組み合わせた IAST は、その他の種類のテストでは見つからない重大なセキュリティ上の欠陥を検出するために使用されます。

SCA は、オープンソースのセキュリティおよびライセンス・リスクを識別して管理するために使用されます。これは特に、いかなるアプリケーションでも 4 分の 3 を超えるコードがオープンソースである可能性が高いことを考えると、現在のソフトウェア開発では不可欠な要件です。また、多くの組織が、独立系ソフトウェア・ベンダーから調達したパッケージ・ソフトウェアや、IoT 機器、組み込み用ファームウェアを使用しているため、その多くは AST ツールボックス内で何らかの形式での、SCA のバイナリ解析が必要になります。

図 G 使用しているアプリケーション・セキュリティ・ツールはどの程度有益ですか



概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

テストおよびパッチのタイミングとスケジュールへの影響

アプリケーション・セキュリティ・テストの実行頻度は、アプリケーションのビジネス上の重要度、業種、脅威の状況など、いくつもの要因によって変わります。調査結果 (図 H) からわかるように、非常に重要なアプリケーションでは定期的に評価を実行する必要があります。ビジネスに不可欠なアプリケーションに対する脆弱性スキャンの頻度として最も多かったのは、平均で 1 週間あたり 2 ～ 3 日です。

28% の組織が、重大な脆弱性にパッチを適用するまでに最大 3 週間かかっているという調査結果は (図 I)、一見すると気がかりに思えますが、ほかにも考慮すべき要素があります。開発者はあらゆる脆弱性を修正できるという俗説がありますが、開発者が解決を優先されていない脆弱性を徹底的に調査することは合理的に考えて期待できません。

DevSecOps を実装する際の主な障壁として、回答者の 31% が「開発 / 運用作業の透明性欠如」を挙げており、ほかに 29% が「開発、運用、セキュリティの間にある組織の壁」を挙げている (図 K) ことにも注目すべきです。どちらも、セキュリティチームから開発チームへのリスク伝達の問題と、セキュリティ・ポリシーを使用した迅速なアラートと自動化の必要性を示しています。

いずれのケースでも、パッチ適用の優先順位が、パッチ対象資産のビジネス上の重要性、資産の重要度、悪用のリスクに適合している必要がありますが、最も重要なのは悪用のリスクです。さまざまな調査から、報告される脆弱性のうち半分を超えるものが公開後 1 週間以内に悪用されていることが判明しています。

図 H ビジネスに不可欠なアプリケーションのセキュリティを評価またはテストする頻度は平均でどの程度ですか

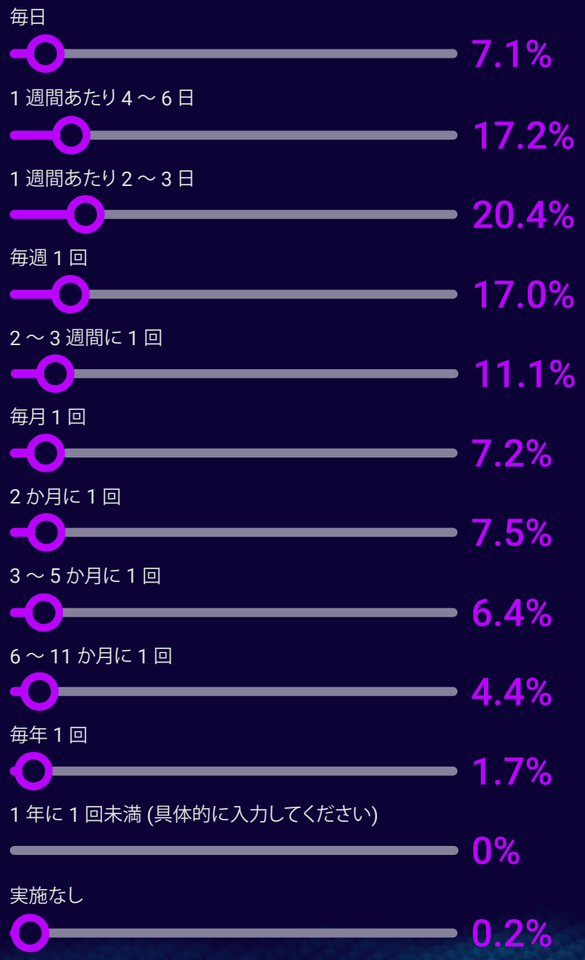
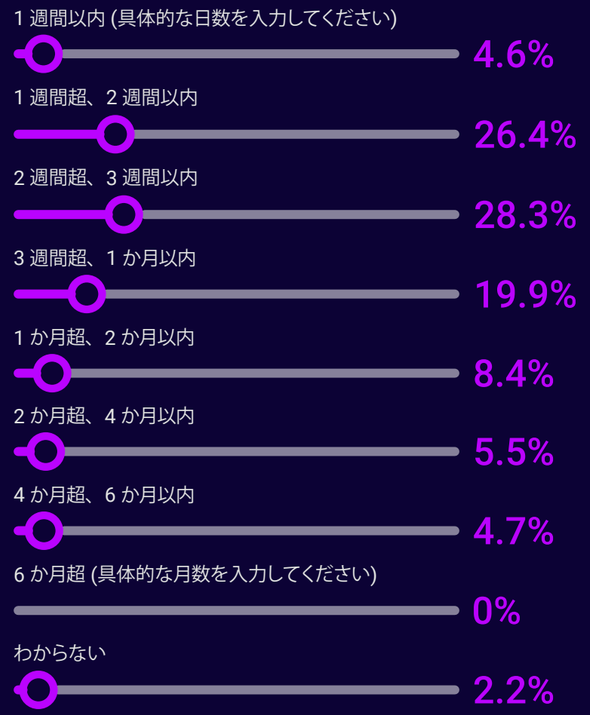


図 I デプロイ済み / 使用中のアプリケーションで、重大なセキュリティ・リスク / 脆弱性に対するパッチ適用 / 解決までに平均でどのくらいの時間がかかっていますか



概要

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

- DevSecOps の採用
- セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
- セキュリティ・プログラムの測定
- DevSecOps の成功における部門横断的チームの重要性
- 最善の結果を得るための手動テストと自動テストの組み合わせ
- 重要業績評価指標 (KPI)
- 使用している AST ツールとその有用性
- テストおよびパッチのタイミングとスケジュールへの影響
- 効果的な DevSecOps を妨げる課題
- AI への期待と落とし穴

調査結果からの学び

調査対象者の属性

付録

以上をふまえ、組織は、共通脆弱性評価システム (CVSS) スコアと共通脆弱性タイプ一覧 (CWE) 情報に加えて、(脆弱性開示の「ゼロデイ」だけでなく、アプリケーションのライフサイクルを通じた) 悪用の可能性に基づいて、取り組みの優先順位を決定する必要があります。

CVSS の値は、脆弱性の深刻度を評価するための業界標準です。National Vulnerability Database (NVD) 内で各脆弱性に付与された基本値は、深刻度の算定に役立ち、修正の優先順位付け要因としても使用できます。CVSS の値は、悪用の可能性と影響の両方を考慮した総合的な基本 (Base) 値を表します。

現状 (Temporal) 値は、脆弱性の外部のイベントによって時間とともに変化するメトリクスを考慮したものです。利用可能な対策のレベル (Remediation Level、利用できる正式な修正があるか) と脆弱性情報の信頼性 (Report Confidence、報告は確認されているか) によって総合的な CVSS の値が調整され、妥当なリスク・レベルが決定します。

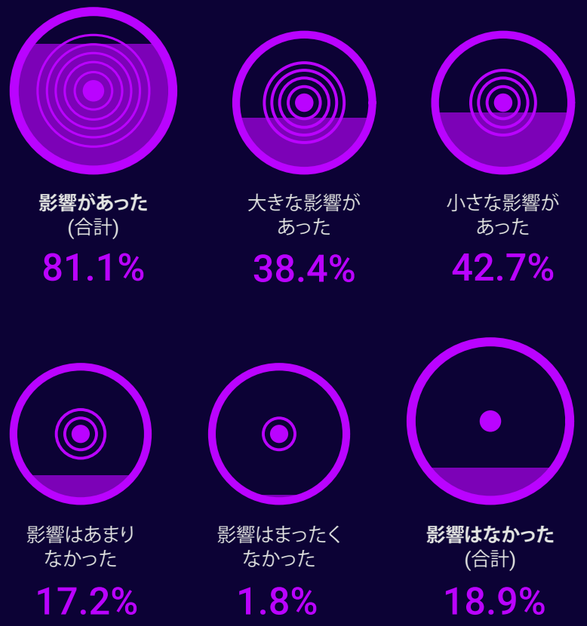
CWE 情報は、セキュリティに影響を与えるソフトウェアまたはハードウェアの弱点を一覧にしたものです。CWE により、開発者は、エクスプロイト (悪用可能な手段やコード) があればどの弱点が悪用され得るのかを把握できます。この情報は、セキュリティおよび開発チームが、開発者のセキュリティ・トレーニングではどこに焦点を合わせるか、SDLC 全体と本番環境で、どの追加セキュリティ対策を実装すべきかを理解するのに役立つとともに、リスクの深刻度を評価するもう 1 つのメカニズムを提供します。たとえば、開発チームは、アプリケーションが扱うデータのコンテキスト、アプリケーションがデプロイされる場所、その他の環境およびセキュリティ要因を考慮して、SQL インジェクションに、バッファ・オーバーフローやサービス拒否 (DoS) とは異なる優先順位を付ける場合があります。

エクスプロイト (悪用可能な手段やコード) があればリスクの値が引き上げられるため、チームは最もリスクが高い脆弱性の修正を優先することができます。総合的なリスクを評価した後は、既存のパッチ、リスク軽減要因、補完する対策があるかどうかを理解することが、調査すべきもう 1 つの重要な情報になります。たとえば、エクスプロイトがなく中程度のリスクの脆弱性が 2 つある場合、どちらを先に修正すべきかの最終判断は、パッチまたは回避策があるかどうかによって決まるかもしれません。

デプロイ済みアプリケーションに重大なセキュリティまたは脆弱性の課題がある場合、組織 (または顧客) の事業活動を中断させる可能性だけでなく、SDLC 全体に及ぶ影響を介して、連鎖的に問題が悪化します (図 J 参照)。

開発の早い段階で把握していれば軽度の修正で済んだかもしれない問題でも、デプロイ済みアプリケーションで見つかった場合は「総動員」が必要な鎮火作業に変わることがあります。自動セキュリティ・テスト・ツールが IDE と CI パイプラインに組み込まれていれば、コードがコミットされ次第すぐに (またはコミットされる前に) 脆弱性と弱点を識別できるため、問題が下流に波及する前に対策を取ることができます。

図 J **過去 1 年間に (2022 ～ 2023 年)、重大なセキュリティ / 脆弱性の課題への対処によって、組織のソフトウェア・デリバリー・スケジュールに及んだ影響はどの程度でしたか (影響があった場合)**



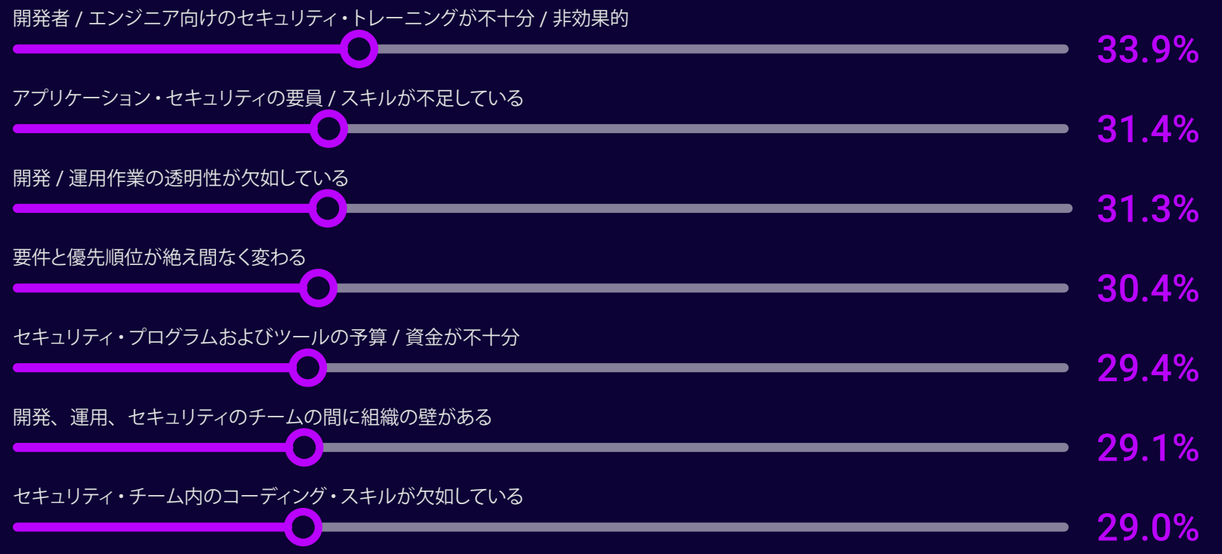
概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

効果的な DevSecOps を妨げる課題

サイバーセキュリティ要員の不足は DevSecOps にとって重大な問題となっており、図 K に示されるように、多くの組織がサイバーセキュリティ関連の重要なポストを埋められない状況にあります。いくつかの調査によると、サイバーセキュリティ担当の欠員は世界で 350 万に上ります。経験を積んだサイバーセキュリティ専門家の需要が増加するにつれ、供給不足によってスキルある専門家の賃金が跳ね上がり、多くの政府機関や中小企業の手が届かないレベルになっています。ただし、最も多い回答からわかるように、開発者 / エンジニア向けのセキュリティ・トレーニングが不十分であることが引き続き最大の課題となっています。

これらの課題への効果的な対処が確認された戦略の 1 つに、セキュリティ・チャンピオン・プログラムの開発があります。セキュリティ・チャンピオンは、セキュリティに対する関心またはスキルが平均以上あり、すでに開発、QA、運用チームにセキュリティの専門知識を提供している、組織全体にまたがる個人で構成されます。セキュリティ・チャンピオンは新規プロジェクトの相談役となって、新しいテクノロジーまたは動きの速いテクノロジー分野で、セキュリティ / エンジニアリング・チームでは過小評価されがちな特定領域の知識をソフトウェア・セキュリティ・スキルに組み合わせる支援をします。

図 K DevSecOps の実装に際して、どのような課題 / 障壁がありますか (当てはまるものをすべて選択)



概要

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

- DevSecOps の採用
- セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
- セキュリティ・プログラムの測定
- DevSecOps の成功における部門横断的チームの重要性
- 最善の結果を得るための手動テストと自動テストの組み合わせ
- 重要業績評価指標 (KPI)
- 使用している AST ツールとその有用性
- テストおよびパッチのタイミングとスケジュールへの影響
- 効果的な DevSecOps を妨げる課題
- AI への期待と落とし穴

調査結果からの学び

調査対象者の属性

付録

前述のように、SAST、DAST、IAST、SCA などの AST ツールは回答者に広く使用されていますが、これらのツールを効果的にビジネス・ニーズに合致させることが引き続き課題となっています (図 L)。

多くの回答者が使用中のセキュリティ・テスト・ツールに関して不満に感じているのは、曝露、悪用の可能性、重要度などの要因に基づいて解決策が優先付けされていない、パフォーマンスが低すぎて継続的デプロイのリリース・サイクルに対応できない、正確さと信頼性に欠ける、といった点です。

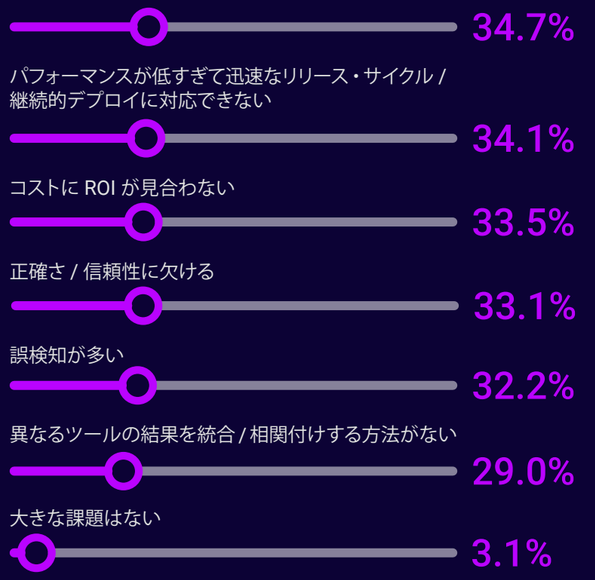
異なるセキュリティ・テストの結果を統合したり互いに関連付けたりする方法がないため、セキュリティおよび DevOps チームが最初に修正すべき課題を決定するまでに過度な時間がかかっています。おそらくはこれが、回答者の 4 分の 3 近くが、既知の重要な脆弱性にパッチを適用するまでに 2 週間から 1 か月かかることがあると述べた理由の 1 つでしょう (図 I)。

迅速にパッチを適用できない場合、最終的な結果に影響が及びます。80% を超える回答者が、2022 年から 2023 年にかけて、デプロイ済みソフトウェアに含まれる重大な脆弱性 / セキュリティ課題への対処が、デリバリー・スケジュールに影響を与えたと述べました (図 J)。

細分化された AST ツールと修正が遅い問題は、まさに、アプリケーション・セキュリティのオーケストレーションと相関付け (ASOC) とアプリケーション・セキュリティ態勢管理 (ASPM) が解決を目指しているものです。ガートナーによると、ASOC/ASPM は複数の AST ツールを取りまとめる管理層の役割を果たし、自動的に結果を相関付けて状況に応じて修正を早め、集中して対応できるようにします。

ASOC/ASPM はさまざまなソースから結果を取り込み、アプリケーション環境全体で統一されたリスク・ビューを提供することで、重大度のようなビジネス・コンテキストに基づくデータ・ドリブンな優先順位付けを可能にし、リスクのより高い脆弱性から先にパッチを適用できるようにします。ASOC/ASPM によって本番環境が可視化されるため、デプロイ済みアプリケーションの修正に長い時間がかかることと、ほとんどのエクスプロイト (悪用可能な手段やコード) が数日以内に出現するという現実の間にあるギャップが解消されます。

図 L 使用しているアプリケーション・セキュリティ・テスト・ツールに関する最大の課題は何ですか (最大で 3 つまで選択)



概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

AI への期待と落とし穴

50% を超える回答者が DevSecOps のプラクティスで AI を積極利用していると述べるなど、今回の調査結果から、すでに多くの組織のソフトウェア・セキュリティ・イニシアティブに AI 使用が深く組み込まれていることがわかります。54% の回答者は、AI によってセキュリティ対策の効率と精度が上がると期待しています。また、58% の回答者は、AI を通じてセキュリティ・テストの手動レビューを減らしたいと考えています。

AI が DevSecOps にもたらすであろう大きな利点を考えれば当然です。アプリケーション・セキュリティ・チームは、一貫性のあるセキュリティ・テストをひととおり実施する必要性と、DevOps メソドロジーおよび CI パイプラインを使用する開発チームに遅れをとらないようにする必要性との間で、絶えず板挟みになっています。期限が迫る中、開発者は重要なセキュリティ・リスク評価手順を省略しがちです。

セキュアな SDLC に AI を取り入れることで期待される主なメリットとしては、「セキュリティ対策の精度と効率の向上」(54%) と「セキュリティ・データを手動でレビューし分析する必要性が減る」(48%) の 2 つが挙げられました。

しかし、回答者は、AI によって「ソフトウェア・セキュリティが複雑化して技術要件が高くなる」とも述べています。いつの日か、AI によって生成されたコードを適切にレビューできるのは AI 自身だけになるのかもしれません。

図 M 現在、ソフトウェアのセキュリティ対策を強化する目的で何らかの AI ツールを使用していますか

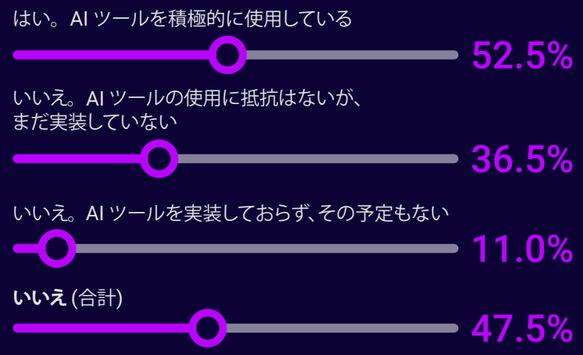
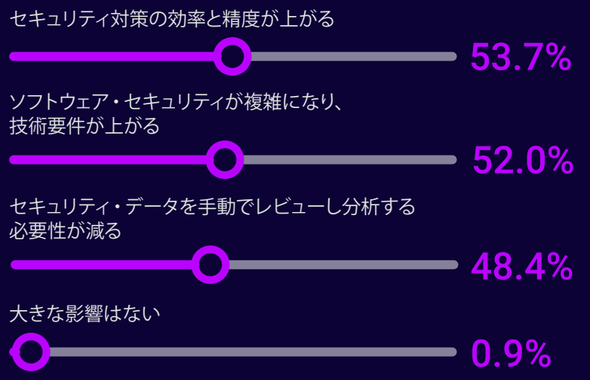


図 N AI ツールの使用は、DevSecOps プロセスおよびワークフローにどのような影響を与えると思いますか (当てはまるものをすべて選択)



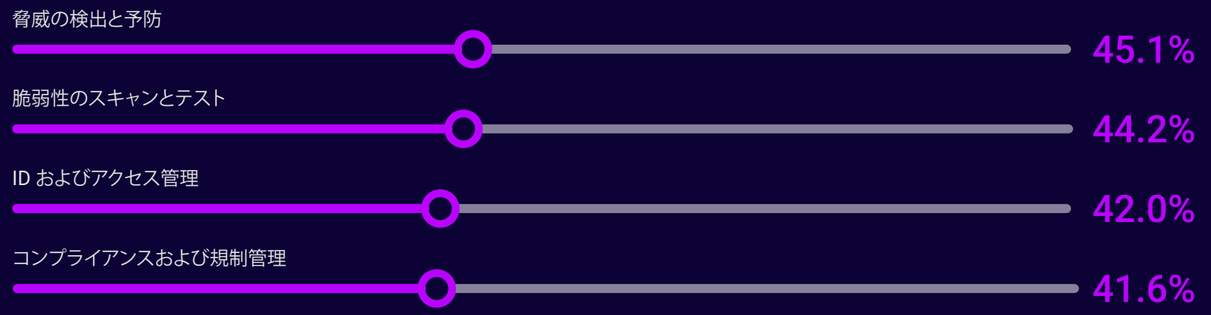
概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
DevSecOps の採用
セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
セキュリティ・プログラムの測定
DevSecOps の成功における部門横断的チームの重要性
最善の結果を得るための手動テストと自動テストの組み合わせ
重要業績評価指標 (KPI)
使用している AST ツールとその有用性
テストおよびパッチのタイミングとスケジュールへの影響
効果的な DevSecOps を妨げる課題
AI への期待と落とし穴
調査結果からの学び
調査対象者の属性
付録

DevSecOps への AI の実装には、データの品質確保とセキュリティおよびプライバシーの懸念への対応など、新たな課題が伴います。AI ツールが DevOps パイプラインにさらに統合されれば、ほぼ間違いなく、セキュリティ上の脅威の主な対象となるでしょう。AI のトレーニングに使用される機密データの取り扱いもまた、プライバシーの課題の原因となる可能性があります。

AI 利用による潜在的なリスクを表す 1 つのシナリオが AI の支援によるコーディングの使用であり、ここから AI が生成したコードの所有権、著作権、ライセンスに関する疑問が生じています。

2022 年後半、オートコンプリート・スタイルでコードを提案するクラウドベースの AI ツール GitHub Copilot が、著作権法およびソフトウェア・ライセンス要件に加えて、Copilot サービスのトレーニングに使用されたオープンソース・コードの開発者の権利を侵害しているとして、GitHub、Microsoft、OpenAI を相手にした集団代表訴訟が起こされました。この訴訟では、さらに、Copilot によって提案されるコードが、帰属や著作権を表示せず、元のライセンス条件に準拠することもなく、ライセンス対象コードを使用しているとしています。

図 0 AI ツールの使用は、どのソフトウェア・セキュリティ領域の強化に最も効果的だと考えますか



概要

2023 年シノプシス DevSecOps 調査の主な発見事項

2023 年の DevSecOps の現状

- DevSecOps の採用
- セキュリティ・プラクティスの実装は成熟度レベルの高さを示す
- セキュリティ・プログラムの測定
- DevSecOps の成功における部門横断的チームの重要性
- 最善の結果を得るための手動テストと自動テストの組み合わせ
- 重要業績評価指標 (KPI)
- 使用している AST ツールとその有用性
- テストおよびパッチのタイミングとスケジュールへの影響
- 効果的な DevSecOps を妨げる課題
- AI への期待と落とし穴

調査結果からの学び

調査対象者の属性

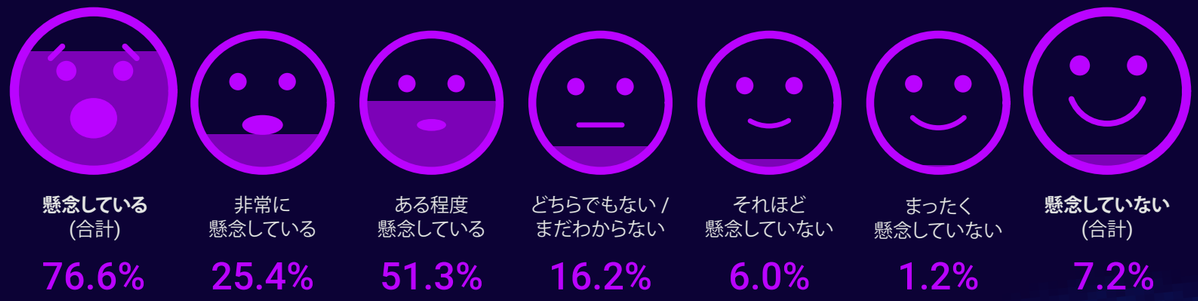
付録

ChatGPT や Google Bard などの大規模言語モデルに基づく生成 AI チャットボットにも問題があり、「ハルシネーション (幻覚)」、つまり信頼でき自信に満ちているように見えても真実ではない、分かり易く言えば「嘘」である誤った応答をランダムに生成するという問題を抱えています。

AI のハルシネーションは、ソフトウェア・サプライチェーンのセキュリティにとって明らかな脅威です。ChatGPT は場合によって、嘘の存在しないコード・ライブラリやパッケージを推奨することが、研究者によって確認されています。悪意のある攻撃者は、同じ名前でパッケージを作成し、そこに悪意のあるコードを格納して、疑いもせず AI の推奨に従う開発者にそれを配布することができます。そうすれば、タイポスクワッティング (または URL ハイジャッキング) やマスカレーディング (なりすまし) など、より従来型の簡単に検出できるテクニックを使わずに済むため、サイバー犯罪者にとってのゲーム・チェンジャーとなりかねません。実際に、ChatGPT の嘘の推奨に基づいて作成された悪意のあるパッケージが、PyPI や npm などお馴染みのパッケージ・インストーラにすでに含まれていることが明らかになっています。

こういった脅威は架空のものではなく、今、現実に発生している脅威です。防ぐべきサプライチェーン攻撃の発端が AI ハルシネーションであるか、悪意のある攻撃者であるかにかかわらず、コードの出所を把握し、開発者とメンテナンス担当者を認証し、信頼できるベンダーまたはソースからのみダウンロードすることが必要不可欠です。

図 P AI ベースのセキュリティ・ソリューションにバイアスまたは誤りが含まれる可能性について、どの程度懸念していますか



概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

調査結果からの学び

ほとんどの組織は、一定程度の DevSecOps プラクティスを広く導入していますが、その効果的な実装については依然として障壁に直面しています。調査から明らかになった 2 つの主な問題は次のとおりです。

- 複数のアプリケーション・セキュリティ・テスト (AST) ツールの結果を統合し、ビジネス上の優先順位に合わせて調整する
- 重大な脆弱性の解決に必要な時間を短縮する

回答者の 28% が、デプロイ済みアプリケーションで、重大なセキュリティ・リスク / 脆弱性に対するパッチを適用するまでに 3 週間ほどかかると述べています。また、ほとんどのエクスプロイト (悪用可能な手段やコード) は数日以内に出現しているというのに、別の 20% は最大 1 か月かかると回答しています。AST ツールに関する最大の不満として挙げられたのは、脆弱性の解決策をビジネス・ニーズに基づいて優先順位付けできないことです。

本レポートの最初に述べたとおり、調査の質問を開発する際の課題の 1 つは、「DevSecOps」という用語がいくつもの異なる領域に及んでおり、その多くに独自のペルソナがある点でした。「ビジネス上の優先事項」と言っても、役割ごとに別のものを意味する可能性があります。

たとえば、ビジネス・リーダーにとっての優先事項は、アプリケーション・セキュリティ・ツールの有効性を理解することであり、複数のチームにまたがるプロセスとパフォーマンスを完全に可視化することを求めます。開発および運用チームは、すべての課題を一元化したビューを求め、最も影響の大きいセキュリティ・アクティビティを特定したいと考えます。セキュリティに特化した要員は、ノイズを排除して重大な課題を素早く優先処理したいと希望します。

ビジネス面での要求にペースを合わせながら、サイロ化したセキュリティ・ツールの結束力を高めようと奮闘中の組織にとって、アプリケーション・セキュリティ態勢管理 (ASPM) は必要な結束力の増強装置となり得ます。ASPM はツールの連携、テストの解釈、修正の優先順位付けを自動化することで、組織は最も重要なアプリケーション・セキュリティ・ビジネスの優先事項に重点的に取り組むことができます。

- ASPM は、開発ツール、セキュリティ・テスト・ツール、運用監視ツールを統合することで、組織内の各所から収集したセキュリティ関連情報を 1 つにまとめたビューに表示します。
- ASPM は、特定のアプリケーションおよび脆弱性を解析する各種ツールから収集した情報を関連付けてグループ化することで、アプリケーションの全体的なセキュリティ態勢を包括的なビューに表示します。DevSecOps グループが各自の役割と責任に関連するデータを生成すると、ASPM により、事業部門のマネージャーなど、大局的な見方を必要とする人々にとって理解しやすい方法でデータが表示されます。
- ASPM では、特定のアプリケーションと、ある脆弱性によってもたらされる特定のリスクに対して、セキュリティ・ポリシーを作成して適用できます。ASPM を開発または運用インフラストラクチャと統合すると、可能な限りプロセスの早い段階で修正する必要のあるセキュリティ課題を特定することもできます。

ガートナーは、2021 年のデータから、調査対象組織の約 5% が、ASPM ツール、またはその基となったアプリケーション・セキュリティのオーケストレーションと相関付け (ASOC) ツールを採用していると述べました。この採用ペースが急速に加速するというガートナーの予想は今回の 2023 年の調査結果に表れており、回答者の 28% が ASOC/ASPM を使用していると回答しました。また、アーリー・アダプターは成熟した DevSecOps プログラムを導入し、複数のセキュリティ・ツールを使用するグループになる傾向があると指摘していますが、これはどちらも今回の DevSecOps 調査の回答者に当てはまる特性です。

本レポートを詳しく見てみると、セキュリティ・ツールからの関連性の見出せないテスト結果、チームへの過負荷、脆弱性の解決の遅れが、DevOps の成功に対する根本的な課題であることが説得力をもって示されています。多数のアプリケーション・セキュリティ・テスト・ツールを使用する多様な DevSecOps チームを抱える組織にとって、これらの課題を効果的に解決する鍵となり得るのが ASPM です。

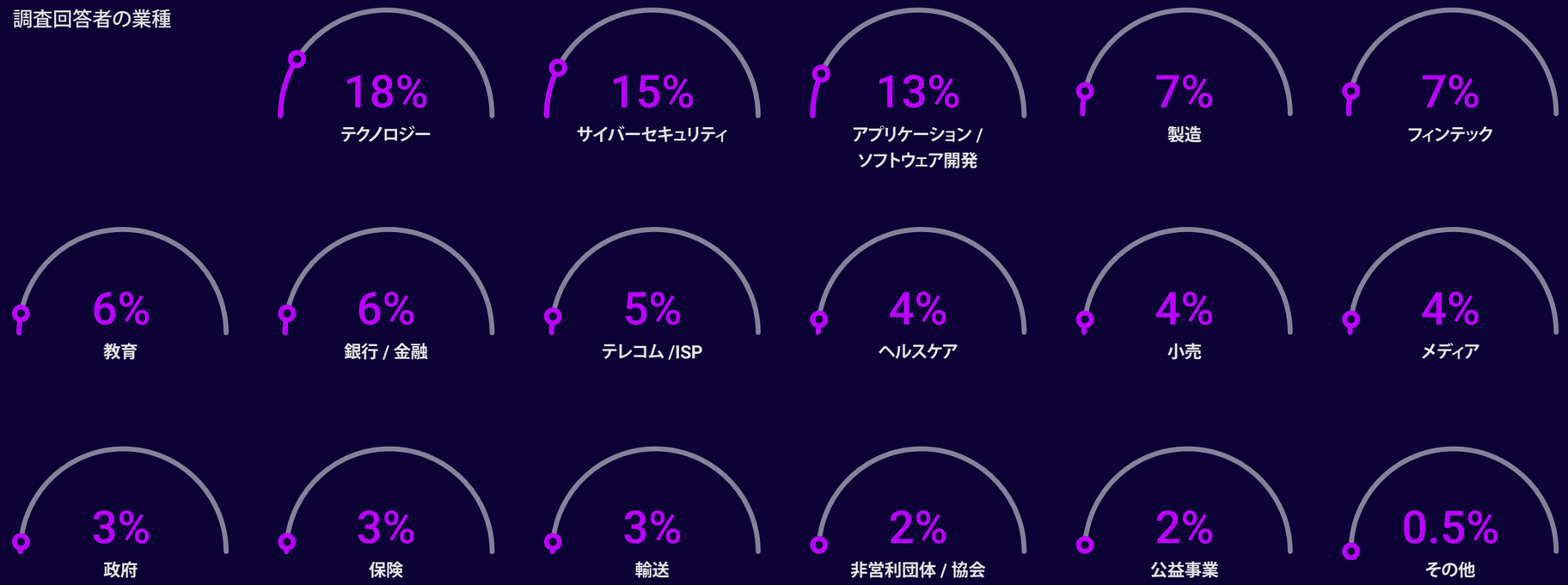
Software Risk Manager: ASPM が提供する成果を保証する

- アプリケーション・セキュリティ管理を簡略化
- アプリケーション・セキュリティ・リスクを包括的に把握
- 重大な課題を迅速に優先順位付け
- アプリケーション・セキュリティ・ワークフローを標準化
- ビジネス要求に対応する速度でテスト

ASPM の利点がどのようなものか実際にご覧になりたい場合は、Software Risk Manager のデモをシノプシスにご依頼ください。

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

調査回答者の業種

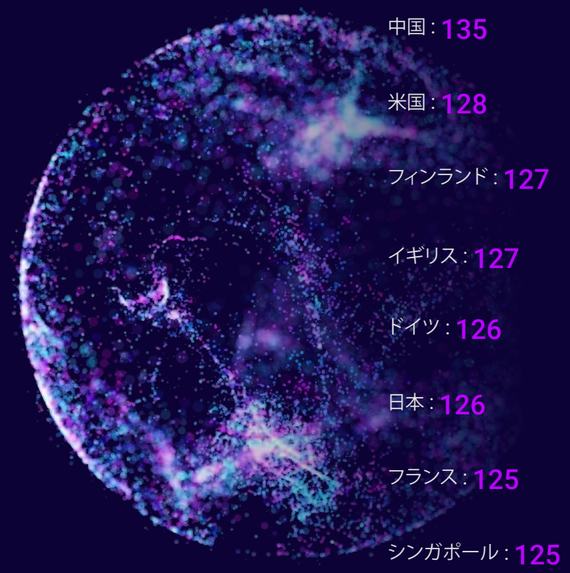


回答者の役職

アプリケーション・セキュリティ・アーキテクト
アプリケーション・セキュリティ・マネージャー
CISO
開発者
DevOps エンジニア
アプリケーション・セキュリティ担当ディレクター
サイバーセキュリティ担当ディレクター
IT リスク管理担当ディレクター
IT 共有サービス担当ディレクター
プロダクト・セキュリティ担当ディレクター
セキュリティ保証担当ディレクター
プロダクト・セキュリティ担当エグゼクティブ・ディレクター
インシデントおよびセキュリティ・マネージャー
情報保証ディレクター
ソフトウェア・セキュリティ・エンジニアリング担当マネージャー
運用エンジニア
プロダクト・セキュリティ、アプリケーション・セキュリティ
プログラマー
QA/ テスト担当者 / テスト・マネージャー
リリース・エンジニア / マネージャー
セキュリティ管理者 / セキュリティ・アナリスト
セキュリティ・アーキテクト
セキュリティ・ディレクター
セキュリティ・エンジニアリング・マネージャー
プロダクト・セキュリティ担当シニア・ディレクター
プロダクト・セキュリティおよびテクノロジー担当 SVP
テクニカル・リード
プロダクトおよびアプリケーション・セキュリティ担当 VP
セキュリティ・アーキテクチャ担当 VP
セキュリティ・コンプライアンス担当 VP

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

国別の回答者数



- 中国 : 135
- 米国 : 128
- フィンランド : 127
- イギリス : 127
- ドイツ : 126
- 日本 : 126
- フランス : 125
- シンガポール : 125

組織が作成 / 管理するソフトウェア / アプリケーション

- アプリケーション・ソフトウェア 46%
- システム・ソフトウェア 44%
- Web アプリケーション 42%
- プロダクト・ソフトウェア 38%
- AI ソフトウェア 37%
- エンジニアリング / 科学ソフトウェア 35%
- 組み込みソフトウェア 31%

採用しているセキュリティ・プラクティス

- セキュリティ・リスク管理 35%
- 継続的な監視と測定 30%
- 構成管理 30%
- 脅威に関するデータと対応 30%
- 継続的デプロイ 29%
- 自動デプロイ 29%
- 継続的テスト 28%
- アプリケーション・セキュリティのオーケストレーションと相関付け (ASOC) 28%
- 継続的インテグレーション 28%
- 自動テスト 28%
- インフラストラクチャ・アズ・コード (Infrastructure-as-code) 28%

組織の規模 (従業員 / 契約社員の人数)

- 1% 100,000 超
- 4% 50,001 ～ 100,000
- 7% 15,001 ～ 50,000
- 8% 10,001 ～ 15,000
- 13% 5,001 ～ 10,000
- 12% 2,001 ～ 5,000
- 19% 1,001 ～ 2,000
- 19% 501 ～ 1,000
- 15% 100 ～ 500
- 2% 100 未満

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q1 貴社の主たる業種は何ですか

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
テクノロジー	**18.45%**	10.24%	34.38%	14.40%	12.60%	9.52%	42.96%	12.00%	9.52%
サイバーセキュリティ	**14.52%**	17.32%	13.28%	20.00%	14.96%	10.32%	7.41%	18.40%	15.08%
アプリケーション / ソフトウェア開発	**12.66%**	4.72%	7.03%	20.00%	14.17%	1.59%	26.67%	5.60%	20.63%
製造	**7.26%**	3.94%	3.13%	4.00%	5.51%	9.52%	13.33%	8.80%	9.52%
フィンテック	**6.87%**	6.30%	7.03%	4.80%	10.24%	11.11%	2.22%	8.80%	4.76%
教育	**5.59%**	6.30%	5.47%	7.20%	6.30%	3.97%	0.00%	9.60%	6.35%
銀行 / 金融	**5.50%**	7.09%	3.91%	5.60%	4.72%	11.11%	0.74%	4.00%	7.14%
テレコム /ISP	**5.10%**	5.51%	3.13%	6.40%	8.66%	7.14%	2.22%	3.20%	4.76%
ヘルスケア	**4.12%**	6.30%	7.03%	4.00%	3.94%	3.17%	1.48%	4.00%	3.17%
小売	**4.02%**	7.09%	5.47%	4.00%	3.94%	5.56%	0.00%	3.20%	3.17%
メディア	**3.63%**	3.15%	2.34%	0.80%	3.94%	5.56%	0.74%	4.80%	7.94%
政府	**3.14%**	5.51%	3.13%	2.40%	3.15%	4.76%	0.74%	4.00%	1.59%
保険	**2.85%**	5.51%	3.13%	1.60%	3.15%	4.76%	0.00%	3.20%	1.59%
輸送	**2.55%**	3.94%	0.00%	3.20%	1.57%	6.35%	0.74%	3.20%	1.59%
非営利団体 / 協会	**1.67%**	3.94%	0.78%	0.80%	1.57%	3.17%	0.00%	2.40%	0.79%
公益事業	**1.57%**	2.36%	0.78%	0.00%	0.79%	2.38%	0.74%	4.00%	1.59%
その他 (具体的に入力してください)	**0.49%**	0.79%	0.00%	0.80%	0.79%	0.00%	0.00%	0.80%	0.79%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q2 貴社の規模はどのくらいですか (正社員と契約社員の両方を含めた規模)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
100 人未満 (具体的に入力してください)	**1.57%**	1.57%	0.00%	2.40%	0.00%	0.00%	3.70%	1.60%	3.17%
100 ～ 500	**15.11%**	11.02%	16.41%	20.80%	12.60%	19.05%	14.81%	6.40%	19.84%
501 ～ 1,000	**19.04%**	14.96%	23.44%	23.20%	14.96%	21.43%	8.89%	16.00%	30.16%
1,001 ～ 2,000	**18.65%**	15.75%	17.19%	15.20%	19.69%	15.87%	37.78%	16.00%	10.32%
2,001 ～ 5,000	**12.37%**	22.83%	10.94%	16.00%	18.11%	7.14%	5.93%	8.80%	9.52%
5,001 ～ 10,000	**13.05%**	18.11%	11.72%	7.20%	15.75%	6.35%	20.00%	17.60%	7.14%
10,001 ～ 15,000	**8.44%**	10.24%	9.38%	3.20%	8.66%	5.56%	2.96%	16.80%	11.11%
15,001 ～ 50,000	**6.67%**	3.94%	4.69%	4.00%	6.30%	17.46%	0.74%	10.40%	6.35%
50,001 ～ 100,000	**4.42%**	1.57%	5.47%	4.00%	3.15%	7.14%	5.19%	6.40%	2.38%
100,000 超 (具体的に入力してください)	**0.69%**	0.00%	0.78%	4.00%	0.79%	0.00%	0.00%	0.00%	0.00%

Q3 貴社で作成または管理しているソフトウェア / アプリケーションの種類を選択してください (当てはまるものをすべて選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
アプリケーション・ソフトウェア	**46.03%**	40.94%	61.72%	48.00%	37.01%	34.13%	70.37%	36.80%	37.30%
システム・ソフトウェア	**44.06%**	42.52%	54.69%	40.00%	30.71%	34.92%	67.41%	39.20%	41.27%
Web アプリケーション	**41.71%**	27.56%	45.31%	40.80%	44.09%	37.30%	68.89%	39.20%	28.57%
プロダクト・ソフトウェア	**38.27%**	29.13%	47.66%	28.80%	39.37%	30.16%	65.19%	30.40%	33.33%
AI ソフトウェア	**36.60%**	30.71%	41.41%	32.00%	32.28%	33.33%	57.04%	35.20%	29.37%
エンジニアリング / 科学ソフトウェア	**35.23%**	25.20%	39.84%	27.20%	31.50%	38.89%	57.04%	30.40%	30.16%
組み込みソフトウェア	**30.91%**	29.13%	34.38%	20.80%	29.92%	30.16%	42.22%	29.60%	30.16%
その他 (具体的に入力してください)	**0.20%**	0.79%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.79%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q4 現在使用しているプラクティスはどれですか (当てはまるものをすべて選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
セキュリティ・リスク管理	**35.13%**	35.43%	40.63%	33.60%	32.28%	19.84%	56.30%	32.80%	28.57%
継続的な監視と測定	**29.93%**	25.20%	34.38%	29.60%	32.28%	22.22%	44.44%	25.60%	24.60%
構成管理	**29.64%**	19.69%	31.25%	24.80%	23.62%	23.02%	49.63%	30.40%	33.33%
脅威に関するデータと対応	**29.34%**	22.83%	39.84%	31.20%	28.35%	19.84%	41.48%	27.20%	23.02%
継続的デプロイ	**29.05%**	27.56%	35.16%	21.60%	29.13%	28.57%	41.48%	20.80%	26.98%
自動デプロイ	**28.56%**	18.90%	28.91%	32.80%	28.35%	23.81%	48.15%	24.80%	21.43%
継続的テスト	**28.46%**	22.05%	32.03%	24.80%	30.71%	23.02%	48.15%	17.60%	27.78%
アプリケーション・セキュリティのオーケストレーションと相関付け (ASOC)	**28.36%**	29.13%	39.84%	20.00%	19.69%	18.25%	51.85%	28.00%	18.25%
継続的インテグレーション	**28.16%**	23.62%	30.47%	24.80%	25.98%	19.84%	47.41%	28.00%	23.81%
自動テスト	**27.87%**	19.69%	33.59%	28.00%	24.41%	15.08%	48.15%	20.00%	32.54%
インフラストラクチャ・アズ・コード (Infrastructure-as-code)	**27.58%**	23.62%	41.41%	22.40%	20.47%	22.22%	48.15%	25.60%	15.08%
その他 (具体的に入力してください)	**0.10%**	0.00%	0.00%	0.00%	0.79%	0.00%	0.00%	0.00%	0.00%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q5 アプリケーション・セキュリティに関する以下のツール、プラクティス、テクニックを使用している場合、その有用性を回答してください

SDLC 要件段階の一部としてセキュリティ要件を定義する	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**71.25%**	**66.93%**	**78.91%**	**73.60%**	**81.10%**	**62.70%**	**97.04%**	**55.20%**	**52.38%**
非常に有益である	**32.09%**	25.20%	46.88%	32.00%	35.43%	24.60%	54.07%	17.60%	19.05%
ある程度有益である	**39.16%**	41.73%	32.03%	41.60%	45.67%	38.10%	42.96%	37.60%	33.33%
それほど有益ではない	**16.78%**	15.75%	12.50%	16.80%	13.39%	20.63%	2.96%	26.40%	26.98%
まったく有益ではない	**7.56%**	11.02%	3.13%	8.00%	3.15%	11.90%	0.00%	14.40%	9.52%
有益ではない (合計)	**24.34%**	**26.77%**	**15.63%**	**24.80%**	**16.54%**	**32.54%**	**2.96%**	**40.80%**	**36.51%**
該当なし	**4.42%**	6.30%	5.47%	1.60%	2.36%	4.76%	0.00%	4.00%	11.11%

BSIMM および SAMM などのモデルを使用した、ソフトウェア・セキュリティの正式な測定	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**69.38%**	**55.91%**	**79.69%**	**71.20%**	**70.87%**	**57.94%**	**94.81%**	**67.20%**	**55.56%**
非常に有益である	**33.56%**	24.41%	47.66%	25.60%	30.71%	26.98%	57.04%	28.80%	25.40%
ある程度有益である	**35.82%**	31.50%	32.03%	45.60%	40.16%	30.95%	37.78%	38.40%	30.16%
それほど有益ではない	**18.06%**	25.20%	10.94%	17.60%	25.20%	23.02%	3.70%	16.80%	23.02%
まったく有益ではない	**8.44%**	11.81%	7.03%	8.80%	2.36%	16.67%	0.74%	10.40%	10.32%
有益ではない (合計)	**26.50%**	**37.01%**	**17.97%**	**26.40%**	**27.56%**	**39.68%**	**4.44%**	**27.20%**	**33.33%**
該当なし	**4.12%**	7.09%	2.34%	2.40%	1.57%	2.38%	0.74%	5.60%	11.11%

自動化されたコード・スキャンによるセキュリティの脆弱性およびその他の不具合の検出 (例 : 静的アプリケーション・セキュリティ・テスト (SAST))	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**71.54%**	**62.20%**	**76.56%**	**76.00%**	**78.74%**	**65.87%**	**94.07%**	**54.40%**	**62.70%**
非常に有益である	**34.35%**	29.13%	46.09%	33.60%	38.58%	27.78%	54.07%	21.60%	22.22%
ある程度有益である	**37.19%**	33.07%	30.47%	42.40%	40.16%	38.10%	40.00%	32.80%	40.48%
それほど有益ではない	**17.37%**	22.05%	10.94%	16.80%	18.11%	17.46%	5.93%	29.60%	19.05%
まったく有益ではない	**7.65%**	13.39%	8.59%	5.60%	2.36%	11.90%	0.00%	12.80%	7.14%
有益ではない (合計)	**25.02%**	**35.43%**	**19.53%**	**22.40%**	**20.47%**	**29.37%**	**5.93%**	**42.40%**	**26.19%**
該当なし	**3.43%**	2.36%	3.91%	1.60%	0.79%	4.76%	0.00%	3.20%	11.11%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

オープンソース / サードパーティの依存関係解析 (SCA)	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**67.62%**	**50.39%**	**75.00%**	**73.60%**	**74.80%**	**61.11%**	**94.81%**	**53.60%**	**55.56%**
非常に有益である	**30.32%**	22.05%	33.59%	32.00%	30.71%	23.81%	60.74%	20.00%	17.46%
ある程度有益である	**37.29%**	28.35%	41.41%	41.60%	44.09%	37.30%	34.07%	33.60%	38.10%
それほど有益ではない	**19.73%**	25.98%	16.41%	18.40%	22.05%	22.22%	5.19%	27.20%	21.43%
まったく有益ではない	**8.34%**	14.17%	5.47%	6.40%	1.57%	11.90%	0.00%	12.80%	15.08%
有益ではない (合計)	**28.07%**	**40.16%**	**21.88%**	**24.80%**	**23.62%**	**34.13%**	**5.19%**	**40.00%**	**36.51%**
該当なし	**4.32%**	9.45%	3.13%	1.60%	1.57%	4.76%	0.00%	6.40%	7.94%

内部またはサードパーティによるペネトレーション・テスト	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**67.91%**	**53.54%**	**71.88%**	**72.00%**	**80.31%**	**56.35%**	**96.30%**	**54.40%**	**56.35%**
非常に有益である	**30.23%**	18.11%	37.50%	35.20%	43.31%	23.02%	48.89%	17.60%	16.67%
ある程度有益である	**37.68%**	35.43%	34.38%	36.80%	37.01%	33.33%	47.41%	36.80%	39.68%
それほど有益ではない	**19.33%**	29.13%	19.53%	16.80%	16.54%	20.63%	3.70%	24.80%	24.60%
まったく有益ではない	**8.64%**	10.24%	7.03%	7.20%	3.15%	17.46%	0.00%	15.20%	9.52%
有益ではない (合計)	**27.97%**	**39.37%**	**26.56%**	**24.00%**	**19.69%**	**38.10%**	**3.70%**	**40.00%**	**34.13%**
該当なし	**4.12%**	7.09%	1.56%	4.00%	0.00%	5.56%	0.00%	5.60%	9.52%

ファジング・テスト	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**62.32%**	**50.39%**	**75.00%**	**58.40%**	**68.50%**	**53.97%**	**88.15%**	**55.20%**	**46.83%**
非常に有益である	**25.02%**	19.69%	35.94%	17.60%	23.62%	27.78%	42.96%	18.40%	12.70%
ある程度有益である	**37.29%**	30.71%	39.06%	40.80%	44.88%	26.19%	45.19%	36.80%	34.13%
それほど有益ではない	**19.73%**	18.90%	12.50%	22.40%	18.90%	23.02%	10.37%	25.60%	26.98%
まったく有益ではない	**9.52%**	14.96%	4.69%	4.80%	9.45%	18.25%	0.74%	12.00%	11.90%
有益ではない (合計)	**29.24%**	**33.86%**	**17.19%**	**27.20%**	**28.35%**	**41.27%**	**11.11%**	**37.60%**	**38.89%**
該当なし	**8.44%**	15.75%	7.81%	14.40%	3.15%	4.76%	0.74%	7.20%	14.29%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q6 アプリケーション・セキュリティに関する以下のツール、プラクティス、テクニックを使用している場合、その有用性を回答してください

動的アプリケーション・セキュリティ・テスト (DAST)	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**67.12%**	48.82%	74.22%	76.80%	74.80%	62.70%	91.11%	49.60%	57.14%
非常に有益である	**29.44%**	16.54%	38.28%	36.80%	29.92%	27.78%	46.67%	20.00%	18.25%
ある程度有益である	**37.68%**	32.28%	35.94%	40.00%	44.88%	34.92%	44.44%	29.60%	38.89%
それほど有益ではない	**19.63%**	32.28%	16.41%	16.80%	17.32%	20.63%	7.41%	28.80%	18.25%
まったく有益ではない	**9.62%**	12.60%	6.25%	5.60%	6.30%	12.70%	0.74%	18.40%	15.08%
有益ではない (合計)	**29.24%**	44.88%	22.66%	22.40%	23.62%	33.33%	8.15%	47.20%	33.33%
該当なし	**3.63%**	6.30%	3.13%	0.80%	1.57%	3.97%	0.74%	3.20%	9.52%

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)	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**68.50%**	60.63%	72.66%	75.20%	77.17%	53.97%	96.30%	53.60%	56.35%
非常に有益である	**31.11%**	22.05%	35.16%	34.40%	37.01%	18.25%	54.07%	24.00%	22.22%
ある程度有益である	**37.39%**	38.58%	37.50%	40.80%	40.16%	35.71%	42.22%	29.60%	34.13%
それほど有益ではない	**18.06%**	18.11%	20.31%	15.20%	18.11%	21.43%	3.70%	24.80%	23.81%
まったく有益ではない	**9.62%**	14.17%	6.25%	9.60%	3.15%	18.25%	0.00%	14.40%	11.90%
有益ではない (合計)	**27.67%**	32.28%	26.56%	24.80%	21.26%	39.68%	3.70%	39.20%	35.71%
該当なし	**3.83%**	7.09%	0.78%	0.00%	1.57%	6.35%	0.00%	7.20%	7.94%

Web アプリケーション・ファイアウォール (WAF)	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**68.99%**	62.99%	78.13%	66.40%	78.74%	55.56%	97.78%	51.20%	58.73%
非常に有益である	**33.17%**	33.86%	39.84%	32.00%	36.22%	21.43%	52.59%	21.60%	26.19%
ある程度有益である	**35.82%**	29.13%	38.28%	34.40%	42.52%	34.13%	45.19%	29.60%	32.54%
それほど有益ではない	**18.25%**	19.69%	14.84%	20.00%	15.75%	23.02%	2.22%	32.80%	19.05%
まったく有益ではない	**8.73%**	11.02%	6.25%	10.40%	3.94%	14.29%	0.00%	12.80%	11.90%
有益ではない (合計)	**26.99%**	30.71%	21.09%	30.40%	19.69%	37.30%	2.22%	45.60%	30.95%
該当なし	**4.02%**	6.30%	0.78%	3.20%	1.57%	7.14%	0.00%	3.20%	10.32%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

コンテナ・セキュリティ・テスト	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**66.93%**	48.82%	79.69%	73.60%	74.80%	57.94%	91.11%	57.60%	50.00%
非常に有益である	**29.93%**	20.47%	38.28%	29.60%	39.37%	24.60%	49.63%	21.60%	14.29%
ある程度有益である	**37.00%**	28.35%	41.41%	44.00%	35.43%	33.33%	41.48%	36.00%	35.71%
それほど有益ではない	**18.65%**	29.13%	13.28%	14.40%	17.32%	19.84%	6.67%	24.00%	25.40%
まったく有益ではない	**9.42%**	14.96%	3.91%	8.80%	6.30%	18.25%	1.48%	12.80%	9.52%
有益ではない (合計)	**28.07%**	44.09%	17.19%	23.20%	23.62%	38.10%	8.15%	36.80%	34.92%
該当なし	**5.00%**	7.09%	3.13%	3.20%	1.57%	3.97%	0.74%	5.60%	15.08%

脆弱性 / リスク管理ツール (例 : XDR、SRM など) の使用	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**69.77%**	58.27%	82.81%	74.40%	74.02%	57.14%	97.78%	53.60%	57.94%
非常に有益である	**32.58%**	24.41%	47.66%	35.20%	41.73%	22.22%	50.37%	20.00%	17.46%
ある程度有益である	**37.19%**	33.86%	35.16%	39.20%	32.28%	34.92%	47.41%	33.60%	40.48%
それほど有益ではない	**17.86%**	21.26%	8.59%	19.20%	22.05%	19.05%	1.48%	27.20%	25.40%
まったく有益ではない	**9.62%**	16.54%	7.03%	5.60%	1.57%	20.63%	0.74%	16.00%	9.52%
有益ではない (合計)	**27.48%**	37.80%	15.63%	24.80%	23.62%	39.68%	2.22%	43.20%	34.92%
該当なし	**2.75%**	3.94%	1.56%	0.80%	2.36%	3.17%	0.00%	3.20%	7.14%

修正の優先順位付け	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**67.12%**	53.54%	82.81%	67.20%	71.65%	53.97%	96.30%	56.80%	52.38%
非常に有益である	**29.83%**	21.26%	40.63%	24.80%	36.22%	21.43%	54.07%	21.60%	16.67%
ある程度有益である	**37.29%**	32.28%	42.19%	42.40%	35.43%	32.54%	42.22%	35.20%	35.71%
それほど有益ではない	**18.45%**	28.35%	7.81%	19.20%	22.05%	19.84%	3.70%	24.00%	23.81%
まったく有益ではない	**9.91%**	9.45%	7.03%	10.40%	5.51%	17.46%	0.00%	12.00%	18.25%
有益ではない (合計)	**28.36%**	37.80%	14.84%	29.60%	27.56%	37.30%	3.70%	36.00%	42.06%
該当なし	**4.51%**	8.66%	2.34%	3.20%	0.79%	8.73%	0.00%	7.20%	5.56%

ソフトウェア・サプライチェーンの管理 / 監視	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
有益である (合計)	**69.28%**	59.84%	72.66%	71.20%	77.95%	58.73%	95.56%	56.00%	60.32%
非常に有益である	**32.29%**	24.41%	36.72%	33.60%	32.28%	25.40%	57.04%	19.20%	27.78%
ある程度有益である	**37.00%**	35.43%	35.94%	37.60%	45.67%	33.33%	38.52%	36.80%	32.54%
それほど有益ではない	**18.84%**	22.83%	17.19%	17.60%	18.11%	23.81%	3.70%	31.20%	17.46%
まったく有益ではない	**8.34%**	11.81%	7.81%	10.40%	1.57%	10.32%	0.74%	11.20%	13.49%
有益ではない (合計)	**27.18%**	34.65%	25.00%	28.00%	19.69%	34.13%	4.44%	42.40%	30.95%
該当なし	**3.53%**	5.51%	2.34%	0.80%	2.36%	7.14%	0.00%	1.60%	8.73%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q7 貴社における現在のソフトウェア・セキュリティ・プログラム / イニシアティブの成熟度を最もよく表すものを選択してください

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
レベル 1: 構造化されていない / 体系的ではない	**8.54%**	11.02%	3.91%	4.80%	11.02%	12.70%	2.22%	10.40%	12.70%
レベル 2: 特定のチームのセキュリティ・プロセスは文書化されており、繰り返し可能である	**24.14%**	28.35%	23.44%	16.00%	29.13%	26.19%	9.63%	34.40%	26.98%
レベル 3: レベル 2 のプロセスおよび手順が組織全体で標準化されている。リーダーシップにより、積極的なセキュリティ文化が支持され伝達されている	**34.25%**	33.07%	38.28%	40.00%	35.43%	36.51%	21.48%	33.60%	36.51%
レベル 4: セキュリティ・プロセスおよび対策がロギング、管理、監視されている	**24.53%**	22.05%	20.31%	28.00%	14.96%	21.43%	48.89%	20.00%	19.05%
レベル 5: セキュリティ・プロセスが継続的に分析されて改善されている	**8.54%**	5.51%	14.06%	11.20%	9.45%	3.17%	17.78%	1.60%	4.76%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q8 ビジネスに不可欠なアプリケーションのセキュリティを評価またはテストする頻度は平均でどの程度ですか

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
毎日	**7.07%**	3.94%	8.59%	19.20%	4.72%	3.17%	3.70%	2.40%	11.11%
1 週間あたり 4 ～ 6 日	**17.17%**	15.75%	16.41%	15.20%	11.81%	11.11%	37.04%	11.20%	17.46%
1 週間あたり 2 ～ 3 日	**20.41%**	18.90%	21.09%	28.00%	14.96%	20.63%	27.41%	14.40%	17.46%
毎週 1 回	**16.98%**	16.54%	15.63%	14.40%	18.11%	16.67%	17.78%	19.20%	17.46%
2 ～ 3 週間に 1 回	**11.09%**	11.02%	12.50%	5.60%	18.11%	12.70%	5.19%	14.40%	9.52%
毎月 1 回	**7.16%**	6.30%	4.69%	5.60%	12.60%	7.94%	5.19%	5.60%	9.52%
2 か月に 1 回	**7.46%**	7.87%	7.81%	3.20%	11.02%	3.97%	2.22%	18.40%	5.56%
3 ～ 5 か月に 1 回	**6.38%**	7.87%	10.16%	5.60%	3.15%	7.14%	1.48%	7.20%	8.73%
6 ～ 11 か月に 1 回	**4.42%**	7.87%	2.34%	1.60%	4.72%	10.32%	0.00%	6.40%	2.38%
毎年 1 回	**1.67%**	2.36%	0.78%	1.60%	0.79%	6.35%	0.00%	0.80%	0.79%
1 年に 1 回未満 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
実施していない	**0.20%**	1.57%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q9 ビジネスに不可欠なアプリケーションのセキュリティをどのような方法で評価またはテストしていますか (当てはまるものをすべて選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
手動評価と自動評価の組み合わせ	**52.61%**	50.40%	65.63%	44.80%	50.39%	51.59%	68.89%	47.20%	40.48%
外部ペネトレーション・テスト	**44.15%**	37.60%	39.06%	40.00%	43.31%	47.62%	63.70%	45.60%	34.92%
自動化された評価およびテスト	**43.66%**	40.00%	46.88%	39.20%	42.52%	45.24%	68.15%	29.60%	35.71%
手動による評価および / またはテスト (ペネトレーション・テストは除く)	**43.07%**	36.00%	46.88%	37.60%	46.46%	44.44%	58.52%	33.60%	39.68%
知らない / わからない	**0.20%**	0.00%	0.00%	0.80%	0.79%	0.00%	0.00%	0.00%	0.00%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q10 過去 1 年間に (2022 ～ 2023 年)、重大なセキュリティ / 脆弱性の課題への対処によって、組織のソフトウェア・デリバリー・スケジュールに及んだ影響はどの程度でしたか (影響があった場合)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
影響があった (合計)	**81.06%**	**72.44%**	**86.72%**	**80.00%**	**92.91%**	**89.68%**	**79.26%**	**80.80%**	**66.67%**
大きな影響があった	**38.37%**	24.41%	41.41%	33.60%	33.86%	54.76%	60.74%	24.80%	31.75%
小さな影響があった	**42.69%**	48.03%	45.31%	46.40%	59.06%	34.92%	18.52%	56.00%	34.92%
影響はあまりなかった	**17.17%**	25.20%	12.50%	17.60%	7.09%	7.94%	20.00%	18.40%	28.57%
影響はまったくなかった	**1.77%**	2.36%	0.78%	2.40%	0.00%	2.38%	0.74%	0.80%	4.76%
影響はなかった (合計)	**18.94%**	**27.56%**	**13.28%**	**20.00%**	**7.09%**	**10.32%**	**20.74%**	**19.20%**	**33.33%**

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q11 組織内でセキュリティ・テスト実施の責任を負っているのは誰ですか (当てはまるものをすべて選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
内部セキュリティ・チーム	**46.03%**	39.37%	50.00%	36.80%	41.73%	38.89%	67.41%	46.40%	46.03%
開発者 / ソフトウェア・エンジニア	**45.14%**	34.65%	53.13%	33.60%	44.88%	42.86%	63.70%	44.00%	42.86%
QA/ テスト・チーム	**37.59%**	41.73%	35.94%	32.80%	33.86%	38.89%	51.11%	34.40%	30.95%
部門横断的な DevSecOps チーム	**35.53%**	31.50%	44.53%	28.80%	39.37%	30.95%	48.15%	32.00%	27.78%
外部コンサルタント	**32.88%**	29.92%	46.09%	28.00%	28.35%	38.10%	32.59%	31.20%	28.57%
わからない	**0.10%**	0.00%	0.00%	0.00%	0.00%	0.79%	0.00%	0.00%	0.00%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q12 デプロイ済み / 使用中のアプリケーションで、重大なセキュリティ・リスク / 脆弱性に対するパッチ適用 / 解決までに平均でどのくらいの時間がかかっていますか

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
1 週間以内 (具体的な日数を入力してください)	**4.61%**	0.00%	7.81%	11.20%	5.51%	0.00%	6.67%	3.20%	2.38%
1 週間超、2 週間以内	**26.40%**	14.96%	21.88%	40.80%	25.98%	14.29%	57.04%	10.40%	23.81%
2 週間超、3 週間以内	**28.26%**	33.86%	28.91%	24.80%	26.77%	23.02%	29.63%	28.00%	30.95%
3 週間超、1 か月以内	**19.92%**	22.83%	19.53%	16.00%	21.26%	32.54%	4.44%	26.40%	17.46%
1 か月超、2 か月以内	**8.44%**	9.45%	5.47%	3.20%	11.81%	11.90%	1.48%	14.40%	10.32%
2 か月超、4 か月以内	**5.50%**	3.94%	5.47%	3.20%	4.72%	11.11%	0.74%	8.80%	6.35%
4 か月超、6 か月以内	**4.71%**	9.45%	10.16%	0.80%	1.57%	4.76%	0.00%	8.00%	3.17%
6 か月超 (具体的な月数を入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
わからない	**2.16%**	5.51%	0.78%	0.00%	2.36%	2.38%	0.00%	0.80%	5.56%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q13 DevSecOps アクティビティの成功を測定するために使用している主な KPI はどれですか (最大で 3 まで選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
オープンなセキュリティ脆弱性の数	**28.95%**	27.56%	32.81%	28.80%	27.56%	24.60%	40.00%	26.40%	23.02%
開発プロセス終盤でのセキュリティ関連の発見事項の削減	**28.26%**	33.07%	33.59%	24.00%	24.41%	29.37%	30.37%	30.40%	20.63%
課題解決までの時間	**27.58%**	24.41%	30.47%	28.00%	24.41%	23.02%	31.11%	25.60%	33.33%
セキュリティ課題の解決に費やされる時間の短縮	**27.38%**	27.56%	30.47%	24.00%	21.26%	34.13%	32.59%	24.80%	23.81%
セキュリティに関連するビルド遅延の削減	**26.50%**	25.98%	28.91%	28.80%	26.77%	19.84%	27.41%	26.40%	27.78%
セキュリティに不具合のあるビルドの削減	**24.44%**	22.05%	24.22%	21.60%	25.20%	27.78%	25.93%	25.60%	23.02%
コンプライアンス関連の KPI (合格した監査の割合など)	**23.75%**	30.71%	28.91%	17.60%	22.83%	26.98%	24.44%	23.20%	15.08%
顧客からの問い合わせの数 (チケット)	**22.77%**	29.13%	28.91%	25.60%	21.26%	22.22%	15.56%	25.60%	14.29%
不具合脱出率	**22.28%**	22.83%	17.19%	16.00%	30.71%	23.81%	28.15%	17.60%	21.43%
DevSecOps アクティビティの成功評価に使用している主な KPI はない	**1.08%**	0.00%	0.00%	0.00%	1.57%	0.00%	0.00%	0.80%	6.35%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q14 DevSecOps の実装に際して、どのような課題 / 障壁がありますか (当てはまるものをすべて選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
開発者 / エンジニア向けのセキュリティ・トレーニングが不十分 / 非効果的	**33.86%**	33.07%	42.97%	27.20%	31.50%	35.71%	32.59%	35.20%	32.54%
アプリケーション・セキュリティの要員 / スキルが不足している	**31.40%**	25.98%	29.69%	28.80%	23.62%	31.75%	46.67%	32.80%	30.95%
開発 / 運用作業の透明性が欠如している	**31.31%**	27.56%	37.50%	28.80%	35.43%	29.37%	36.30%	28.00%	26.98%
要件と優先順位が絶え間なく変わる	**30.42%**	25.20%	30.47%	27.20%	29.13%	27.78%	43.70%	32.80%	26.19%
セキュリティ・プログラムおよびツールの予算 / 資金が不十分	**29.44%**	30.71%	39.06%	32.80%	37.01%	23.02%	22.96%	21.60%	28.57%
開発、運用、セキュリティの間に組織の壁がある	**29.05%**	31.50%	42.19%	24.80%	28.35%	29.37%	29.63%	22.40%	23.81%
セキュリティ・チーム内のコーディング・スキルが欠如している	**28.95%**	24.41%	30.47%	26.40%	31.50%	30.95%	28.89%	29.60%	29.37%
課題 / 障壁はない	**2.06%**	4.72%	3.13%	1.60%	2.36%	0.79%	1.48%	0.00%	2.38%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q15 使用しているアプリケーション・セキュリティ・テスト・ツールに関する最大の課題は何ですか (最大で 3 まで選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
曝露、悪用の可能性、重要度に基づいて解決策が優先付けされない	**34.74%**	35.43%	41.41%	40.00%	37.01%	34.13%	35.56%	22.40%	31.75%
パフォーマンスが低すぎて迅速なリリース・サイクル / 継続的デプロイに対応できない	**34.15%**	26.77%	42.97%	33.60%	28.35%	30.16%	47.41%	40.00%	23.02%
コストに ROI が見合わない	**33.46%**	29.92%	34.38%	32.00%	38.58%	34.92%	33.33%	30.40%	34.13%
正確さ / 信頼性に欠ける	**33.07%**	25.20%	39.84%	28.80%	36.22%	33.33%	31.85%	32.00%	37.30%
誤検知が多い	**32.19%**	38.58%	39.06%	21.60%	31.50%	35.71%	29.63%	36.00%	25.40%
異なるツールの結果を統合 / 相関付けする方法がない	**28.95%**	23.62%	28.91%	22.40%	26.77%	30.95%	34.07%	28.00%	36.51%
大きな課題はない	**3.14%**	6.30%	3.13%	4.00%	2.36%	0.00%	5.19%	0.00%	3.97%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q16 セキュリティ・プログラムの成功に寄与した最大の要因はどれだと考えますか (最大で 3 つまで選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
インフラストラクチャ・アズ・コード (Infrastructure-as-code) を介したセキュリティ / コンプライアンス・ポリシーの適用	**33.56%**	36.22%	37.50%	39.20%	26.77%	26.98%	40.74%	29.60%	30.95%
開発および運用チームでのセキュリティ・チャンピオンの育成	**32.58%**	22.05%	39.06%	32.80%	28.35%	38.89%	28.15%	40.00%	31.75%
開発、運用、セキュリティ・チーム間でのコミュニケーションの改善	**32.48%**	34.65%	42.97%	27.20%	31.50%	34.13%	32.59%	34.40%	22.22%
ビルド / デプロイ・ワークフローへの自動セキュリティ・テストの組み込み	**32.29%**	28.35%	36.72%	32.00%	36.22%	33.33%	32.59%	28.00%	30.95%
脆弱性修正にかかる時間 / コストの自動化による最小化	**30.03%**	32.28%	31.25%	31.20%	23.62%	27.78%	40.74%	27.20%	25.40%
部門横断的な DevSecOps チームの設立	**28.95%**	29.92%	32.03%	21.60%	37.01%	28.57%	35.56%	26.40%	19.84%
セキュアなコーディングに関する開発者 / エンジニアのトレーニング	**27.58%**	25.20%	28.91%	20.80%	35.43%	26.98%	33.33%	21.60%	27.78%
最大の要因はない	**0.79%**	2.36%	0.00%	0.80%	0.00%	0.79%	0.74%	0.00%	1.59%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q17 現在、ソフトウェアのセキュリティ対策を強化する目的で何らかの AI ツールを使用していますか

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
はい。AI ツールを積極的に使用している	**52.50%**	38.58%	64.06%	47.20%	47.24%	69.84%	57.04%	47.20%	48.41%
いいえ。AI ツールの使用に抵抗はないが、まだ実装していない	**36.51%**	39.37%	23.44%	42.40%	47.24%	22.22%	40.00%	35.20%	42.06%
いいえ。AI ツールを実装しておらず、その予定もない	**10.99%**	22.05%	12.50%	10.40%	5.51%	7.94%	2.96%	17.60%	9.52%
いいえ (合計)	**47.50%**	**61.42%**	**35.94%**	**52.80%**	**52.76%**	**30.16%**	**42.96%**	**52.80%**	**51.59%**

Q18 AI ツールの使用は、DevSecOps プロセスおよびワークフローにどのような影響を与えると思いますか (当てはまるものをすべて選択)

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
セキュリティ対策の効率と精度が上がる	**53.69%**	51.52%	58.93%	49.11%	44.17%	43.97%	68.70%	57.28%	54.39%
ソフトウェア・セキュリティが複雑になり、技術要件が上がる	**52.04%**	51.52%	64.29%	42.86%	50.83%	54.31%	61.83%	47.57%	41.23%
セキュリティ・データを手動でレビューし分析する必要性が減る	**48.40%**	50.51%	45.54%	42.86%	50.83%	45.69%	64.12%	42.72%	42.11%
大きな影響はない	**0.88%**	0.00%	0.00%	0.89%	0.83%	2.59%	0.00%	0.00%	2.63%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Q19 AI ツールの使用は、どのソフトウェア・セキュリティ領域の強化に最も効果的だと考えますか

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
脅威の検出と予防	**45.09%**	42.42%	50.00%	46.43%	46.67%	41.38%	44.27%	46.60%	42.98%
脆弱性のスキャンとテスト	**44.21%**	39.39%	46.43%	45.54%	46.67%	37.07%	52.67%	42.72%	41.23%
ID およびアクセス管理	**42.01%**	43.43%	50.00%	44.64%	38.33%	37.93%	54.20%	33.98%	31.58%
コンプライアンスおよび規制管理	**41.57%**	47.47%	46.43%	31.25%	42.50%	36.21%	45.04%	37.86%	45.61%
その他 (具体的に入力してください)	**0.00%**	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

概要
2023 年シノプシス DevSecOps 調査の主な発見事項
2023 年の DevSecOps の現状
調査結果からの学び
調査対象者の属性
付録

Q20 AI ベースのセキュリティ・ソリューションにバイアスまたは誤りが含まれる可能性について、どの程度懸念していますか

	グローバル	イギリス	米国	フランス	フィンランド	ドイツ	中国	シンガポール	日本
懸念している (合計)	**76.63%**	**76.77%**	**83.93%**	**74.11%**	**77.50%**	**84.48%**	**55.73%**	**82.52%**	**81.58%**
非常に懸念している	**25.36%**	27.27%	33.04%	16.96%	15.83%	50.00%	7.63%	28.16%	27.19%
ある程度懸念している	**51.27%**	49.49%	50.89%	57.14%	61.67%	34.48%	48.09%	54.37%	54.39%
どちらでもない / わからない	**16.21%**	15.15%	10.71%	22.32%	18.33%	8.62%	28.24%	12.62%	11.40%
それほど懸念していない	**5.95%**	6.06%	4.46%	2.68%	3.33%	6.03%	13.74%	3.88%	6.14%
まったく懸念していない	**1.21%**	2.02%	0.89%	0.89%	0.83%	0.86%	2.29%	0.97%	0.88%
懸念していない (合計)	**7.17%**	**8.08%**	**5.36%**	**3.57%**	**4.17%**	**6.90%**	**16.03%**	**4.85%**	**7.02%**

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。