GitGuardian

Voice Of Practitioners

AppSecにおけるシークレットの現状

シークレットのスプロール化およびリスク軽減について
IT分野の意思決定者507名から得られた知見

ここ数年、シークレットはソフトウェア開発サイクルの至るところに存在するようになり、その数は過去最高となっています。シークレットは、ソフトウェアアプリケーションのビルディングブロックを互いに結び付ける役割を果たし、認証や承認、暗号化といった、重要セキュリティ対策の基盤となっています。実際、デジタルID管理やアクセス管理は、シークレットに大きく依存している状態です。

今年初旬に公開した、GitGuardianの「2023 State of Secrets Sprawl」では、ソースコード中のシークレットについて再度注意喚起を行いました。2022年には、1,000万件ものシークレットがGitHubで検出されており（2021年比で67%増）、スキャンを実施した新規コミットは全部で10.27億件を超えました。

近年注目を集めた、シークレット絡みのサイバーセキュリティインシデントでは、大手テック企業にも被害が及んでおり、シークレットを大規模環境で管理することの難しさが浮き彫りになっています。

コードのセキュリティやサプライチェーンのレジリエンシーに対する関心も大分高まってきているとはいえ、新たなランドスケープに合わせてセキュリティポスチャー（姿勢）を変えるということは、至難のわざと言えるでしょう。

GitGuardianでは今年、開発現場における問題の認知状況およびセキュリティ責任者が直面する障害について正確な状況把握を得ようと、Sapio Research社との提携により、ソースコードに書きこまれたシークレットのリスクと軽減策に関するフィールド調査を実施しました。

これと併せて、米国・英国の**IT分野の意思決定者**（IT部門の責任者、IT担当VP、CIO、CSO、CISO、サイバーセキュリティ担当VP等）**507名**から得られた回答について分析を実施しました。以下は、こうした調査・分析の結果です。

エグゼクティブサマリー

今回の調査から得られた重要な知見

75%
シークレット流出の経験があると回答した人の割合

60%
流出の影響が、会社または自社の従業員に及んだと回答した人の割合

47%
「ハードコードされたシークレット」を自社のソフトウェアサプライチェーンにおける重要なリスクポイントとみなしていると回答した人の割合

27%
実はハードコードされたシークレットの検出は人手に頼っていると回答した人の割合

53%
シークレットはメッセージングアプリで平文形式で共有されていると考えている経営幹部の割合（例: CSO、CISO、サイバーセキュリティ担当VP）

94%
今後12～18か月で自社のシークレットに関する慣習を改めたいと回答した人の割合

26%
2023年はシークレット検出と修復に投資するつもりだと回答した人の割合

フィールド調査

シークレット流出によるリスクは業界で認知されている

本フィールド調査の一番の目的は、DevOps環境におけるシークレット流出がもたらすリスクについての認知状況の評価でした。「貴組織においてシークレット（APIキーやユーザー名＋パスワード、暗号キー等）流出の影響を受けたあるいはその事実の報告を受けたことはありますか？」と尋ねたところ、次のような結果が得られました：

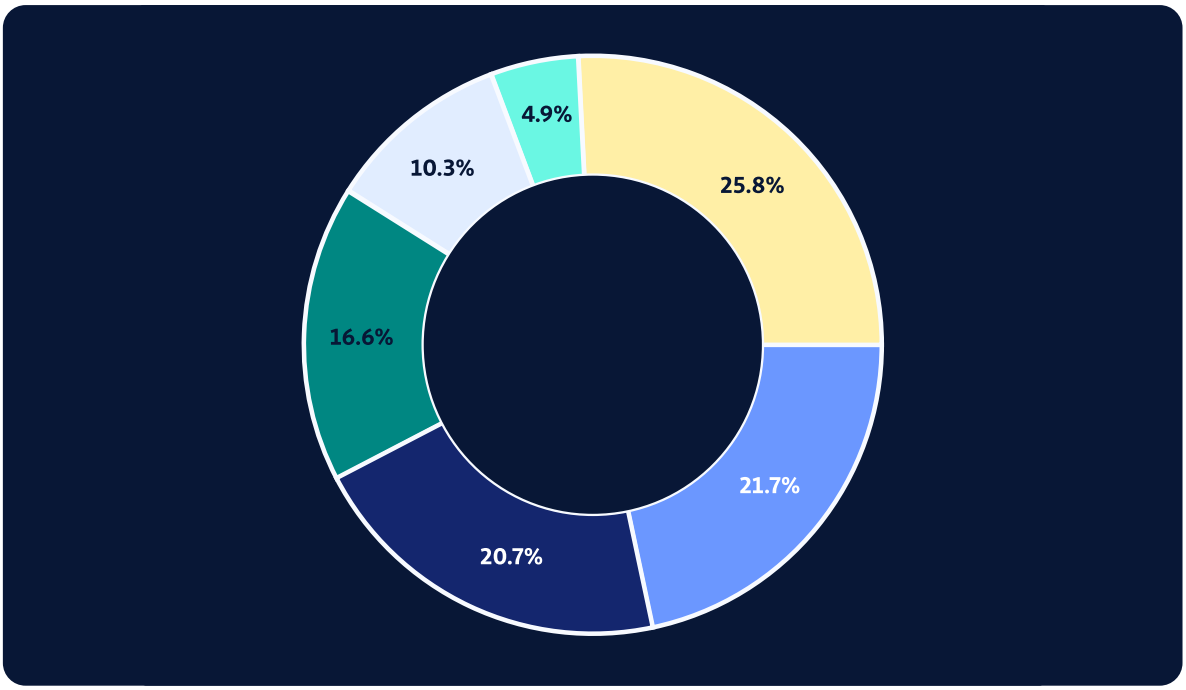
75%

過去にシークレットの流出が発生したと回答した人の割合

60%

会社、従業員、あるいはその両方に問題が生じたと回答した人の割合

貴組織においてシークレット（APIキーやユーザー名＋パスワード、暗号キー等）流出の影響を受けたあるいはその旨の報告を受けたことはありますか？



- ある。流出が発生したことは知っているが、影響についてはよくわからない。
- ある。流出が発生したことは知っているが、影響は受けていない。
- ある。流出が発生したことは知っており、会社と従業員の両方に問題が生じた。
- ある。流出が発生したことは知っており、会社に被害が生じた。（技術的な混乱、金銭的損失、ブランドイメージの損失等）
- ある。流出が発生したことは知っており、従業員の問題が生じた。
- ない。

ソフトウェアサプライチェーンにおける重要リスクポイントについて尋ねたところ、次のような結果が得られました：

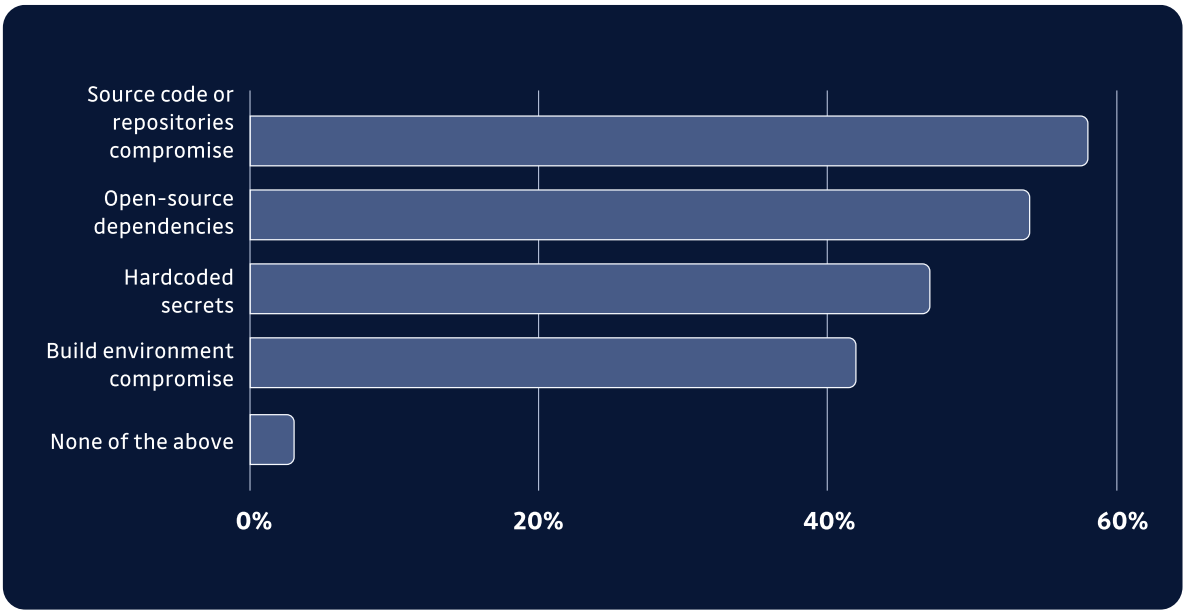
58%

「ソースコードとリポジトリ」と回答した人の割合

47%

「ハードコードされたシークレット」と回答した人の割合

貴組織のソフトウェアサプライチェーンにおける重要リスクポイントは何だとお考えですか？どれですか？ 3つまで選んでください



つまり、回答者の大多数が、**シークレットの保護**をアプリケーション**リスク管理**における**必須**要素の一つと考えているということになります。

ソフトウェア開発における最低セキュリティ基準

「コード中で、ハードコードされたパスワードや暗号のためのプライベートキーの有無を検証するには、ヒューリスティックタイプのツール[1]の利用を推奨する。こうしたツールが向いているのは、機能やサービスに条件設定のための専用インターフェイスが用意されているためである。動的テストでは、このような好ましくないコードを検出できない可能性がある。」

米国NISTソフトウェア検証の最低基準に関するガイドライン[2]

“「認証情報等の機密データは、組織のどこであっても平文形式で保管しない。また、アクセスできるのは認証・許可された正規ユーザーに限定する。認証情報は、クレデンシャル/パスワードマネージャーやボールトといった特権アカウントの管理ソリューションを使って安全に保管する。」“

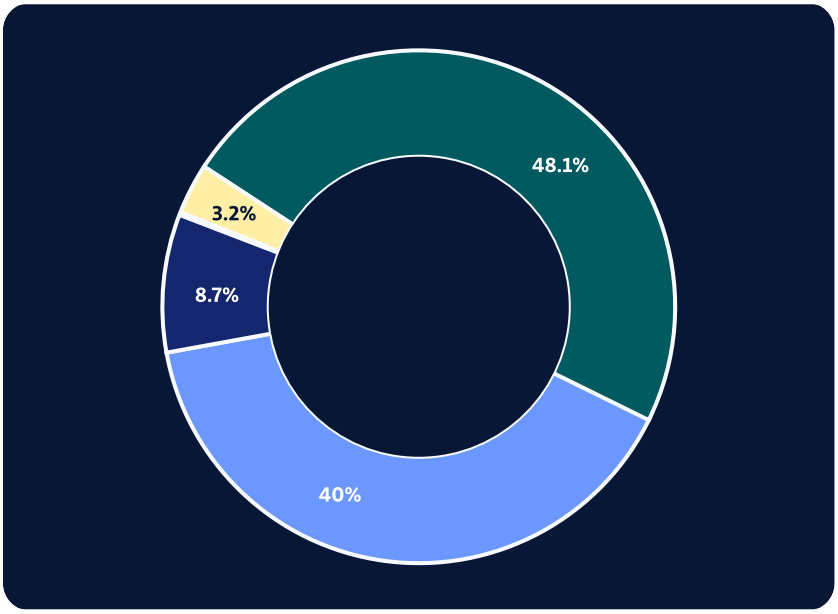
米国 CISAサイバーセキュリティ・パフォーマンス目標(CPG)チェックリスト[3]

バイデン政権下では、インフラのサイバーレジリエンスおよび専門家強化の施策が増えています。中でも記憶に新しいのが、国家サイバーセキュリティ戦略です。今のところ、こうした勧告に義務はありません。ただし、近いうちに変わる可能性があります。米ホワイトハウスは、ソフトウェアベンダーのアカウンタビリティならびに「市場原理形成」に注力することで、安全なソフトウェア開発の実践を促進していくことを確約しているからです。

[1] ヒューリスティック手法とは、不確実さの考慮を想定した手法である。
[2] Guidelines on Minimum Standards for Developer Verification of Software
[3] https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf

シークレット管理の成熟度は足並みが揃っていない

「今現在、シークレットの流出をどの程度防げていると思いますか？」という設問に対し、回答者の48%が「かなり」防げていると回答しています。



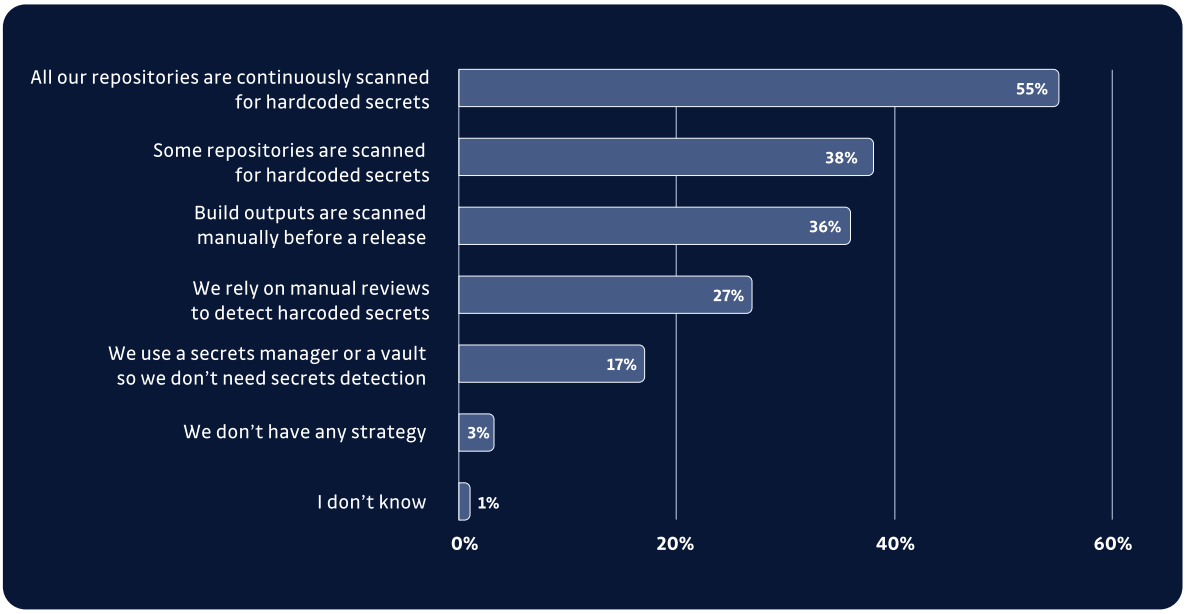
今現在、シークレットの流出をどの程度防げていると思いますか？1つ選択してください。

- かなりできている
- ある程度できている
- ほとんどできていない
- 全くできていない

ただし、ほかの設問に対する回答を見ると、もう少し複合的な見方が可能です。たとえば、ハードコードされたシークレットに対する戦略について尋ねたところ、次のような結果が得られました：

回答者のうち
- 27%が「ハードコードされたシークレットの検出は手作業による確認に頼っている」と回答
- 17%が「シークレットマネージャーあるいはボールトを使っているので、シークレット検出は不要」と回答
- 3%が「戦略は立てていない」と回答

ソースコードに書きこまれたシークレットに対する貴組織の戦略について、最も適切に言い表しているのは次のうちどれですか？記述として最も当てはまるものはどれですか？
当てはまるものすべてを選択してください

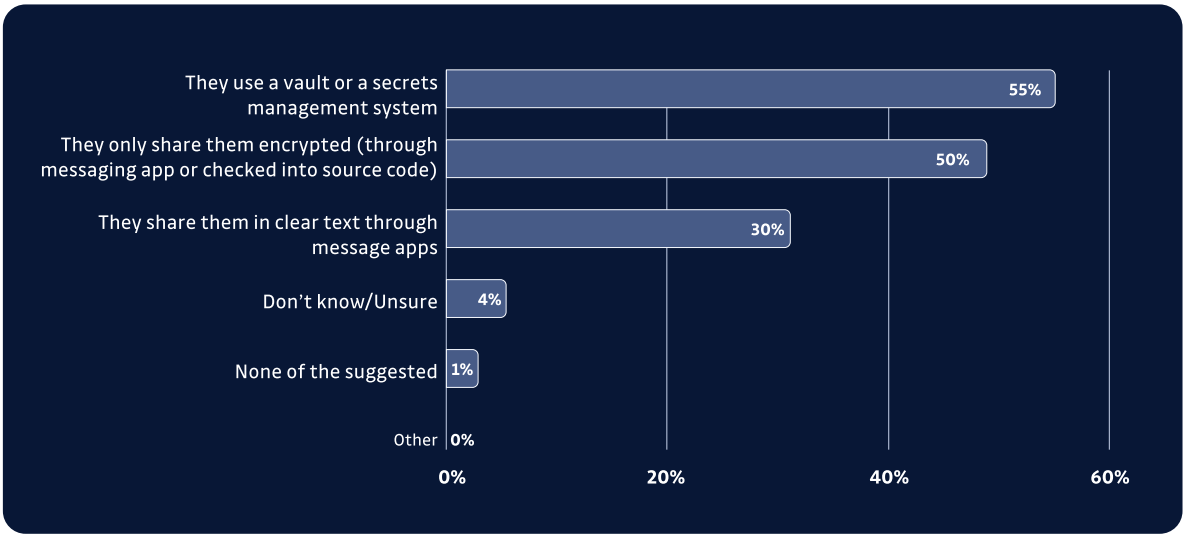


93%が「すべて」あるいは「一部」のリポジトリでハードコードされたシークレットの有無を継続的にスキャンしていると回答しています。ただし、その前の結果を見ると、シークレット流出防止の能力は過大評価されている可能性もあります。

ソースコードにシークレットが書きこまれていないかどうかを検出する場合、手作業によるコードレビューでは不十分です。レビュー対象となるのはコードベースの直近のバージョンであり、シークレットが書き込まれている可能性のある過去の改訂版は対象にならないためです(**これについての詳細はこちらでご覧いただけます**)シークレットマネージャーの使用については、確かに重要ではあるものの、シークレット流出の対策にはなりません。シークレット管理と検出は、互いに補完し合う関係にある機能です。

同様に、「今現在、貴組織の開発チームは、アプリケーションの開発時、どのような方法でパスワードやシークレットを共有していますか？」という設問に対し、回答者の30%が「メッセージングアプリを使って平文形式で共有している」と答えており、シニアセキュリティマネジメントの下位グループ（例：サイバーセキュリティ担当のCSO、CISO、VP）については53%が同様の回答をしています！

今現在、貴組織の開発チームは、アプリケーションの開発時、どのような方法でパスワードやシークレットを共有していますか？
当てはまるものすべてを選択してください

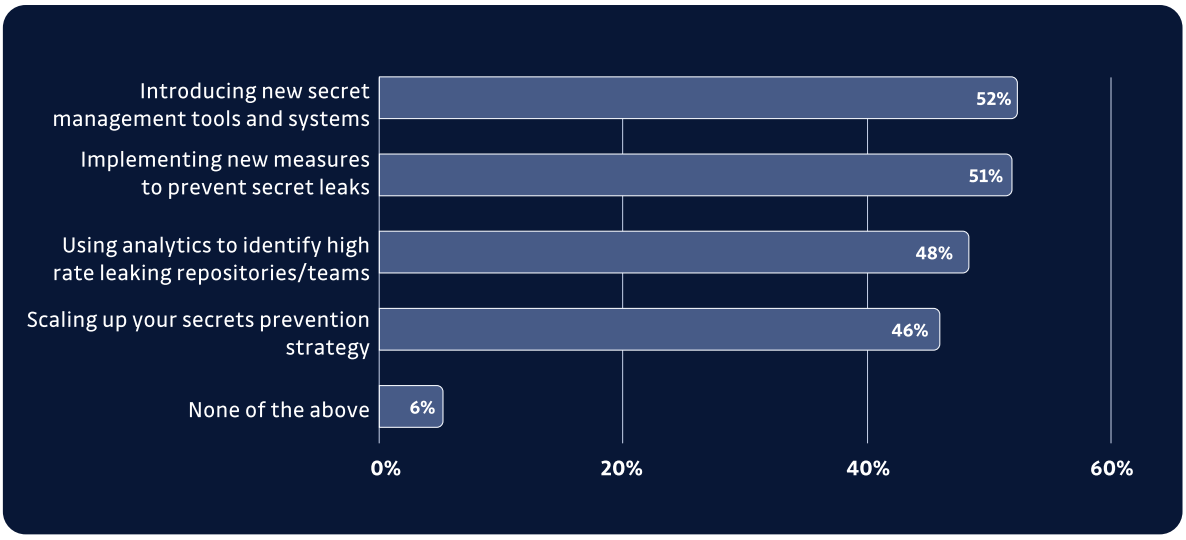


全リポジトリでハードコードされたシークレットを継続的にスキャン

[シークレット管理成熟度モデル](#)と比較した場合、こうした回答は、回答者のかなりの部分で、運用上の成熟度が低く、成熟度スケールの一番低いレベルに相当することを示しています。

ただし、明るい側面もあります。**回答者の94%が、「今後12～18か月以内に何らかの形でシークレットの慣習を改善するつもりであると答えています。**

今後12～18か月以内に以下のいずれかの実行を検討していますか？
当てはまるものすべてを選択してください



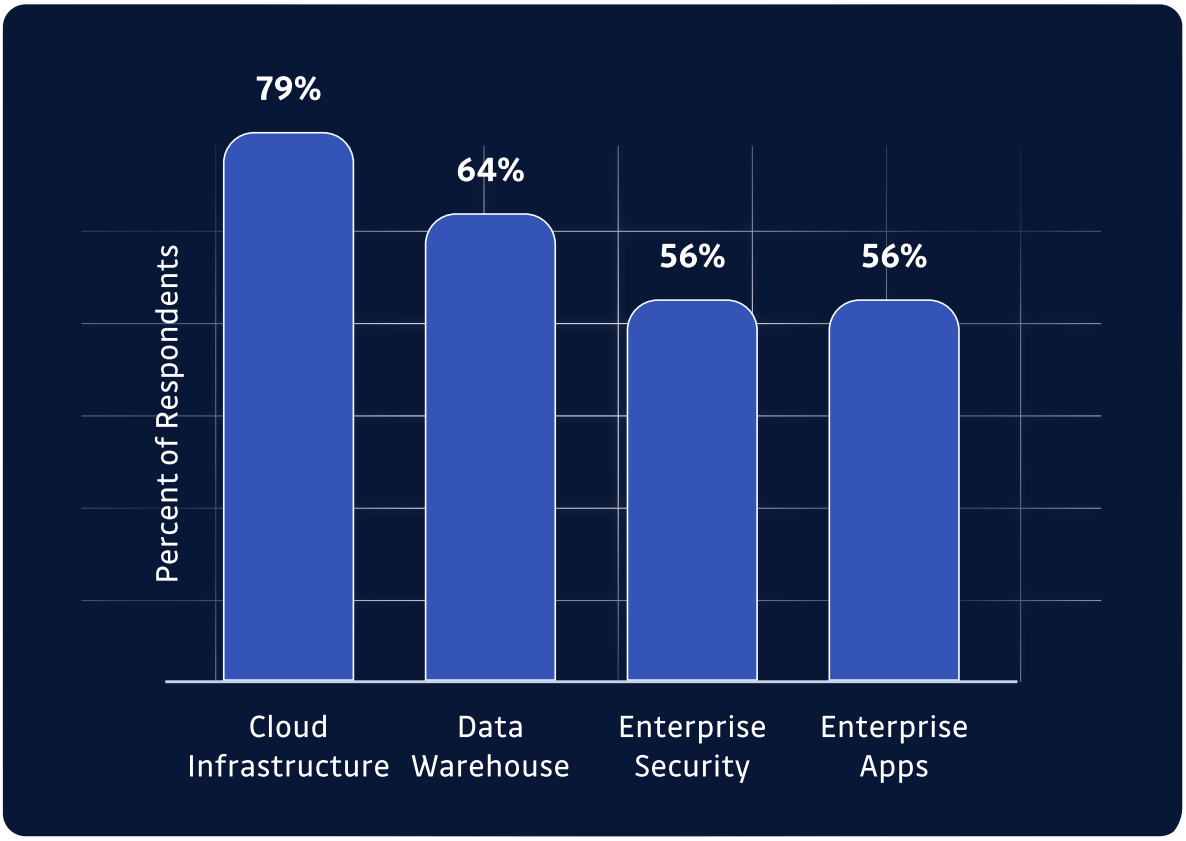
セキュリティ投資予算の短期的優先事項

一部、経済の見通しに不確実性があるものの、大企業のセキュリティ予算は安定した状況が続いており、特に企業セキュリティといった支出の優先事項においては顕著です。以下は Battery社2023年度第1四半期クラウドソフトウェア支出調査 で報告された調査結果からの引用です。

報告書には次の記述があります：「予算は相対的に見て弾力性に乏しい：マクロレベルでは逆風が続くものの、経営幹部である回答者の46%が、テクノロジーに対する予算総額を増やす予定である。」

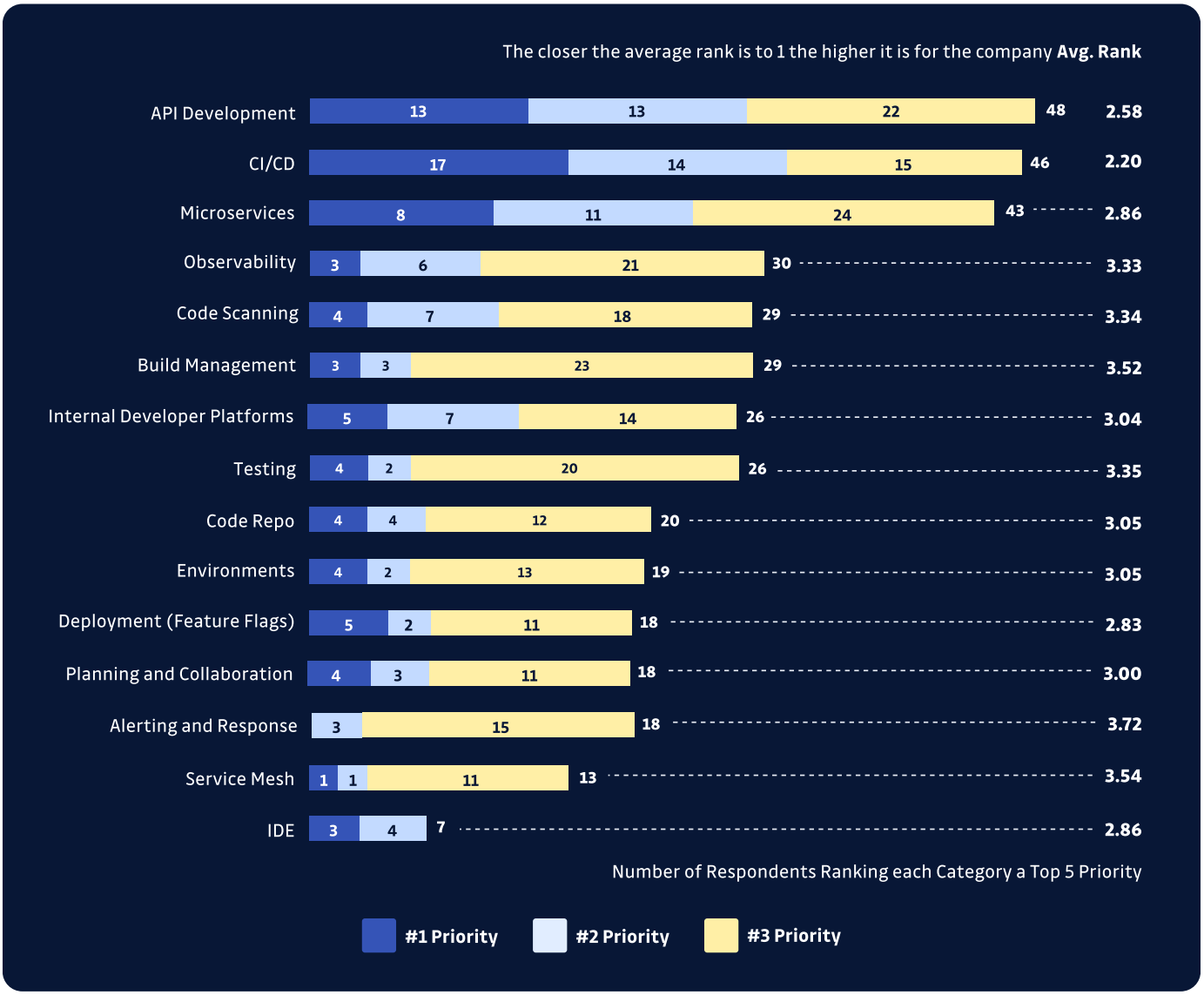
中でも企業セキュリティは、経営幹部が今後12か月で最も重視したい投資カテゴリ第3位となっています：「経営幹部の多くは優先事項トップ5のうち、特にインフラソフトウェア、エンタープライズセキュリティ、企業の基幹アプリケーションを重要視している。」

経営幹部が今後12ヵ月で最も重視したいカテゴリトップ5



「企業がコードの効率化による信頼性のある運用実現に注力する中、スピード、安全性、レジリエンシーは開発ツールの最優先事項となっています。AppSecとオブザーバビリティ（可観測性）は開発チームとセキュリティチームで分担されています。」

開発ツールに関する企業の重点事項トップ 5 企業ランキング

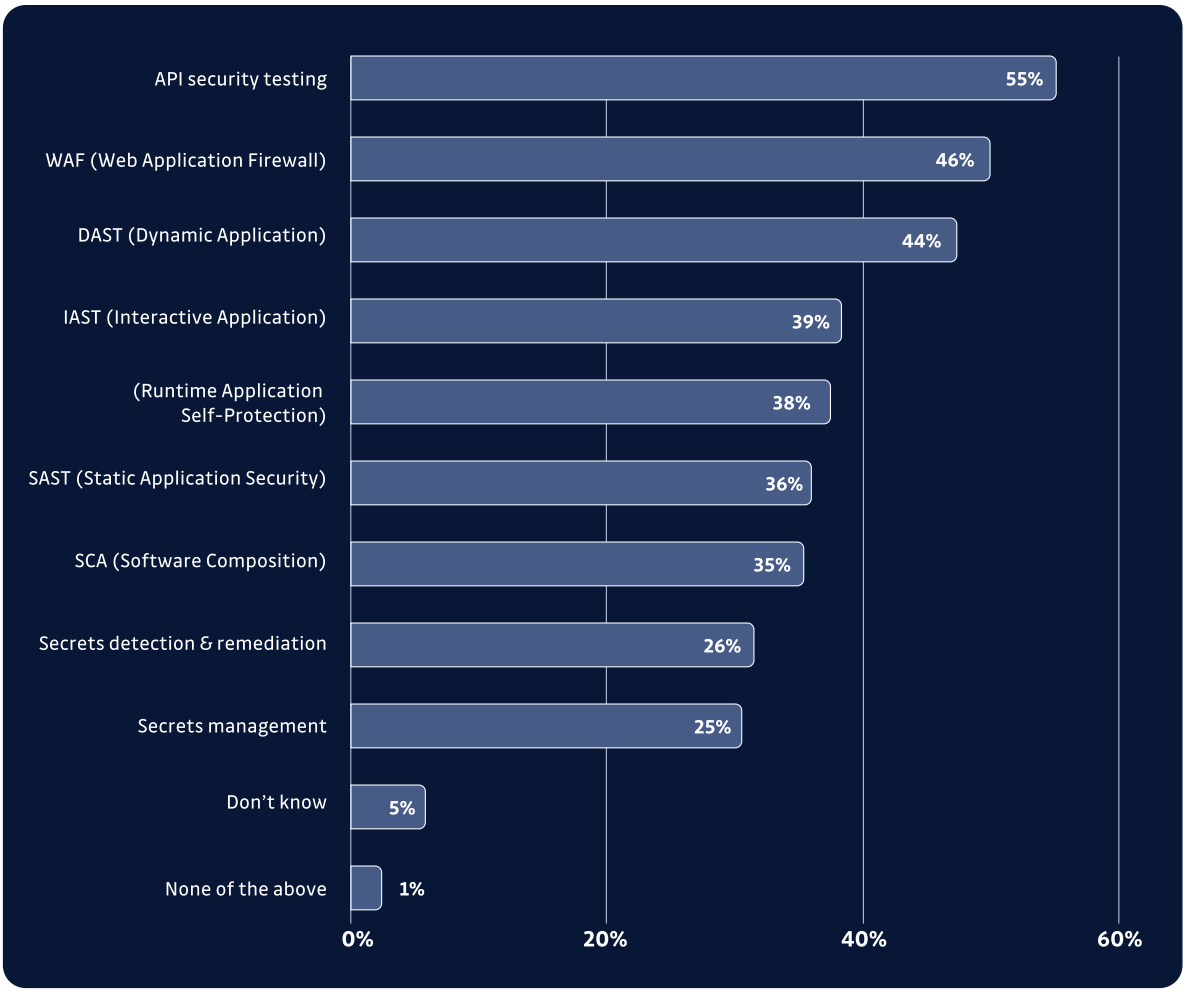


AppSecの余力の確保には優先順位の見直しが必要である

優先順位の観点で調査から判明したことは、ランタイム保護ツールといったほかのツールと比べてシークレット検出・修復やシークレット管理の優先度があまり高くないという点です（投資面で）。

意思決定者のほぼ半数が、ランタイム保護全体と比較してシークレット保護に投資したいと回答しています：

2023年はどのアプリケーションセキュリティツールに投資する予定ですか？
当てはまるものすべてを選択してください



AppSecが最も時間を割いている業務トップ3について尋ねる設問では、回答者の21%が「ハードコードされたシークレットへの対応」をトップ3に挙げており、回答者の半数が「セキュリティツールの実行あるいはコードレビュー」を選択しています。

AppSecが最も時間を割いている業務トップ3について尋ねる設問では、回答者の21%が「ハードコードされたシークレットへの対応」をトップ3に挙げており、回答者の半数が「セキュリティツールの実行あるいはコードレビュー」を選択しています。

本当に必要とされているのは、AppSecチームの余力の確保です。組織は、アラート疲れの軽減を図りながら、AppSecチームの業務効率化も図る必要があります。昨年当社が発表した報告によると、AppSecエンジニア一人が毎年対応するハードコードされたシークレットの出現件数は平均で3,413件です。戦略の中には、検出、修復、防止を大規模展開した場合、こうした負担の軽減において効果を発揮しているものもあります。

検出・修正・防止を大規模展開する

2022年、GitGuardianはある大手企業と業務提携を行いました。多角的な手法によるシークレット流出防止支援が目的です。開発者が7,500名、監視対象のソースは50,000件、この企業が求めていたのは、堅牢かつスケーラブルなソリューションです。

本セクションでは、検出、防止、修復の大規模展開について詳しく見ていくことにします。また、GitGuardianのサービスの効果と、この企業の機密情報保護にどう役立ったかを事例を交えながら詳しく説明していきます。

Prevention

セキュリティネットを大規模展開する上で、帽子は重要要素の一つです。ハードコードされたシークレットは、開発ライフサイクルの先に行けば行くほど修復にコストがかかります。これについては、修復のセクションで紹介します。**まず、シークレットをハードコードさせないことが、セキュリティ負債の蓄積を抑制する最善の方法です。**

シークレット検出の効果が最も期待できるのは、コード書き込みのタイミングに最も近い、**コミット前の段階** です。機密情報がほかシステムに拡散する前であるため、修復作業はものの数秒もかかりません。

GitGuardianの支援では、この企業の大規模開発者基盤に対し、pre-commitフックの段階的デプロイを支援しました。その結果、**10か月でGitGuardianパーソナルアクセストークンを受け入れた開発者は3倍になりました。**

パーソナルアクセストークン とは、開発者に配布されるトークンで、これにより当社のシークレットスキャンソリューションを自身のローカルマシンにインストールすることができ、またセキュリティの強化を図ることができる。

シフトレフトの進捗と防止フェーズにおける責任共有モデルのプラスの効果を計測することは、AppSec計画の効果を評価する上で重要なアプローチといえます。

検出は重要です。しかし、セキュリティに関していえば、検出も全体を構成する一要素にすぎません。別の重要要素として、あらゆる脆弱性あるいは検出された脅威にフルに対応するためかなりの労力を必要とする、修復があります。

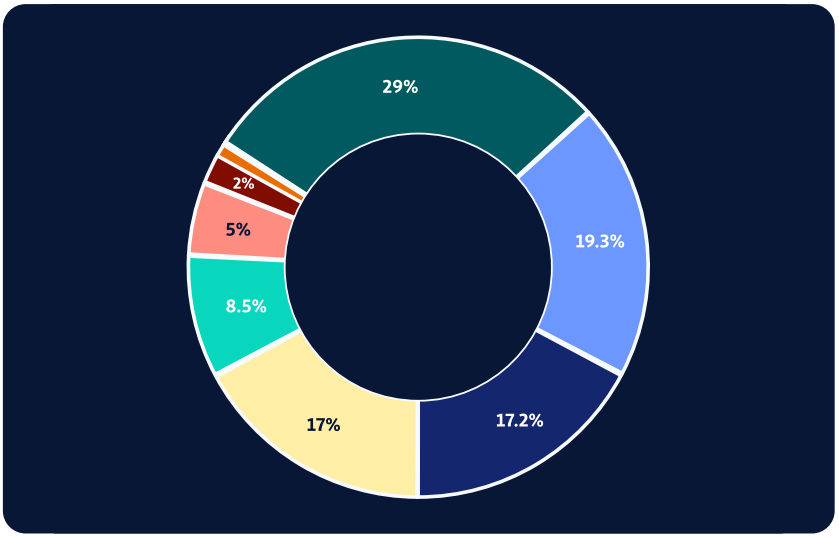
修復：意外に複雑な作業

セントラルリポジトリでシークレットの流出が検出された場合、AppSecエンジニアは調査を実施した上で、その重大度に応じて修復作業の優先順位付けを行う必要があります。情報に基づいて作業の進め方を決める上で、背景情報の収集も欠かせません。残念なことに、こうした工程は部署間の軋轢によりうまくいかないことが少なくありません。

修復作業の課題について理解を深めるため、重要指標をいくつか確認してみましょう。

出現

GitGuardianの監視委対象であるすべての事業用リポジトリを分析したところ、**インシデントあたりの平均出現数は41**であることがわかりました。ただし、この数字は外れ値の可能性も含まれるため注意が必要です。とはいうものの、この指標からは、 AppSecワークフローの効率化を図る上で、**複数の流出を1つの作業単位にグループ化**できることの重要性が見えてきます。この分布状況を可視化するため、以下の図ではインシデントあたりの出現件数を表わしています。



GitGuardianで検出したインシデントの検証を行ったところ、ほぼ半数が以下のいずれかが原因であると考えることができます：

- 削除コミットが原因の2件の出現または
- オーサーが認識していない、あるいは気にしていないハードコードされたシークレットが原因の1件の出現

ファイル

ただし、出現件数は考慮すべき要素の一つにすぎません。インシデントが複数ファイルに分散した状態も、もう一つの複雑性要素といえます。**インシデント1件あたり、平均で3.95個のファイルに分散**しており、インシデントの3分の1が複数ファイルにまたがって発生しています。このことが、修復工程の軋轢が増す要因にもなっています。

リポジトリ

さらに、**インシデントの17%で出現が複数リポジトリにまたがっています。**インシデントがある場所では解決済みになっているのに別の場所では漏えいが発生しているといった状態を避ける上で、リポジトリあるいはバージョン管理システムをすべて監視することがいかに重要かということがわかります。

上記の要素を総合すると、セキュリティインシデントの**すべての側面**に対応する、包括的な修復アプローチの必要性が見えてきます。

開発者の力をかりて修復作業を大規模展開する

修復フェーズは、セキュリティ作業の大半をハードコードされたシークレットの流出後に行います。このフェーズは第一印象より複雑になることが多く、1つのミスがCI/CDパイプラインの中断や運用停止といった重大な状況を招くことがあります。

修復作業を効果的に大規模展開するには、セキュリティエンジニアと開発・オペレーションチーム間の距離を縮めることが重要です。開発者はセキュリティエンジニアより数が多く、またコードに近いため、作業をリードする上では理想的な配置です。**開発者主導の修復の実現は、ソースコードリポジトリの安全性を確保する上で欠かせないステップの一つといえます。**

修復作業の効率化ではオートメーションもまた重要な役割を果たします。妥当性チェックとシビリティアサインメント（重大度の判定）を自動化することでインシデントのトリアージを効率化でき、イベントドリブンなプロセスを採用することで、セキュリティオーケストレーションのスピードアップが可能になります。

最期に、修復のワークフローは組織ごとに大きく異なり、開発者に明確な指示を与えるためにもセキュリティマネージャーが必要です。適切なツールとプロセスを適宜導入することで、修復作業の効率化、データ流出ほかのセキュリティインシデントリスクの低減が可能です。

企業が直面する、急速なAPIキーのスプロール化、一貫性のない設定、エンジニアリングチーム内のシークレット等が原因のリスクは非常に大きなリスクです。**シークレットは、企業の最重要資産、データにつながる出入口**となります。私たちは今、エンジニアリングチームとセキュリティチームが協力し合い、包括的なシークレット戦略を策定しなければならない**重要な時期にあります。**

シークレットのスプロール化は多くの企業が経験する問題である一方、解決が難しい問題というわけではありません。最近では、開発者のワークフローとネイティブに連携して、シークレットの管理、オーケストレーション、ローテーションを行うツールの利用も可能です。

Doppler CEO
Brian Vallelunga

まとめ

本調査は、これまで言われてきた**「大企業の経営幹部の多くがハードコードされたシークレットに伴うリスクを認識している」**という状況についてエビデンスを示すものです。調査結果では、回答者の47%がハードコードされたシークレットを重要なリスクであると認めています。

しかしながら、こうした問題への対応は複雑な作業であり、問題の複雑さを考えると**画一的なソリューションでは十分な対応を期待できそうにはありません。** 一方で、当社の調査では、開発組織のシークレット流出に対するレジリエンシーを高めたいという回答者の間に明確な意欲が示されています。事実、回答者の94%が今後12～18か月以内にシークレットにまつわる慣習を改善するつもりであると答えています。

こうした、開発におけるシークレット流出という複雑な問題に対処するには、機密性の高い環境順に優先順位付けを行った、多面的なアプローチが必要です。**修復フェーズは、ハードコードされたシークレットの流出発生後にセキュリティ業務の大半を行います。**そのため、修復フェーズは複雑かつ費用のかかるフェーズです。開発者主導の修復作業の実現は、ソースコードリポジトリの安全性を確保する上で欠かすことのできないステップです。

GitGuardianでは、ソリューション導入によるデータ流出リスクの軽減と機密情報の保護の効果をこの目で見てきています。当社は、シークレット検出と修復機能を展開することで、**大企業における不正侵入リスクを軽減し、貴重な時間とリソースの有効活用実現のお手伝いをすることが可能です。**

自組織のシークレット管理の改善をお考えの方は、当社のシークレット管理に関するアンケート (匿名のアンケートです)で、現状診断を行っていただくことをお勧めします。5分程度の診断で、自組織の強みと弱みを瞬時に把握でき、セキュリティ改善に向けた取り組みに活かすことができます。

また、当社では成熟度モデルを提案しています。こちらの理解を深めていただくために、添付のホワイトペーパー「 Secrets Management Maturity Model white paper. 」のご一読をお勧めいたします。なお、GitHubにおけるシークレットスプロールの状況については「 2023 State of Secrets Sprawl」で詳細をご確認いただけます。

最期に、DevSecOps、シークレット管理、コードセキュリティに関するガイダンスあるいは支援が必要な方は、お問い合わせをお願いいたします。当社の専門家チームが、お客様に合った方法で支援を提供いたします。

GitGuardianについて

GitGuardianは、DevOps向けソリューションを提供するコードセキュリティプラットフォーマーです。シークレット検出・修復市場のパイオニアである同社のソリューションは、何十万もの開発者により使用されています。

GitGuardianは、開発者やクラウドオペレーション、セキュリティ、コンプライアンスの専門家を対象に、複数システムへの一貫した包括的な方法でのポリシー定義・適用を支援しています。

GitGuardianのソリューションは、パブリックリポジトリ、プライベートリポジトリをリアルタイムで監視し、シークレットや機密ファイル、IaCの設定ミス等を検出するとアラートを通知します。そのため、迅速な調査・修復が可能です。
また、GitGuardianのハニートークンモジュールは、AWS認証情報等のリソースをおとりとして使用することで、ソフトウェアのデリバリパイプラインにおける侵入検知の確率を高めています。

GitGuardianは

そして、Instacart Snowflake、Orange、Bouygues Telecom、Iress、Maven Wave、
NOW: Pensions、DataDog、PayFit をはじめとする大手企業の信頼を得ています。

GitGuardianの詳細については以下をクリックしてください

Website | Public Monitoring | Secrets detection | Honeytoken

調査手法

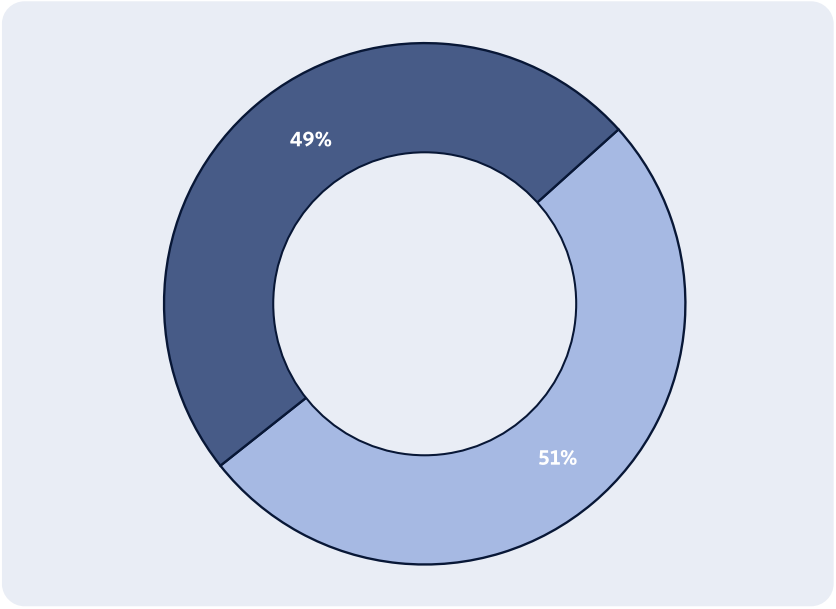
Sapio Research社について

Sapio Research は、高い実績を誇る、市場調査専門の国際的総合コンサルタント企業です。あらゆる領域の定量的・定性的調査を得意とし、難解かつ複雑な案件にも対応可能です。

専門領域は、オーディエンス分析、ブランド調査、コンテンツリサーチです。

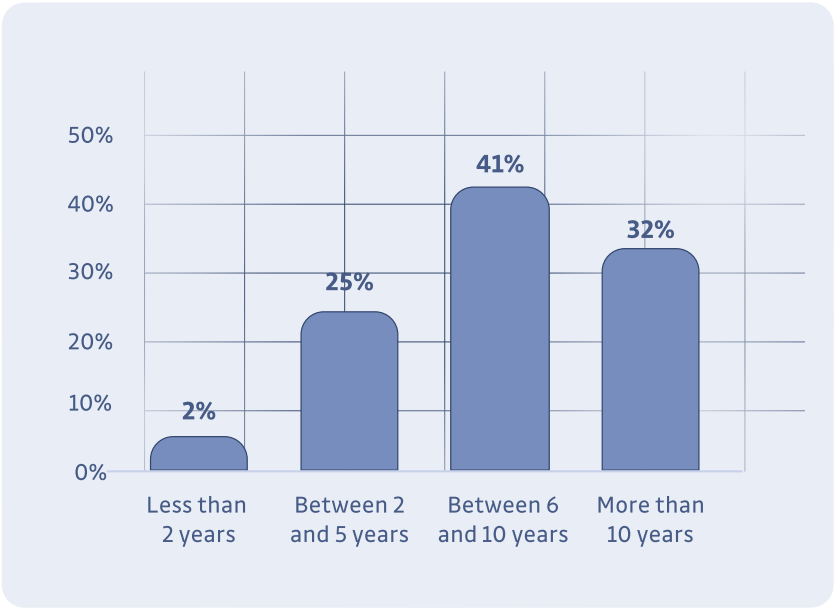
アンケート調査

今回のアンケート調査では、米国・英国の大企業に勤務する、**IT分野の意思決定者507名**を対象に調査を実施しました：

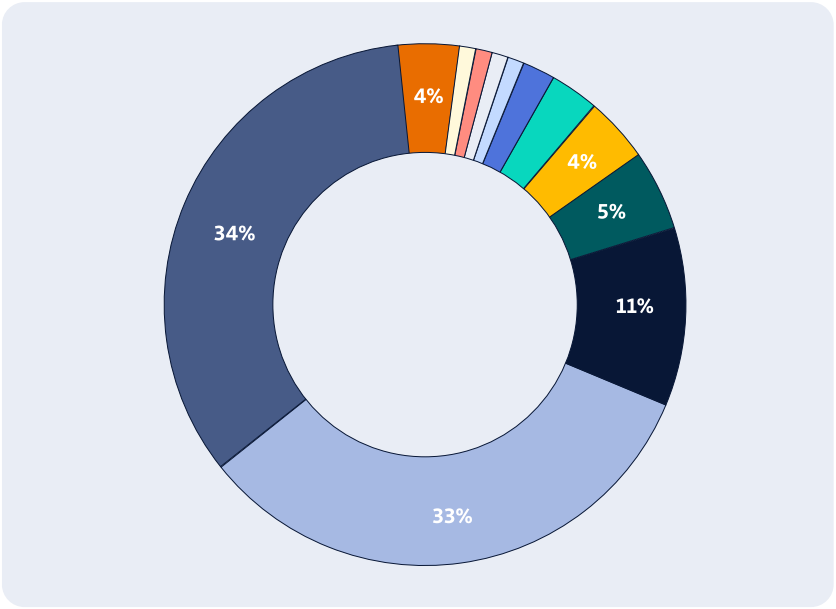


現在お住まいの地域はどこですか？

- UK
- US

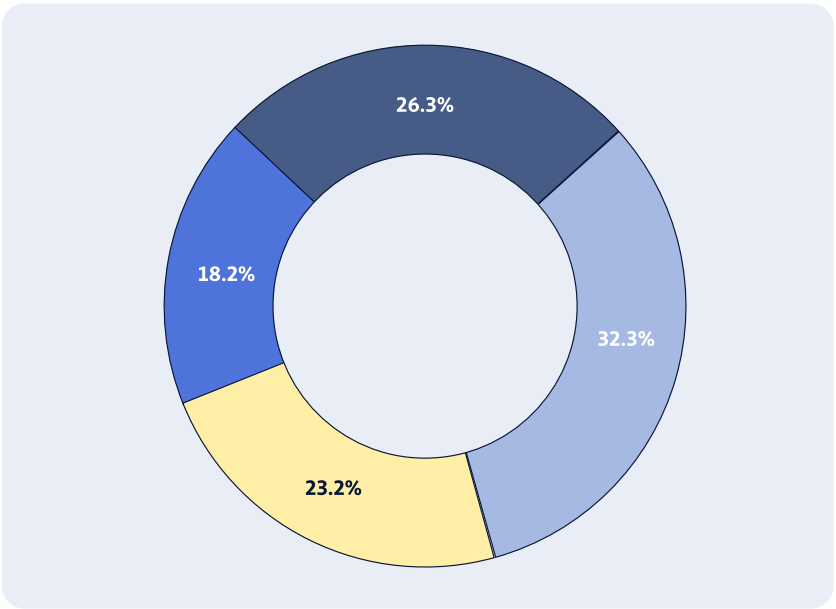


現職での勤務年数はどれくらいですか？



現職の説明として最も当てはまるのは次のうちどれですか？

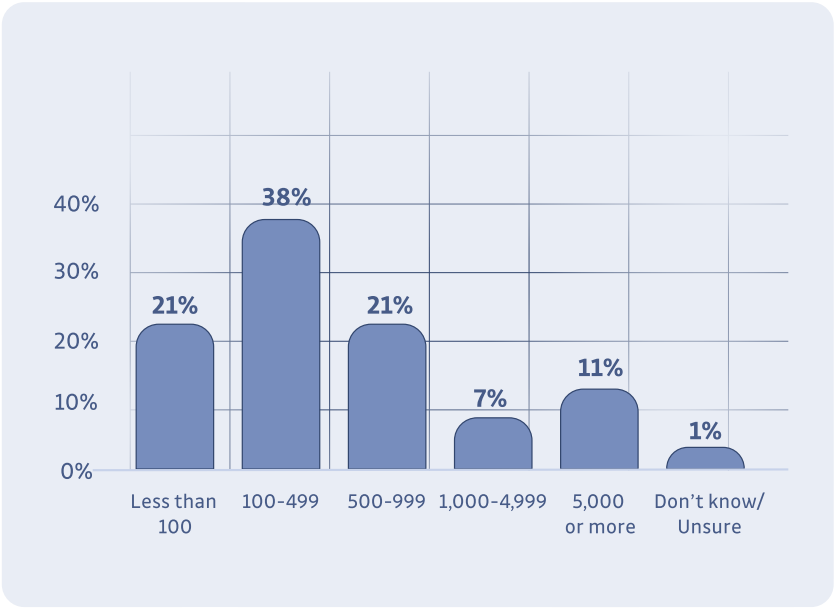
- ITマネジメント（例：IT担当の重役）
- IT担当シニアマネジメント（例：CIO、担当VP）
- ソフトウェアエンジニアリングのシニアマネジメント
- IT/ネットワークアーキテクト
- 開発チームの責任者
- セキュリティのシニアマネジメント（例: CSO）
- セキュリティ/セキュリティオペレーションのマネジメント
- インフラオペレーション
- クラウドオペレーション
- アプリケーションアーキテクト
- クラウドアーキテクト
- その他



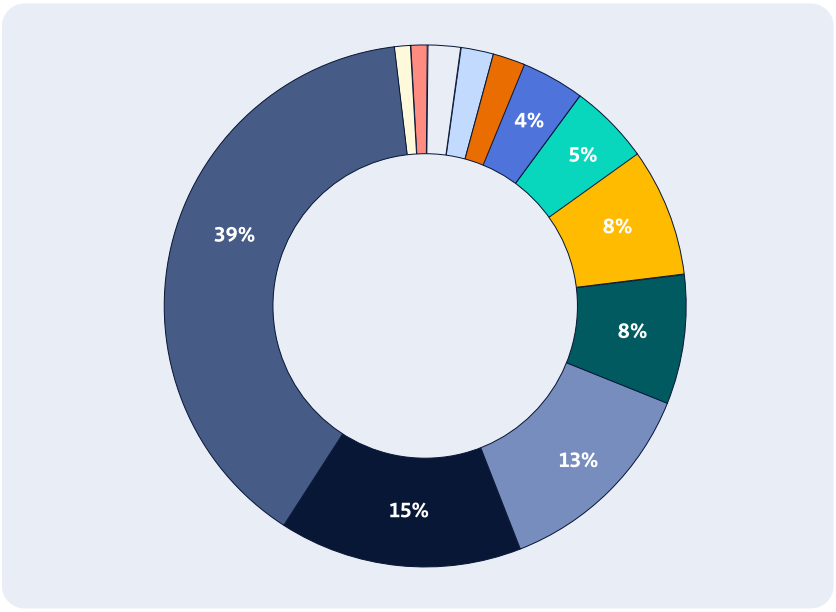
貴社の従業員が従事する拠点すべてについて、そこで働く従業員数を合計するとどれくらいになりますか？

- 1,000-2,999
- 3,000-4,999
- 5,000-9,999
- 10,000+

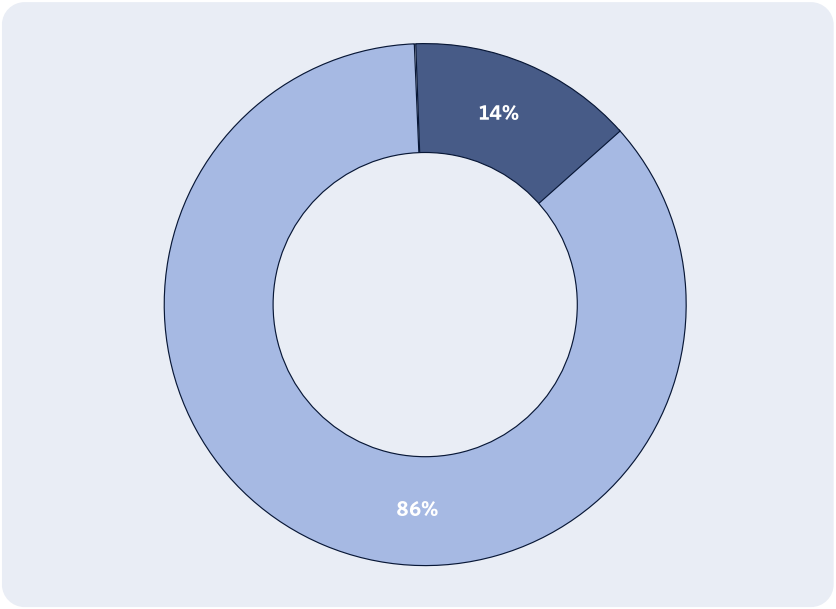
貴社のソフトウェア開発チームの人員数はどれくらいですか？



貴組織の業界の説明として最も近いのは次のうちどれですか？

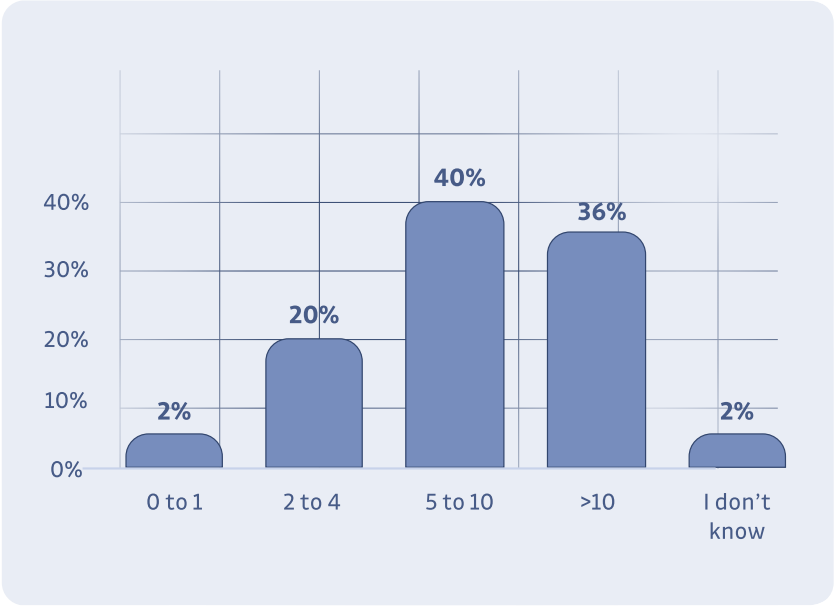


- ソフトウェア/テクノロジー/通信
- 製造/卸し
- 金融/保険/卸し
- 観光/小売り
- 医療
- 輸送/公共サービス
- 政府/NGO
- 建設
- その他
- 教育
- メディア/マーケティング/広告
- 法律



貴組織ではアプリケーションセキュリティ（AppSec）プログラムを導入していますか？

- はい、導入しています
- 今は導入していないが、将来的に導入する予定



貴社においてアプリケーションセキュリティに従事している人数はどれくらいですか？


GitGuardian