BLACKDUCK®

シークレット・スキャン

レポート「The State of Secrets Sprawl, 2023」によると、GitHub にコミットされたファイルにハードコーディングされたシークレットが検知された件数はこの 1 年間で平均 67% 増加しています。

シークレットのハードコーディングが招くリスク

近年発生した大規模なデータ侵害の多くは、防ぐことができたはずの一見単純なミスが原因で起こっています。シークレットが設定ファイルやソースコードにハードコーディングされたまま曝露されると、攻撃者にデータを盗まれたり、組織の最も機微なシステムに侵入されたりする危険があります。

ブラック・ダックのシークレット・スキャンは、ソースコードや IaC (Infrastructure-as-Code) テンプレートなど、さまざまな種類のファイルを解析し、ハードコーディングされたシークレットを検知します。これらのシークレットを削除することで、ビジネスや顧客のデータを危険にさらすことを未然に防ぐことができます。

さまざまな種類のシークレット

ブラック・ダックは、正規表現によるパターン・マッチングにアプリケーション・コンテキストと言語のセマンティクスを組み合わせ、攻撃者の手に渡るとシステムやデータを危険にさらすおそれのあるシークレットを幅広く検知します。

シークレットの種類

- パスワード
- アクセス・トークン
- SSH キー
- API キー
- クラウド・プロバイダーのシークレット
- 一般的なシークレット

ファイルの種類

- ソースコード
- 設定ファイル
- スクリプト
- IaC テンプレート
- テキスト・ファイル

既知のシークレット、未知のシークレット

ブラック・ダックは、AWS、Docker、GitHub などの一般的なテクノロジーに特化したシークレットのパターン検知を 200 種類以上サポートしています。この特化型スキャンにより、これらシステムとの統合が悪用されるのを防ぎます。

しかし、GitGuardian のレポート「The State of Secrets Sprawl, 2023 (シークレット拡散の現状 2023)」によると、2022 年に公開リポジトリで見つかったシークレットの 67% は汎用型スキャン手法によって検知されています。汎用型スキャンは事前のパターン定義が不要で、よく使用されるシークレットに類似したテキスト文字列を特定します。この手法は検知対象が既知である必要がなく、特化型スキャンでは取りこぼしてしまうような脆弱性を補完的に検知します。ブラック・ダックは特化型スキャンと汎用型スキャンを組み合わせることにより、アプリケーションに含まれるシークレットの検知率を最大限に高めています。

ハードコーディングされたシークレットを SDLC 全体で検知

脆弱性は、それがどのような種類のものであれ、開発プロセスの早期段階で見つけて取り除くのがベスト・プラクティスであり、他のコードにマージされたり他のチームに影響を与えたりする前に対処する必要があります。ブラック・ダックはハードコーディングされたシークレットをソフトウェア開発ライフサイクル（SDLC）の複数のステージで検知し、なるべく早い段階での修正を可能にすることにより、シークレットが公開リポジトリや本番環境にプッシュされる可能性を最小に抑えます。

リアルタイム IDE
- Code Sight

静的解析
- Polaris fAST Static
- Coverity

ソフトウェア・コンポジション解析
- Black Duck
- Black Duck Binary Analysis

IAST
- Seeker

- **Code Sight™（IDE プラグイン）：**コーディングの問題やハードコーディングされたシークレットをリアルタイムに指摘します。開発者はツールを切り替える必要がなく、コードをコミットする前に問題を解決できます。
- **静的アプリケーション・セキュリティ・テスト（SAST）によるスキャン：**アプリケーション全体に潜むシークレットを特定します。コミットやプル・リクエストと同時にスキャンをトリガーする機能もあり、シークレットがメイン・ブランチにマージされるのを防ぎます。
- **ソフトウェア・コンポジション解析（SCA）によるスキャン：**IaC テンプレート内や、パイプラインのビルド・フェーズでコンテナにパッケージ化されるソース・ファイル内のシークレットを検知します。
- **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）によるスキャン：**web サーバーが生成してモバイル・フロントエンドに送信する JavaScript コード内のシークレットなど、実行時に露出する脆弱性を検知します。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp