Black Duck Polaris Platform

アプリケーション・セキュリティのための単一のプラットフォーム

AI を活用した野心的なソフトウェア開発のスピードと規模に対応した、妥協のない AppSec プラットフォーム。

概要

Black Duck Polaris™ Platform は、現代の DevSecOps に最適化されたクラウド・ベースのアプリケーション・セキュリティ・プラットフォームです。開発ワークフローにシームレスに統合し、リスクに優先順位を付け、スピードや精度を犠牲にすることなくポリシーへの遵守を徹底します。

主な利点

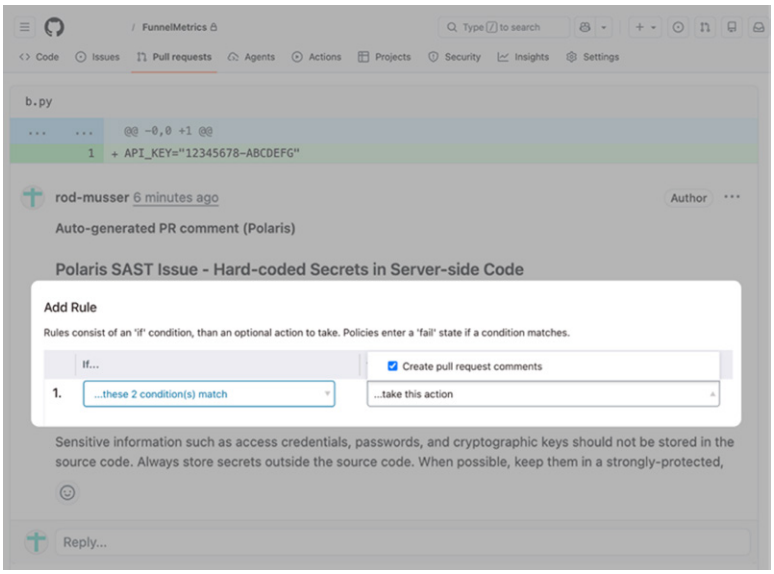
- **開発者中心のワークフローと統合。**セキュリティを開発ワークフローにシームレスに統合するため、摩擦を起こさず効率が最大限に向上します。
- **リスクの優先順位付けとノイズの排除。**誤検知や優先度の低いノイズが排除されるため、95% のリスクを生み出している 5% の問題に集中できます。
- **ポリシー、ガバナンス、コンプライアンス。**カスタマイズ可能なポリシーを使用した集中型のガバナンスにより、SDLC 全体を通じてセキュリティ標準を適用できます。
- **AI 駆動型のセキュリティと自動化。**AI を活用した修正ガイダンスにより、リアルタイムでの問題の要約とワンクリックでの修正提案を示します。
- **深さと精度を備えた包括的なスキャン。**業界をリードする SAST、SCA、および DAST エンジンを統合しており、正確で包括的な結果が一元的に得られます。
- **ROI とリスク態勢を可視化して証明。**対話型のダッシュボードとレポートにより、脆弱性やセキュリティ・プログラムの価値に対する知見がリアルタイムに得られます。

「Black Duck は、セキュリティ部門が定義したポリシーに合わせながら、コード・コミット、プルリクエスト、ビルドなどパイプライン上のトリガーによって自動的に動作するため、プロジェクトごとの差異、コンテキストの変化、リスク許容度に応じて、可能な限り早い段階でスキャンを実行できます。」

—Michael Knight 氏（Datascan 社、VP of Technology）

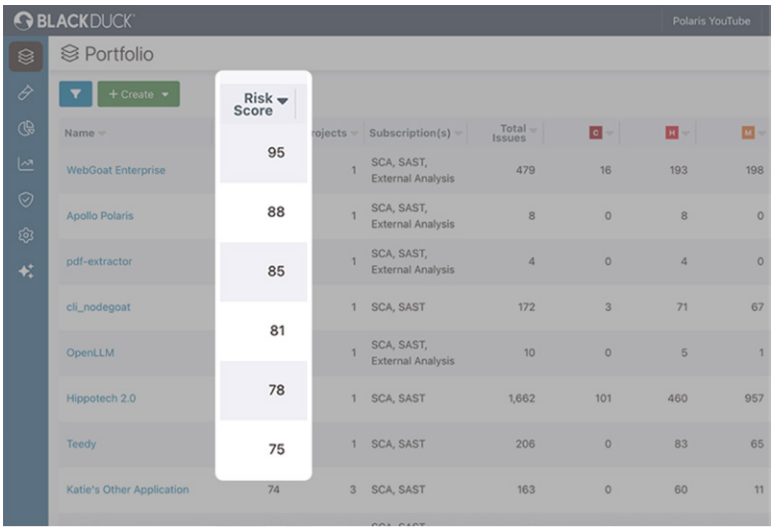
スピードを犠牲にせずセキュリティを強化する機能の数々

開発者中心のワークフロー



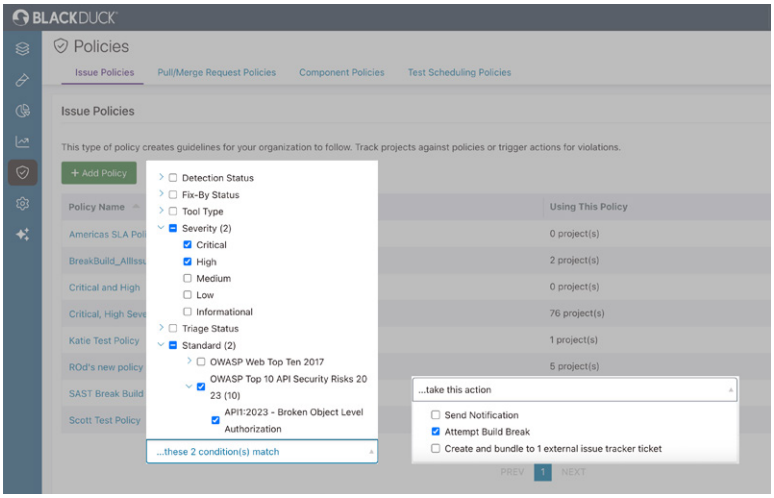
- SCM の一括オンボーディングを自動で実行。新規リポジトリも自動で検出して即座にスキャンを実行し、AppSec リスク・プロファイルを作成します。
- プルリクエスト時に高速スキャンを実行し、結果をプルリクエスト・コメントとして返すため、SCM 内で迅速にフィードバックを受けとることができ、下流リスクが軽減します。
- コード・マージ時にフルスキャンを実行し、結果を Jira や ADO のインスタンスに流し込むことができます。

リスクの優先順位付けとノイズの排除



- SAST、SCA、および DAST の結果を集約してインテリジェントにスコア化することで、開発者は重要な問題だけを修正して次の作業に移ることができます。
- 環境リスク、ビジネス・リスク、アプリケーション・リスクを含む複数のリスク・プロファイルを統合してリスクをスコア化します。
- 脆弱性を特定し、その重大度、リスク・スコア、標準への違反度、および到達可能性に基づいて優先順位を付けます。

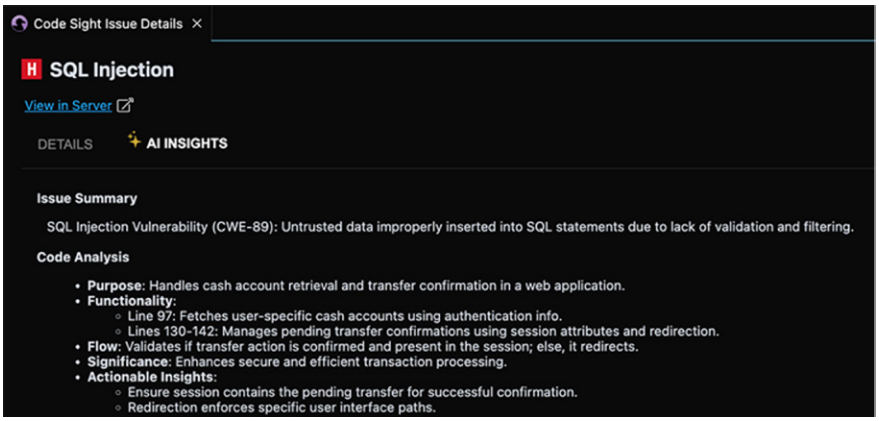
ポリシー、ガバナンス、コンプライアンス



- ビジネス・リスク・プロファイルに基づいてカスタマイズしたポリシーを使用して、集中型のガバナンスを実施できます。
- ポリシー違反があった場合は、ビルドの中断、プルリクエストのブロック、通知の送信により、SDLC 全体を通じてセキュリティ標準を自動で適用できます。
- レポート機能およびカスタマイズしたダッシュボードにより、どのチームがセキュリティ目標を達成しているかを追跡し、ポリシーへの遵守を証明することができます。

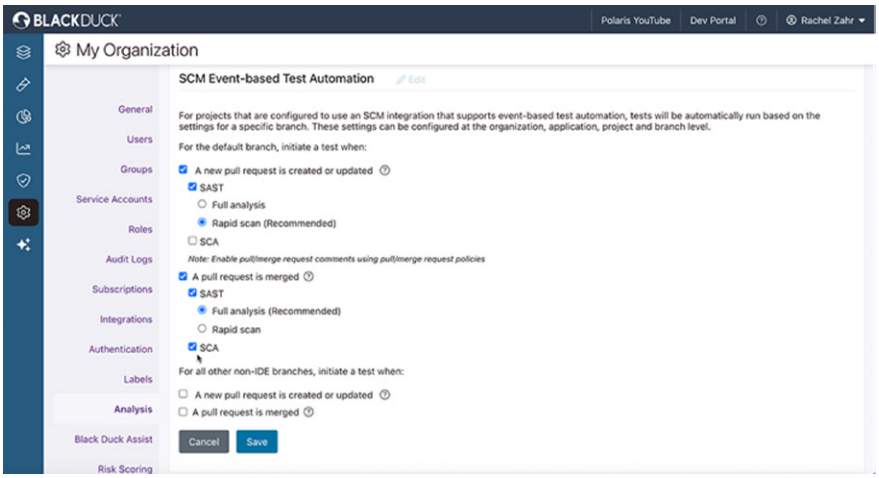
AI 駆動型のセキュリティ、包括的なスキャン、ROI の証明

AI 駆動型のセキュリティと自動化



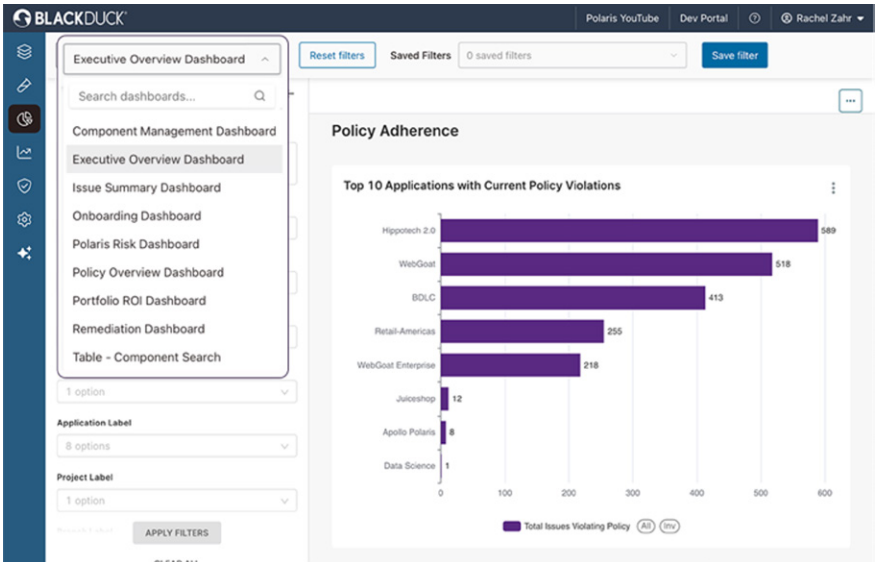
- Black Duck Assist™により、ワンクリックでの高品質な修正提案を IDE およびパイプライン内で直接受け取ることができます。
- 検出結果に対して自動的に背景情報まで提示してくれるコンテキスト対応型のセキュリティ・トレーニングにより、開発者は実際の作業をしながらセキュアなコーディング・パターンを学習できます。

深さと精度を備えた包括的なスキャン



- 業界をリードする SAST、SCA、および DAST エンジンを 1 つのプラットフォームに統合。
- 高速スキャンをトリガーして即座にフィードバックを得ることも、フルスキャンを開始してより深く包括的な解析結果を得ることもできます。
- 主要な言語、フレームワーク、パッケージ・マネージャーを幅広くサポートしているほか、IaC、API、およびシークレットのスキャンにも対応しています。

ROI とリスク態勢を可視化して証明



- 対話型のダッシュボードにより、リアルタイムのアプリケーション・リスクを一元的に可視化できます。
- 脆弱性の解決率やポリシーへの遵守状況など、経営幹部向け指標を確認できるレポート機能を内蔵しています。
- リソース配分の優先順位付けに役立つ知見が得られ、セキュリティ・プログラムの価値を実証できます。

サポートされる言語とパッケージ・マネージャー

SAST 言語

- SAST 言語
- Salesforce Apex
- C/C++
- C#
- DART
- Go
- Java
- JavaScript
- Kotlin
- Objective-C/C++
- PHP
- Python
- Ruby
- Scala
- Swift
- TypeScript
- Visual Basic

SCA パッケージ・マネージャー

- Apache Ivy
- BitBake
- Cargo
- Carthage
- CocoaPods
- Conan
- Conda
- CPAN
- CRAN
- Dart
- Erlang/Hex/Rebar
- Git
- Go Dep
- Gogradle
- Go Modules
- Go Vendor
- Gradle
- Hex
- Lerna
- Maven
- Npm
- NuGet
- Packagist
- PEAR
- Pip
- Pnpm
- Poetry
- RubyGems
- SBT
- Swift および Xcode
- Yarn

IaC、クラウド、コンテナ、および構成ファイルのフォーマット

- Ansible
- AWS CloudFormation
- Azure Resource Manager (ARM)
- Docker
- Google Cloud Platform (GCP) Deployment Manager
- Helm
- JSON
- Kubernetes
- Terraform (AWS、Azure、GCP、Kubernetes 用)
- XML
- YAML

開発および DevOps との統合

ソースコード管理 (SCM) システム

- GitHub
- GitLab
- Azure DevOps
- Bitbucket

課題トラッカー

- Jira
- Azure Boards
- GitHub Issues

ビルド /CI ツール

- GitHub Actions
- GitHub App
- GitLab CI
- Azure Pipelines
- Bitbucket Pipelines
- Jenkins
- AWS CodeBuild*
- Bamboo*
- CircleCI*
- CloudBees*
- CodeShip*
- Concourse*
- Sbt*
- TeamCity*
- Gradle*
- Wind River Studio*
- Travis CI*

*Black Duck Bridge CLI 経由でのサポート

学習プラットフォーム

- Secure Code Warrior

SBOM フォーマット

- SPDX
- CycloneDX

サードパーティ製ツール (SCA/SAST)

- Android Lint (SAST)
- Brakeman (SAST)
- Black Duck Binary Analysis (SCA)
- Checkmarx (SAST)
- Clang (SAST)
- Clippy (SAST)
- CodePeer (SAST)
- Coverity® 静的解析 (SAST)
- CppCheck (SAST)
- DefenseCode ThunderScan (SAST)
- Dependency-Check (SCA)
- ErrCheck (SAST)
- Error-prone (SAST)
- ESLint (SAST)
- Fortify (SAST)
- FxCop (SAST)
- Gendarme (SAST)
- Gitlab Security (SAST)
- GoCyclo (SAST)
- GoLint (SAST)
- GoSec (SAST)
- HCL AppScan Source (SAST)
- HCL AppScan on Cloud (ASOC) (SAST/SCA)
- Helix QAC (SAST)
- IneffAssign (SAST)
- JFrog Xray (SCA)
- JLint (SAST)
- Microsoft Code Analysis (SAST)
- MobSF (SAST)
- MobSF Scan (SAST)
- NDepend (SAST)

サードパーティ製ツール (SCA/SAST) 続き

- OCLint (SAST)
- Parasoft JTest / C++Test / dotTest (SAST)
- PHP_CodeSniffer (SAST)
- PHPMD (SAST)
- PMD (SAST)
- Pylint (SAST)
- Rapid Scan SAST (Sigma) (SAST)
- Retire.js (SCA)
- SafeSQL (SAST)
- SARIF (SAST)
- SATE (SAST)
- Scalastyle (SAST)
- SCARF (SAST)
- SciTools Understand (SAST)
- Semgrep (SAST)
- Snyk Open Source (SCA)
- SonarQube Generic Issue Import Format (SAST)
- SpotBugs / FindBugs (SAST)
- Software Risk Manager™ (SAST/SCA)
- Staticcheck (SAST)
- TFLint (SAST)
- TruffleHog (SAST)
- Veracode (SAST/SCA)
- Vet (SAST)
- WPScan (SCA)
- ZPA (SAST)

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