

Polaris Software Integrity Platform

モダン DevSecOps に対して最適化されたクラウド・ベースの統合 AST ソリューション

Polaris は、
モダン DevSecOps に対して
最適化され、エンタープライズ
環境で必要とされる能力と
スケーラビリティを備えた、
使いやすいアプリケーション・
セキュリティ・プラットフォーム
です。

概要

Polaris Software Integrity Platform® は、業界をリードする静的アプリケーション・セキュリティ・テスト (SAST) とソフトウェア・コンポジション解析 (SCA) のエンジンを備えた、統合 SaaS (Software-as-a-Service: サービスとしてのソフトウェア) アプリケーション・セキュリティ・プラットフォームです。マルチタイプの高速スキャン機能は、シノプシスのセキュリティ専門家によってトリアーजされた、高精度のスキャン結果を提供できます。ビジネス・アプリケーションのセキュリティ・ニーズに対応できる、使いやすく費用対効果の高いソリューションである Polaris により、アプリケーション・セキュリティ・チームと開発チームは、エンタープライズ・アプリケーションのリスクを総合的に管理しながら、リアルタイムで協働し、リリース期限に間に合わせることができます。

主な利点

- **柔軟性** オンデマンド型の統合 AppSec プラットフォームにより、エンタープライズ全体で 24 時間体制のスキャンと評価を容易に実施、管理、および監視することができます。
- **スケーラビリティ** アプリケーション・セキュリティを費用対効果が高くなるように拡大・縮小します。テスト対象アプリケーションが 1 つでも数千でも、Polaris は統合 SaaS プラットフォームであらゆるニーズに対応します。
- **使いやすさ** 1 つの統合プラットフォームからの容易なオンボーディング、デプロイメントおよびテスト。既存の開発者とテスト自動化および CI/CD ワークフローのシームレスな統合。
- **同時スキャン** SAST と SCA を同時に実行できるようにすることで同時スキャンのパフォーマンスが向上し、実行可能なテスト数の制限がなくなります。
- **精度の高い検出** 業界をリードするシノプシスの SAST と SCA のエンジンによって、完全かつ精度の高い結果が提供されます。誤検知を特定して削除することで結果を更に改善するために、SAST の結果に対する専門家による分析とトリアージも可能です。
- **エンタープライズ環境の可視化** Polaris のダッシュボードとレポートにより、すべてのチームおよびアプリケーションにわたる脆弱性と傾向を把握できます。

主な特徴

FAST Static

Polaris の FAST Static ですべてのコードベースの自動静的解析を実行することで、開発者とテスト担当者が SDLC の早い段階でコードの潜在的なセキュリティ上の欠陥を容易に見つけることができます。

The screenshot displays the Synopsys Polaris web interface. The top navigation bar shows the project path: GP Big Bubbly Branch Test > Purple Piggy Project / Mic-Check (default). The left sidebar contains filters for Issues, Components, Licenses, Tests, Branches, and Settings. The main panel shows a list of 183 matching issues, with 100 displayed. The issues are categorized by Severity (High, Medium, Low) and Issue Type (SQL Injection, DOM-Based Cross-Site Scripting, Cleartext Storage of Sensitive Information in GUI, Insecure Object Deserialization, Improper Resource Shutdown or Release, Cross-Site Request Forgery (CSRF)). The details panel for a selected 'SQL Injection' issue shows the location (webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqOnlyInputValidation.java) and the contributing code events. The code snippet shows a public method attack that takes a request parameter 'userid' and returns a failed result if the user is not found. The issue is marked as 'Not Triaged' with a CVE of CWE-89.

FAST SCA

Polaris FAST SCA を使用することで、組織は SDLC 全体にわたるソフトウェア・コンポジション解析を自動化し、使用されるライセンス、依存関係ツリー、起源およびアップグレード・ガイダンスを含む、脆弱性のないオープンソース・コンポーネントと脆弱なオープンソース・コンポーネントの完全な部品表 (BOM) を提供できます。

The screenshot displays the Synopsys Polaris web interface for FAST SCA analysis. The top navigation bar shows the project path: SIGApp > TestProject. The left sidebar contains filters for Summary, Issues, Components, Licenses, Tests, and Settings. The main panel shows a list of 2,925 results across 30 pages. The results are categorized by Security Risk (Critical, High, Low) and Component Name (Apache Ant 1.7.1, Apache Ant 1.8.0, BeanstalkClient 1.4.6, FindBugs jar 2.0.1). The details panel for a selected 'Apache Ant 1.7.1' issue shows the component description, component links, component origins, current vulnerabilities, and upgrade guidance. The dependency tree shows the component's dependencies, including Cargo Core Liberator 1.2.0, Apache Ant 1.7.1, and Cargo Core Liberator 1.2.0. The issue is marked as 'Not Triaged' with a CVE of CWE-89.

専門家による検証と解析

SAST のスキャン結果のレビューが実施されることで誤検知が排除され、適時修正するために重要な検出が優先されます。

シームレスな統合

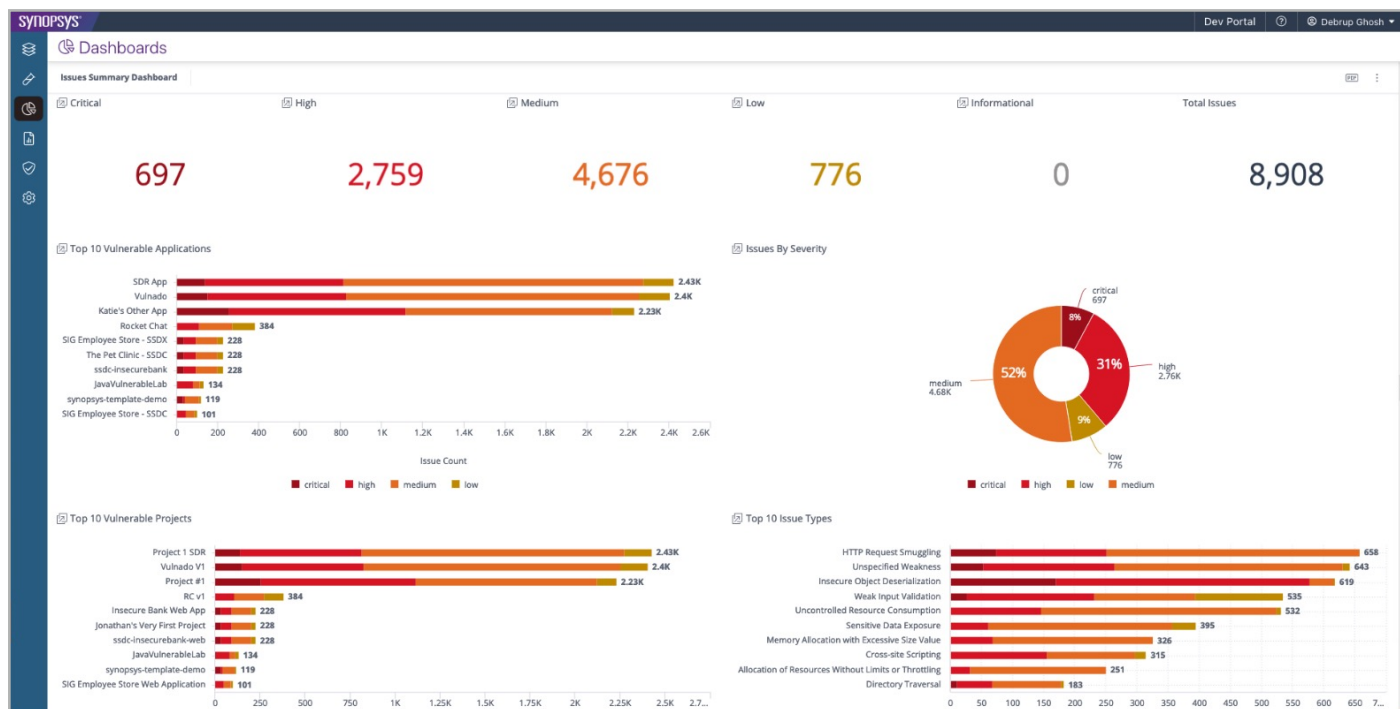
使いやすいプラットフォームで、開発および DevOps のツールチェーンとのシームレスな統合が実現されます。

ポリシー管理

定義されたビジネス・リスク・ポリシーごとに、カスタマイズ可能なルールを簡単にセットアップできます。

企業の知見

アプリおよびプロジェクト全体の健全性および効果的なリスク態勢に対する組織規模の知見が得られます。



対応する言語およびパッケージ・マネージャー

SAST 言語

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

IaC のプラットフォームおよびフォーマット

- AWS Cloud Formation
- Kubernetes
- Terraform
- YAML
- JSON
- XML

ソースコード・マネジメント・システム (SCM)

- GitHub
- GitLab
- Azure DevOps
- Bitbucket

SCA 言語およびパッケージ・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 and Xcode
- Yarn

ニーズに適した Polaris の機能を選択

機能	説明	Polaris SAST (トリアージなし) サブスクリプション	Polaris SAST サブスクリプション	Polaris SCA サブスクリプション	Polaris パッケージ SCA/SAST
fAST Static	SDLC 全体にわたって静的解析を自動化	●	●		●
fAST SCA	SDLC 全体にわたってソフトウェア・コンポジション解析を自動化			●	●
専門家による トリアージ	シノプシスのセキュリティ専門家による SAST 解析結果のレビューが実施されることで、優先順位が付けられ、誤検知が排除されます。		●		●
SCM の統合	アプリケーションをレポジトリから直接、迅速にオンボード	●	●	●	●
ポリシー管理	最適化されたルールによってポリシー管理を簡素化し、セキュリティ・ポリシーとリスク・ポリシーの実施を自動化	●	●	●	●
同時スキャン	アプリケーションで SAST と SCA の複数の同時スキャンを実行	●	●	●	●
CI/CD 統合	スピードが重視されるアジャイル DevOps パイプラインでアプリケーション・セキュリティ・ソリューションを自動化	●	●	●	●
従量課金	ビジネス・ニーズに基づいて消費を調整	●	●	●	●
柔軟性のある レポート、解析	エンタープライズ環境の解析機能を使用して、リスクを管理、リスク態勢を計測して改善	●	●	●	●

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。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス

TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software

©2023 Synopsys, Inc. All rights reserved. Synopsys は Synopsys, Inc. の米国およびその他の国における登録商標です。
Synopsys の商標に関しては、こちらをご覧ください。 <http://www.synopsys.com/copyright.html> その他の会社名および商品名は各社の商標または登録商標です。 2023 年 12 月