

SPARROW

Sparrow Enterprise

AIを活用した統合型
アプリケーションセキュリティテスト



ISO26262 認証取得

アプリケーションセキュリティテストを単一のシステムに統合することで、ソフトウェア開発にかかる時間とコストを削減しながら、DevSecOpsを体系的かつ効果的に推進できます。

ソフトウェアサプライチェーンセキュリティを強化する
統合型アプリケーションセキュリティプラットフォーム

Sparrow Enterprise



Sparrow Enterprise は、

ソースコード (SAST)、オープンソースコンポーネント (SCA)、実行中のアプリケーション (DAST) を分析し、AIを活用した統合環境を提供します。セキュリティ対策を開発の早期段階に組み込むことで、リスクを早期に特定し、手戻りコストを抑えながら、安全で堅牢なソフトウェアの提供を支援します。さらに、SBOMに基づくライセンス管理と脆弱性管理により、ソフトウェアサプライチェーン上の重大な脅威に対する保護を強化します。

主な機能

Sparrow Enterpriseは、ソフトウェア開発ライフサイクル全体を通じて包括的な脆弱性分析を提供し、高度な分析機能と管理機能により、組織全体のセキュリティ体制を強化します。

ダッシュボード

資産別 이슈追跡
(SAST、DAST、SCAの 이슈)

資産概要
(総資産、リスクのある資産、
コンポーネント)

이슈状況
(リスクレベル、
ステータス、期間別)

承認状況
(進行中、承認待ち)

分析機能

ソースコード分析

セキュリティ脆弱性分析
コード品質 (欠陥) 分析
이슈発生箇所の正確な特定
セキュアコード例 / 推奨修正方法

コンポーネント分析

コンポーネント識別
ライセンス表示・通知義務の確認
脆弱性の検出・検証
SBOM (ソフトウェア部品表)
の生成・エクスポート

Web脆弱性分析

分析対象の選択
(URL、OpenAPI)

分析範囲の設定
(URLクロール深度、
除外URLなど)
攻撃手順の再現 /
シミュレーション

分析自動化

各種ツールとの連携
(バージョン管理システム、
CI/CDツールなど)

分析状況のリアルタイムモ
ニタリング (実行中、一時
停止 / 停止、完了)

管理機能

ユーザー

ユーザー・
ユーザーグループ
ロールと権限
分析・監査履歴の確認

承認

承認ルートの設定
承認範囲の設定
(プロジェクト、システム)
承認対象の管理
(이슈、資産、コンポー
ネントなど)

이슈の ステータス

レビュアーの割り当て

이슈の
ステータス変更
(To do, Doing, Done)

ルール・ ワークプロファイル

ポリシーに基づく検出ルール
の選択
(OWASP Top 10、CWEなど)

이슈を5段階の
リスクレベルに分類
(Critical、High、Medium、Low、Trivial)
ルールとオプションのカスタマイズ

レポート

レポートテンプレート
のカスタマイズ
(タイトル、ロゴなど)

参照基準別のレポート設定
(OWASP、CWEなど)

項目のカスタマイズ
(リスクレベル、ルール、資産など)

AI機能

オープンソース
AIモデル利用チェック

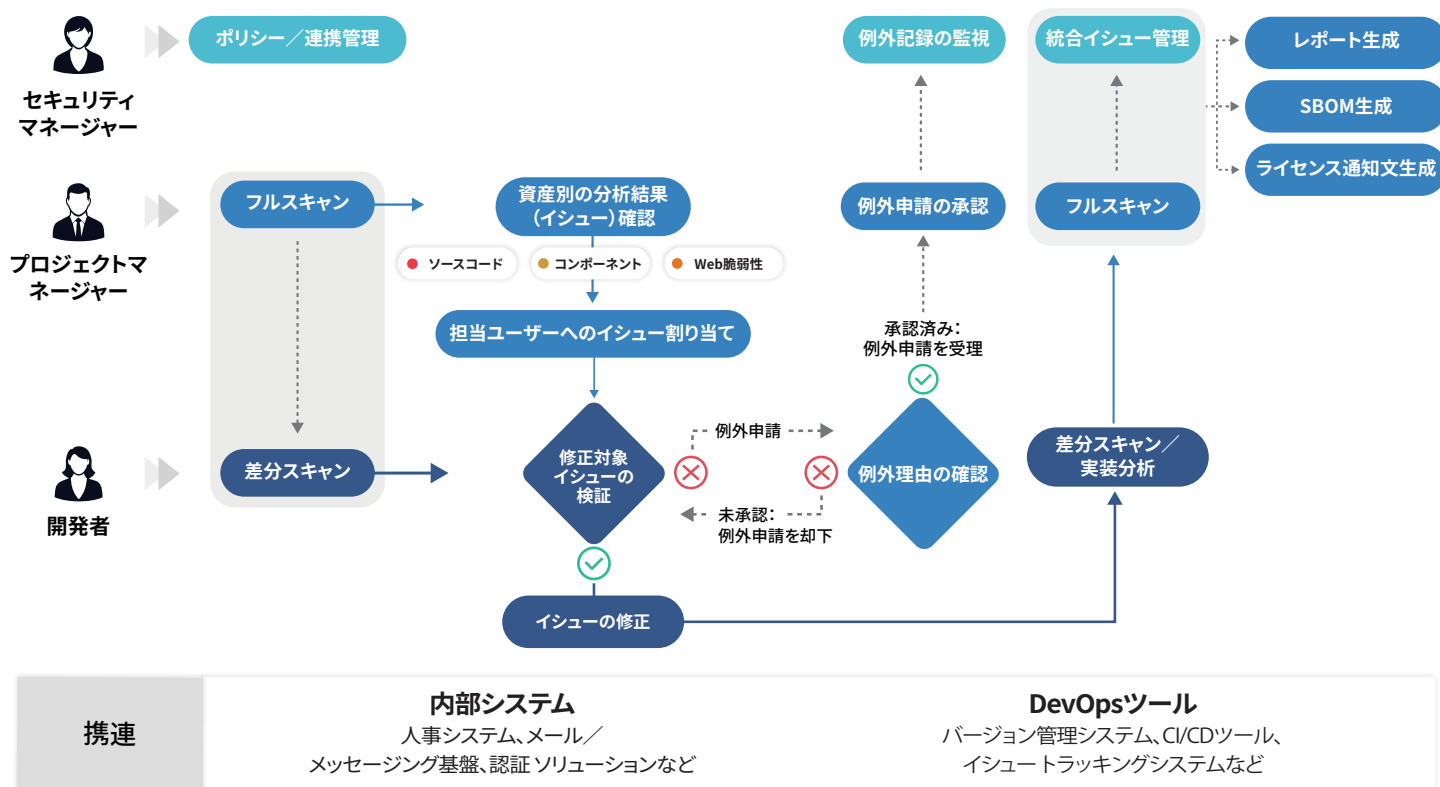
AIによる修正提案

重要度に応じた優先順位付け

分析とイシュー処理プロセス

ソフトウェア開発のライフサイクル全体を通じて、一貫したセキュリティポリシーを設定し、ユーザーごとに役割と権限を適切に付与することで、定期的な全件分析および必要に応じた随時分析が可能です。

資産ごとの分析結果をイシュー単位で管理することで、セキュリティ脅威に効果的に対応します。



導入効果

AIを活用した統合プラットフォームでアプリケーションの脆弱性を一元管理。ソフトウェア開発ライフサイクル全体を通じて脅威を早期に検出・対応します。体系的な修正プロセスを確立することで、対応に必要なリソースを効率的に活用し、ソフトウェアサプライチェーン全体のセキュリティ強化につなげます。

1
Point

統合ソリューションでセキュリティの死角を最小化

- Sparrow Enterpriseは、SAST・SCA・DASTを一つの環境に統合し、単体ツールでは見落としやすい複雑な脆弱性を検出します。
- さまざまなアプリケーションを横断して統合的に分析することで、広範な範囲をカバーし、セキュリティの死角を最小限に抑えます。
- ソフトウェア開発ライフサイクル全体に一貫したセキュリティポリシーを適用し、高い可視性を備えたリスク管理を実現します。

2
Point

AIを活用した早期修正によりDevSecOpsを実現

- DevOpsパイプラインと直接連携し、各段階でセキュリティテストを自動化します。
- 開発チームとセキュリティチームが共通の基準で脅威に対応できるようにし、開発スピードとセキュリティの理想的なバランスを維持します。
- 開発の早い段階で脆弱性を特定・修正することで、高コストな手戻りを防ぎ、実効性の高いDevSecOpsワークフローを実現します。

3
Point

インテリジェントな優先順位付けにより運用効率を最大化

- 統合された一元管理ダッシュボードにより、資産のセキュリティ状況と修正対応状況を即座に可視化できます。
- AIによる優先順位付けと脆弱性再現機能により、チームは優先度の高い 이슈に集中でき、対応時間を大幅に短縮します。
- カスタマイズ可能な承認プロセスと統合イシュートラッキングにより、重複作業を排除し、部門横断的なチーム間の連携を強化します。

導入実績

優れた分析性能と使いやすさにより、Sparrowのソリューションは公共機関や企業に信頼され、ソフトウェアサプライチェーンの安全性確保に活用されています。

政府・公共機関

韓国法務部、雇用労働部、外交部、産業通商資源部、韓国大法院、公共調達庁、韓国気象庁、データ・統計省、韓国特許庁、国税庁、韓国関税庁、警察庁、国会事務処、韓国インターネット振興院(KISA)、仁川国際空港公社、韓国空港公社、韓国資産管理公社、韓国預金保険公社、KEPCO Engineering & Construction Company, Inc.、韓国ガス公社、韓国水資源公社、韓国財政情報院、韓国信用情報院、韓国住宅金融公社、韓国住宅都市保証公社

金融機関

金融監督院、韓国金融決済院、韓国銀行、KB国民銀行、新韓銀行、農協銀行、韓国産業銀行、iM Bank、韓国投資証券、KakaoPay Securities、教保証券、キウム証券、KB国民カード、ウリカード、ロッテカード、農協カード、NH農協損害保険、AXA損害保険、ロッテ損害保険、コリアンリー再保険、サムスン生命保険、NH農協生命保険、ハナ生命、KBキャピタル、メリッツキャピタル、Danal、Finnq、Koscom、NICE Information Service、SBI貯蓄銀行、韓国投資貯蓄銀行、IBK貯蓄銀行、MGセマウル金庫

企業・産業

Samsung SDS、Naver Cloud、CJ OliveNetworks、KT、Kakao Enterprise、NHN、Lotte Innovate、NCSoft、Neople、Hyundai Motor Company、GS Caltex、POSCO、SK Chemicals、Hyundai Rotem、Hanwha Aerospace、SEMES、42dot、Hanwha Ocean、HMM、STX Engine、CJ Logistics、TMAP Mobility、GS Retail、Homeplus、Dongkuk Steel

防衛・セキュリティ

韓国陸軍、海軍、空軍、防衛事業庁、兵務庁、サイバー作戦司令部、国軍防諜司令部、韓国国防研究院、国防技術品質院、国家保安技術研究所、LIG Nex1、Hanwha Systems

海外

公共機関(マレーシア)、金融機関(日本)、製造業(日本、中国)、ヘルスケア(日本)、研究開発(日本、中国)、IT(日本、中国)、セキュリティ(シンガポール)、ならびに日本、中国、インド、マレーシア、ベトナム、インドネシア、アラブ首長国連邦のパートナー

詳細については、

Sparrowまでお問い合わせください。

✉ E. marketing@sparrow.im

📞 T. (韓国) +82-2-6263-7400

日本国内のお問い合わせ先

VERISERVE

✉ E. vs_contact@veriserve.co.jp

📞 T. (日本) +81-3-5909-5703