BLACKDUCK | HUB

オープンソースの脆弱性の検出と修復

Black Duck Hubはセキュリティおよび開発チームによるアプリケーションポートフォリオ全体にわたるオープンソース関連リスクの識別および軽減を容易にします。

Black Duck Hub の機能

- 使用中のオープンソースを検出するためにコードをスキャン
- 使用中のオープンソースの既知の脆弱性を自動的にマッピング
- 重大度判定 – リスク評価と脆弱性の優先順位付け
- 脆弱性除去のスケジューリングとトラッキング
- ライセンスとコミュニティ活動の識別

従来の静的な分析ソリューションでは開発者のコーディングによって取り込まれた脆弱性に関連して発 覚したコードに焦点が当てられていましたが、この手法では次々に報告される脆弱性の一部しか捕捉できませんでした。

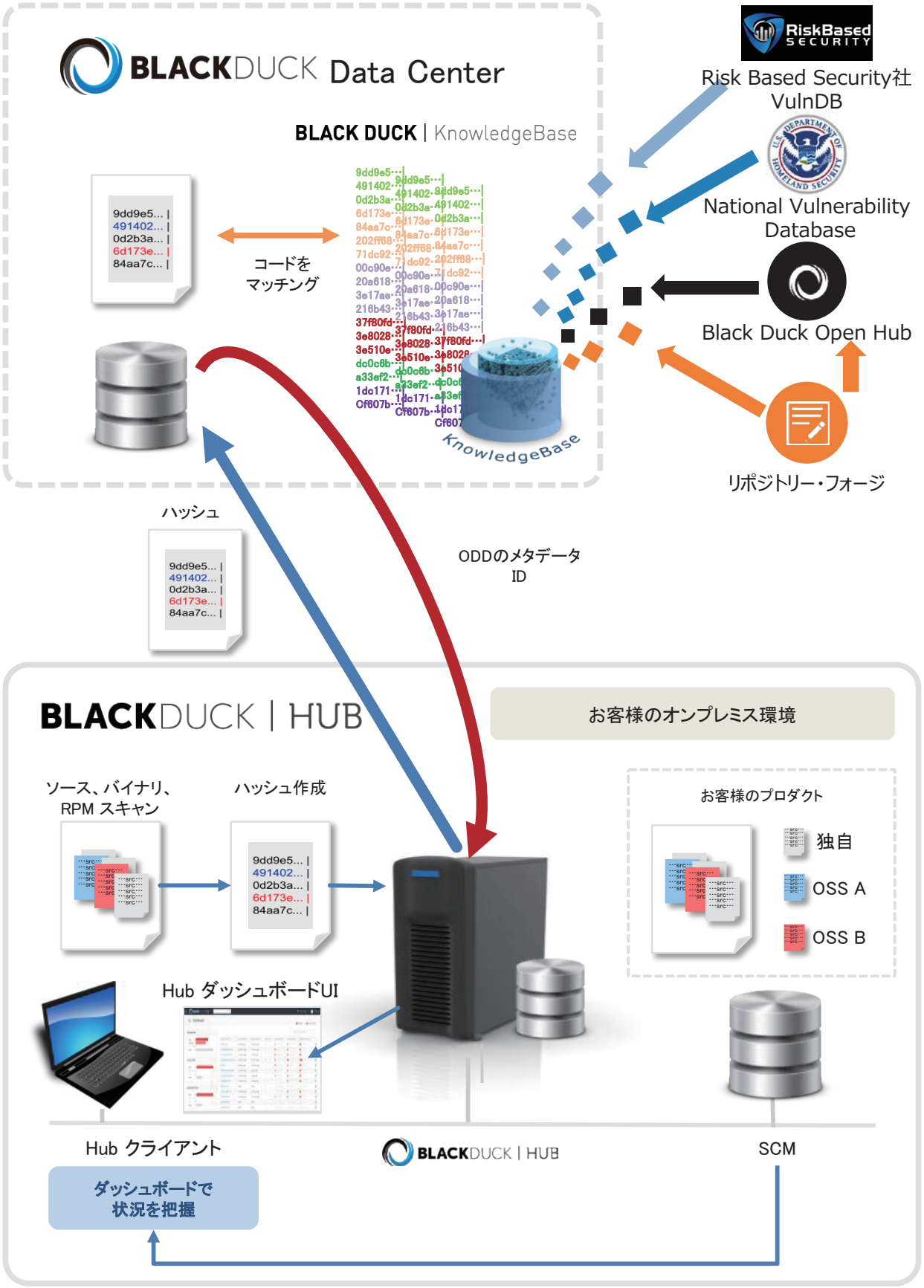
Heartbleed、Shellshock、Poodle、およびGhostのような脆弱性については、一般的に使用されるオープンソースコンポーネントが引き起こす可能性のあるレベルについてのみ強調されていました。これらの広く 認識されている脆弱性は毎年報告される5,000以上ものオープンソースの脆弱性のほんの一部にすぎ ません。

次の特長を備えるのはBlack Duckだけです

- 最も広範囲の言語および開発ツールをカバー
- 世界トップレベルのオープンソースソフトウェアナレッジベース
- 統合修復トラッキング管理

Black Duck Hub の主な特長

迅速スキャン	オープンソースライブラリ、バージョン、ライセンス、コミュニティ活動を軽快かつ迅速に識別
既知のセキュリティに関する脆弱性のマッピング	使用中のオープンソースに関連する既知の脆弱性を識別。高度な脆弱性情報により優先順位付けと修復予定日の割り当てを実行
修復のトラッキング	各プロジェクトの脆弱性に対する予定および実際の修復日をトラッキング。CSV形式でレポートを出力するのでお使いのレポートツールへのインポートが可能
リスク評価サマリ	シンプルなユーザーインタフェースによるリスク評価ダッシュボードを確認することで、企業におけるセキュリティ、コミュニティ、ライセンスに関するリスクを常に把握できます。脆弱性データをドリルダウンすることでプロジェクト内の脆弱性に関連した詳細情報を把握することができる
Black Duck ナレッジベース	世界最高の情報量を誇るオープンソースナレッジベースを検索することで、プロジェクトで使用中のオープンソースの正確な検出、識別、脆弱性とのマッピングが可能
部品表（BOM）	編集可能なオープンソースBOMは、自動識別されたオープンソースソフトウェアライブラリの調整や手動による識別情報の追加が可能
インテグレーション	Jenkinsプラグインを使用して継続的なインテグレーションプロセスと結合することにより、オープンソースBOMのスキャン、検出、自動埋め込みが可能です。オンボードツールを使用してプロジェクトを自動作成することも可能



GRAPE SYSTEMS®
株式会社 グレープシステム® 営業部
横浜市西区みなとみらい2-3-3 クイーンズタワーB 19 〒220-6119
TEL.045-222-3761 FAX.045-222-3760
E-mail : sales@info.grape.co.jp
www.grape.co.jp

2016.04.18