



使用する前に

Black Duck 2024.7.0

Copyright ©2024 by Black Duck.

All rights reserved.本ドキュメントの使用はすべて、Black Duck Software, Inc.とライセンス所有者間の使用許諾契約に準拠します。本ドキュメントのいかなる部分も、Black Duck Software, Inc.の書面による許諾を受けることなく、どのような形態または手段によっても、複製・譲渡することが禁じられています。

Black Duck、Know Your Code、およびBlack Duckロゴは、米国およびその他の国におけるBlack Duck Software, Inc.の登録商標です。Black Duck Code Center、Black Duck Code Sight、Black Duck Hub、Black Duck Protex、Black Duck Suiteは、Black Duck Software, Inc.の商標です。他の商標および登録商標はすべてそれぞれの所有者が保有しています。

30-10-2024

目次

まえがき.....	4
Black Duck documentation.....	4
カスタマサポート.....	5
Black Duck Software Integrityコミュニティ.....	5
トレーニング.....	5
Black Duck 包括性と多様性に関する声明.....	6
Black Duck セキュリティへの取り組み.....	6
1. 概要 Black Duck.....	7
2. ログイン: Black Duck.....	8
3. コードのスキャン.....	9
使用: Black Duck Detect (Desktop).....	9
プロジェクトの作成.....	23
プロジェクトへのスキャンのマッピング.....	25
4. リスクの表示: Black Duck.....	28
ダッシュボード.....	28
プロジェクトバージョンのページ.....	30
ダッシュボードの表示.....	31
プロジェクトの健全性の表示.....	43
セキュリティ上のリスクについて.....	49
セキュリティ上のリスクのレベル.....	49
推定セキュリティリスク.....	50
推奨されるワークフロー.....	50
5. 構成表の表示.....	52
構成表でコンポーネントとコンポーネントバージョンを調整する.....	52

まえがき

Black Duck documentation

Black Duckのドキュメントは、オンラインヘルプと次のドキュメントで構成されています：

タイトル	ファイル	説明
リリースノート	release_notes.pdf	新機能と改善された機能、解決された問題、現在のリリースおよび以前のリリースの既知の問題に関する情報が記載されています。
Docker Swarmを使用したBlack Duckのインストール	install_swarm.pdf	Docker Swarmを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
Kubernetesを使用したBlack Duckのインストール	install_kubernetes.pdf	Kubernetesを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
OpenShiftを使用したBlack Duckのインストール	install_openshift.pdf	OpenShiftを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
使用する前に	getting_started.pdf	初めて使用するユーザーにBlack Duckの使用法に関する情報を提供します。
スキャンベストプラクティス	scanning_best_practices.pdf	スキャンのベストプラクティスについて説明します。
SDKを使用する前に	getting_started_sdk.pdf	概要およびサンプルのユースケースが記載されています。
レポートデータベース	report_db.pdf	レポートデータベースの使用に関する情報が含まれています。
ユーザーガイド	user_guide.pdf	Black DuckのUI使用に関する情報が含まれています。

KubernetesまたはOpenShiftの環境にBlack Duckソフトウェアをインストールするには、Helmを使用します。次のリンクをクリックすると、マニュアルが表示されます。

- ・ [Helm](#)は、Black Duckのインストールに使用できるKubernetesのパッケージ マネージャです。Black Duck は Helm3をサポートしており、Kubernetesの最小バージョンは1.13です。

Black Duck 統合に関するドキュメントは、次のリンクから入手できます：

- ・ <https://sig-product-docs.synopsys.com/bundle/integrations-detect/page/integrations/integrations.html>
- ・ https://sig-product-docs.synopsys.com/category/cicd_integrations

カスタマサポート

ソフトウェアまたはドキュメントについて問題がある場合は、Black Duckカスタマー サポートに問い合わせてください。

Black Duckサポートには、複数の方法でお問い合わせできます。

- ・ オンライン: <https://www.synopsys.com/software-integrity/support.html>
- ・ 電話: お住まいの地域の電話番号については、[サポートページ](#)の下段にあるお問い合わせのセクションを参照してください。

サポート ケースを開くには、Black Duck Software Integrityコミュニティ サイト(<https://community.synopsys.com/s/contactsupport>)にログインしてください。

常時対応している便利なリソースとして、[オンラインカスタマポータル](#)を利用できます。

Black Duck Software Integrityコミュニティ

Black Duck Software Integrityコミュニティは、カスタマー サポート、ソリューション、情報を提供する主要なオンラインリソースです。コミュニティでは、サポートケースをすばやく簡単に開いて進捗状況を監視したり、重要な製品情報を確認したり、ナレッジベースを検索したり、他のSoftware Integrityグループ (SIG) のお客様から情報を得ることができます。コミュニティセンターには、共同作業に関する次の機能があります。

- ・ つながる – サポートケースを開いて進行状況を監視するとともに、エンジニアリング担当や製品管理担当の支援が必要になる問題を監視します。
- ・ 学ぶ – 他のSIG製品ユーザーの知見とベストプラクティスを通じて、業界をリードするさまざまな企業から貴重な教訓を学ぶことができます。さらに、Customer Hubでは、Black Duckからの最新の製品ニュースやアップデートをいつでもご覧いただけます。これは、当社製品やサービスをより有効に活用し、オープンソースの価値を組織内で最大限に高めることができます。
- ・ 解決する – SIGの専門家やナレッジベースが提供する豊富なコンテンツや製品知識にアクセスして、探している回答をすばやく簡単に得ることができます。
- ・ 共有する – Software Integrityグループのスタッフや他のお客様とのコラボレーションを通じて、クラウドソースソリューションに接続し、製品の方向性について考えを共有できます。

[Customer Successコミュニティにアクセスしましょう](#)。アカウントをお持ちでない場合や、システムへのアクセスに問題がある場合は、[こちら](#)をクリックして開始するか、community.manager@synopsys.comにメールを送信してください。


トレーニング

Black Duck Software Integrityグループ (SIG) は、Black Duckの教育ニーズをすべて満たすワンストップ リソースです。ここでは、オンライントレーニングコースやハウツービデオへの24時間365日のアクセスを利用できます。

新しいビデオやコースが毎月追加されます。

Black Duck Software Integrityグループ (SIG) のCustomer Educationでは、次のことができます。

- ・ 自分のペースで学習する。
- ・ 希望する頻度でコースを復習する。
- ・ 試験を受けて自分のスキルをテストする。
- ・ 終了証明書を印刷して、成績を示す。

詳細については、<https://community.synopsys.com/s/education>でご確認ください。また、Black Duckに関するヘルプについては、ヘルプメニューの[チュートリアル] () (Black DuckのUIに表示)を選択してください。

Black Duck 包括性と多様性に関する声明

Black Duck は、すべての従業員、お客様、パートナー様が歓迎されていると感じられる包括的な環境の構築に取り組んでいます。当社では、製品およびお客様向けのサポート資料から排他的な言葉を確認して削除しています。また、当社の取り組みには、設計および作業環境から偏見のある言葉を取り除く社内イニシアチブも含まれ、これはソフトウェアやIPに組み込まれている言葉も対象になっています。同時に、当社は、能力の異なるさまざまな人々が当社のWebコンテンツおよびソフトウェアアプリケーションを利用できるように取り組んでいます。なお、当社のIPは、排他的な言葉を削除するための現在検討中である業界標準仕様を実装しているため、当社のソフトウェアまたはドキュメントには、非包括的な言葉の例がまだ見つかる場合があります。

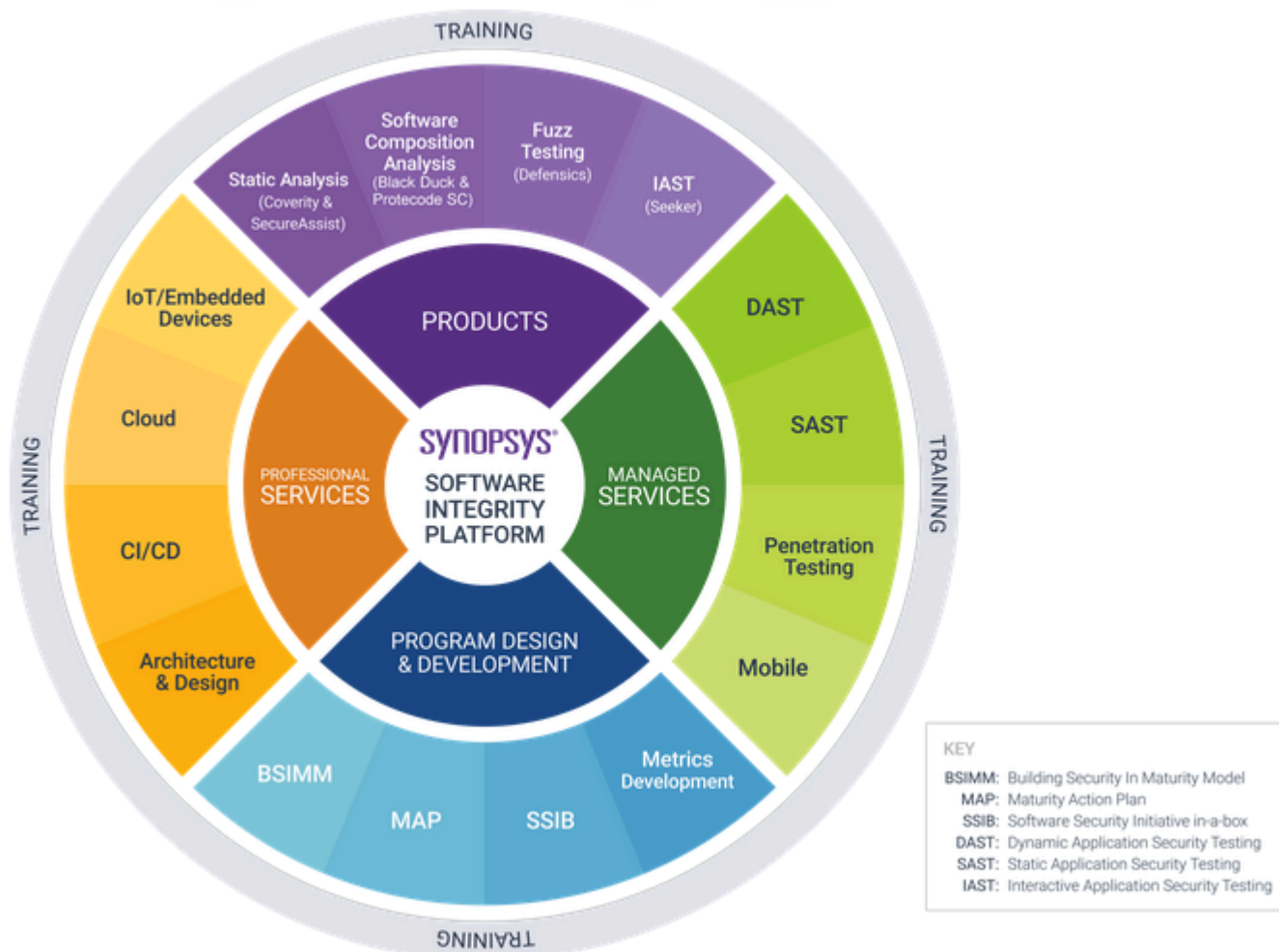
Black Duck セキュリティへの取り組み

Black Duckは、お客様のアプリケーションの保護とセキュリティの確保に専念する組織として、お客様のデータ セキュリティとプライバシーにも同様に取り組んでいます。この声明は、Black Duckのお客様と将来のお客様に、当社のシステム、コンプライアンス認証、プロセス、その他のセキュリティ関連活動に関する最新情報をお届けすることを目的としています。

この声明は次の場所で入手できます。[セキュリティへの取り組み | Black Duck](#)

1. 概要 Black Duck

Black Duck Software Integrityグループ(SIG)は、お客様のセキュリティをサポートする包括的なサービスとツールのスイートを提供します。セキュリティを始めたばかりのお客様から、確立されたプログラムを強化するお客様まで、SIGは成功に必要な専門知識、スキル、製品を備えています。




Black Duckは、ソフトウェアコンポジション解析(SCA)ツールで、ソフトウェアのサプライチェーンの管理、使用中のサードパーティコンポーネントの理解、既知の脆弱性およびライセンスによるリスクの最小化に役立ちます。Black Duck は、主にソース解析に基づいたサプライチェーン管理のための包括的なソリューションです。

Black Duckを使うと、次のことができます。

- ・ コードをスキャンし、コードベース内のオープンソースソフトウェアを判定する。
- ・ ソフトウェアプロジェクトの構成表(BOM)を生成して表示する。
- ・ オープンソースコンポーネントで判定された脆弱性を表示する。
- ・ セキュリティ上のリスク、ライセンス上のリスク、運用上のリスクを評価する。


2. ログイン: Black Duck

Black Duckにログインすると、チームメンバーまたは会社の従業員に限定されている可能性のあるプロジェクトを検索できます。

 **注:** Black Duckにアクセスするには、ユーザー名とパスワードが必要です。ユーザー名を持っていない場合は、システム管理者に問い合わせてください。Black DuckでLDAPの使用を設定している場合は、その認証情報を使ってBlack Duckにログインできる場合があります。

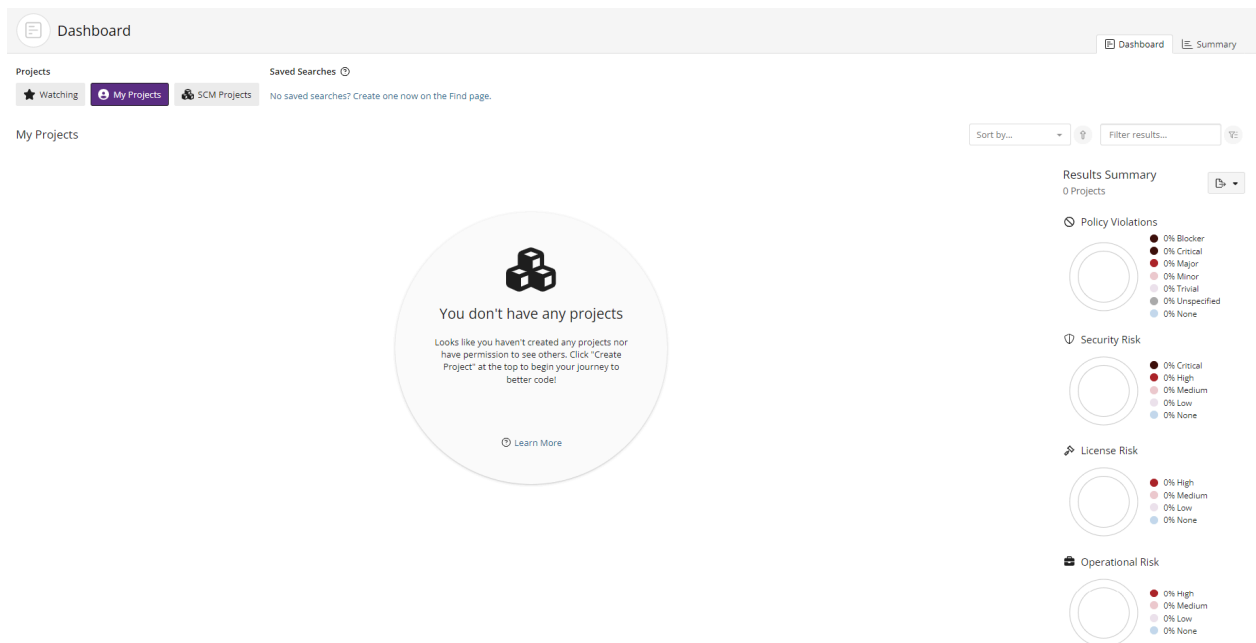
Black Duckにログインするには、次の手順を実行します。

1. ブラウザを使用して、システム管理者から提供されるBlack DuckのURLに移動します。通常、URLはhttps://<サーバーホスト名>という形式になります。
2. Black Duck管理者から提供されたユーザー名とパスワードを入力します。パスワードは大文字と小文字が区別されます。

 **注:** 管理者がパスワード要件を有効にしている、かつパスワードが要件を満たしていない場合は、パスワードを変更する必要があることを通知するダイアログボックスが表示されます。パスワードを更新する際には、ダイアログボックスに表示されている要件を満たしていることを確認してください。パスワードがすべての要件を満たしていない限り、Black Duckにログインすることはできません。

3. [ログイン]をクリックします。

Black Duckをインストールした後の初回ログインでは、空のダッシュボードページが表示されます。Black Duckに情報が表示されるようにするには、次の章で説明するように、コードをスキャンしてコードをプロジェクトにマッピングする必要があります。



デフォルトでは、[ウォッチ]ダッシュボードと[マイプロジェクト]ダッシュボードのみが表示されます。また重要なプロジェクトバージョンやコンポーネントバージョンをすばやく表示できるように、カスタムダッシュボードを作成することもできます。そのためには、プロジェクトやコンポーネントを検索し、検索を保存します。保存済み検索は[ダッシュボード]ページに表示されます。

3. コードのスキャン

Black Duck コンポーネントスキャンは、ソフトウェアプロジェクトを構成するオープンソースソフトウェア (OSS) コンポーネントのセットを自動で特定できるスキャン機能です。コンポーネントスキャンは、コンポーネントのライセンス、脆弱性、OSSプロジェクトの健全性のような追加メタデータを提供するために、OSSコンポーネントを判定およびカタログ化することで、組織によるオープンソースバイナリ使用の管理を支援します。

Black Duck 次のスキャン ツールを提供します。

- Black Duck Detect。 [Detect](#)は、Black Duckに推奨されるスキャンツールです。
- Black Duckの高速スキャンは、開発者が、プロジェクトに含まれているオープンソースコンポーネントのバージョンが、オープンソースの使用に関する企業ポリシーに違反しているかどうかを迅速に判断する方法を提供します。Black Duck Detectを使用すると、高速スキャンがパッケージマネージャのスキャンのみを使用し、Black Duckサーバーデータベースとやり取りしないので、迅速に結果が返されます。高速スキャンの詳細については、Black Duckのオンライン ヘルプまたはユーザー ガイドを参照してください。
- Black Duck Detect (Desktop) (以下で説明)
- 署名スキャナのコマンドライン (CLI) バージョン詳細については、Black Duckのオンライン ヘルプまたはユーザー ガイドを参照してください。

使用: Black Duck Detect (Desktop)


Black Duck Detect (Desktop) には、コードのスキャンを容易にする新規インターフェイスが用意されています。

Black Duck Detect (Desktop) では、次のような操作を実行できます。

- ソースディレクトリ、バイナリと実行可能ファイル、Dockerイメージとディストリビューションを[スキャン](#)する。
- 後からアップロードする[スキャンファイルを作成](#)する。
- [スキャンファイルを管理](#)する。
- [スキャンファイルをBlack Duckに直接アップロード](#)する。
- [アップロードしたスキャンを表示](#)する。

Black Duck Detect (Desktop) を使用するには:

1. Black Duck Detect (Desktop) をダウンロードしてインストールします。
2. Black Duckサーバー設定を使用してBlack Duck Detect (Desktop) を設定し、インストール プロセスを完了します。
3. Black Duck Detect (Desktop) を使用して、ファイルをスキャンまたはアップロードするか、ファイルをスキャンしてアップロードします。

 **注:** スキャンサイズ制限 (5 GB、Black Duck – Binary Analysisは6 GB) を超えるとエラーメッセージが表示されます。このメッセージが表示された場合は、カスタマサポートに連絡してください。

お使いのシステムがBlack Duck Detectのシステム要件を満たしていることを確認してください。


- Black Duck Detectの最新バージョンのシステム要件については、[ここ](#)をクリックしてください。
- Black Duck Detectの前バージョンのドキュメントについては、[ここ](#)をクリックしてください。このページで、Black Duck Detectバージョンの検索とシステム要件の表示ができます。

3. コードのスキャン・使用: Black Duck Detect(Desktop)

ダウンロードとインストール: Black Duck Detect(Desktop)

1. Black Duckにログインします。
2. ユーザー名の下にあるドロップダウンメニューに移動して、[ツール]を選択します。
3. [ダウンロード]の[Black Duck Detect(デスクトップ)]セクションで使用するオペレーティングシステムを選択し、Google Cloud Storageから実行可能ファイルをダウンロードします。
4. 実行可能ファイルを実行し、Black Duck Detect(Desktop)をインストールします。

Black Duck Detect(Desktop)の以前のバージョンからアップグレードする場合には、前のバージョンからデータを移行するオプションが表示されます。

 **注:** アプリケーションはその名前に関連するディレクトリにインストールされるため、Black Duck Detect(Desktop)は、以前のバージョンのBlack Duck Detect Desktopをアンインストールしません。また、デフォルト以外のディレクトリにインストールされたバージョンのBlack Duck Detect(Desktop)もアンインストールしません。以前のバージョンのBlack Duck Detect Desktopやデフォルト以外のディレクトリにインストールされているバージョンのBlack Duck(Desktop)はすべて手動でアンインストールし、ショートカットを修正または削除する必要があります。

インストール後にBlack Duck Detect(Desktop)が開かず、次のエラーメッセージが表示される場合があります。

```
The SUID sandbox helper binary was found, but is not configured correctly. Rather than run without sandboxing I'm aborting now. You need to make sure that /opt/Black Duck Detect/chrome-sandbox is owned by root and has mode 4755.
```

この場合、お使いのオペレーティングシステムはカーネルレイヤーでサンドボックスをサポートしていません。サンドボックスを無効にしてBlack Duck Detect(Desktop)を実行するには、コマンドラインで次のように入力します。

```
synopsys-detect --no-sandbox
```

Windowsのコマンドラインオプション

- Black Duck Detectの無人(サイレント)インストール

```
./synopsys-detect-latest.exe /S
```
- 特定のディレクトリへのインストール

```
./synopsys-detect-latest.exe /D=C:\directory
```

Linuxバージョンのインストール: Black Duck Detect(Desktop)

1. 前のセクションで説明したように、Black Duckサーバーから実行可能ファイルをダウンロードします。
2. Black Duck Detect(Desktop)をインストールします。

```
cd Downloads
```

CentOS/RedHatにインストールするには:

```
sudo yum localinstall synopsys-detect-latest.rpm
```

Ubuntu/Debianにインストールするには:

```
sudo apt install ./synopsys-detect-latest.deb
```

3. chrome-sandboxの権限を変更します。

```
cd "/opt/Black Duck Detect"  
sudo chmod 4755 chrome-sandbox
```

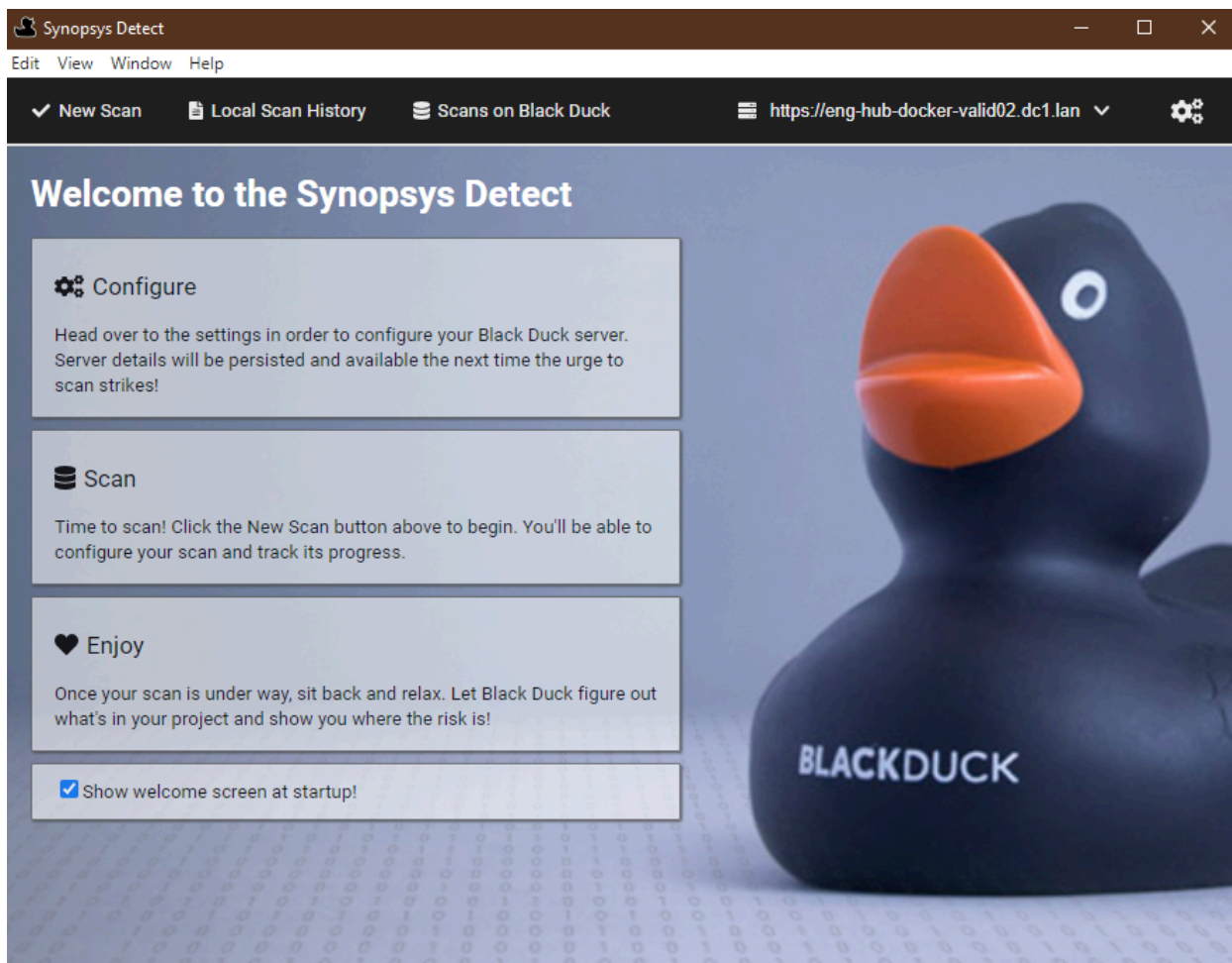
4. Black Duck Detect(Desktop)を実行します。


```
./synopsys-detect --no-sandbox
```

構成: Black Duck Detect (Desktop)

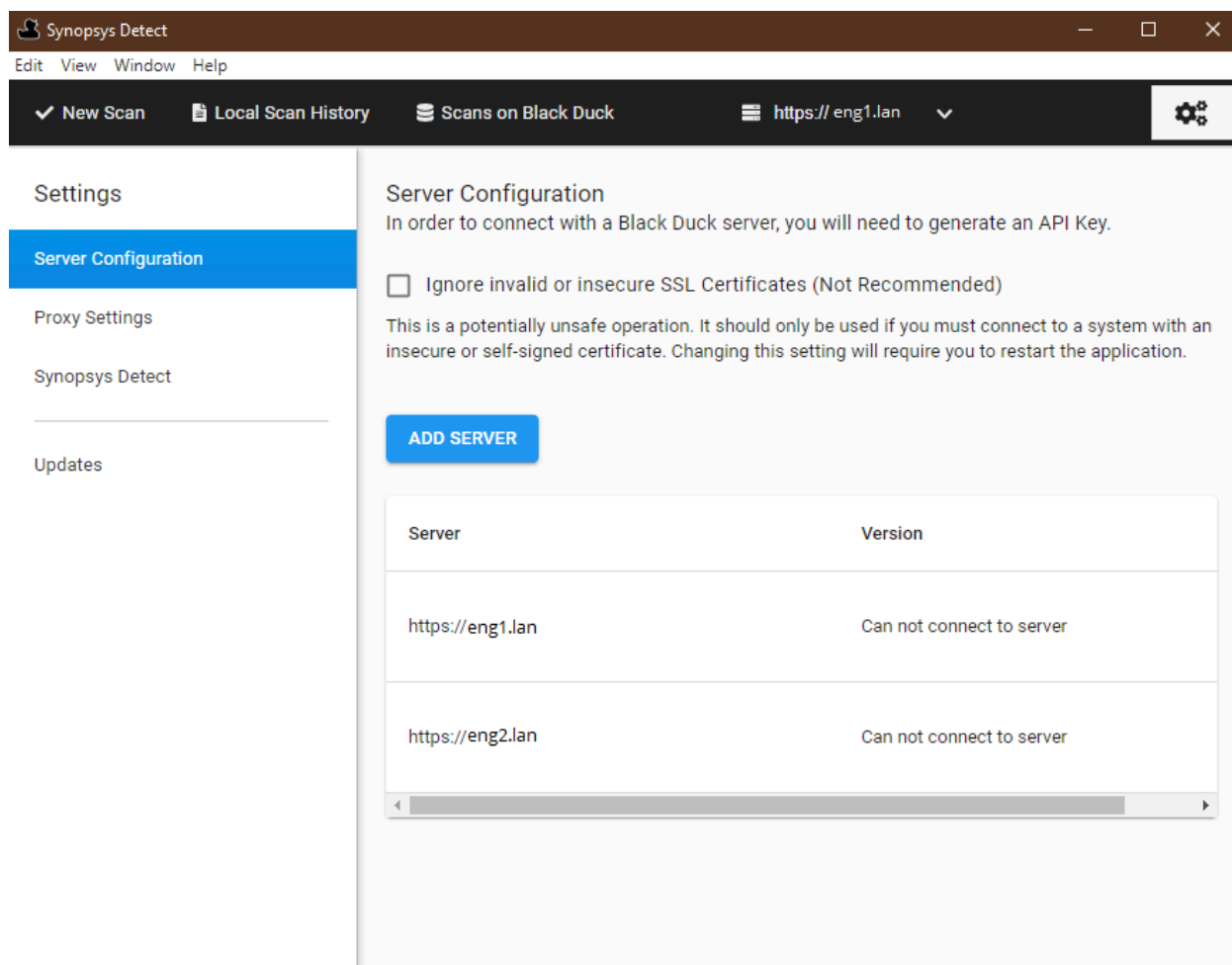
Black Duck Detect (Desktop) をインストールした後、Black Duck 設定を構成してインストールプロセスを続行します。

1. Black Duck Detect (Desktop) のアップグレードまたはインストールが完了すると、[ようこそ]ページが表示されます。



2. 右上隅にある  をクリックすると、[設定]ページが表示されます。

3. コードのスキャン・使用: Black Duck Detect (Desktop)



3. 以下の説明に従って、次のいずれかのタブを選択し、インストールおよび設定プロセスを完了します。

- ・ サーバー構成
- ・ プロキシ設定
- ・ Black Duck 検出
- ・ 更新

Black Duck サーバー構成

サーバーを追加するには、次の手順を実行します。

1. [サーバー構成]タブを選択し、[サーバーの追加]をクリックします。
[サーバーの追加]ダイアログボックスが表示されます。

Add Server

Black Duck Server URL

Generate New API Key

[Already have a key?](#)

To generate a new API key, enter your username and password for your Black Duck server. The API key name is used to identify the key and must be unique.

API Key Name

Username *

Password *

CANCEL

CREATE

2. [Black DuckサーバーURL]を指定します。ブラウザに入力する場合と同様に、Black DuckサーバーにURLを入力します (例: `https://servername:8443/`)。

必要に応じて、コンテキスト情報を入力します。たとえば、プロキシサーバー/ロードバランサ構成でX-Forwarded-Prefixヘッダーが指定される場合などです。

3. APIキー(ユーザーアクセストークン)を生成または入力します。

- ・ 新しいAPIキーを生成するには:
 - a. キー名、ユーザー名、およびパスワードを入力します。
 - b. [作成]をクリックします。
- ・ APIキーを入力するには:
 - a. [キーがすでにある場合]を選択します。
 - b. フィールドにAPIキーを入力します。
 - c. [作成]をクリックします。


4. [保存]をクリックします。Black Duck Detect (Desktop) がBlack Duckサーバーに接続され、接続先のBlack Duckのバージョンが表示されます。

APIキーを削除するには、次の手順を実行します。

APIキーを削除しても、Black Duckのキーは削除されません。ローカルでのみ削除されます。


1. [サーバー構成]タブを選択します。

3. コードのスキャン・使用: Black Duck Detect (Desktop)

2. サーバーの行で  をクリックして、[APIキーの削除]を選択します。
[APIキーの削除]ダイアログボックスが表示されます。

3. [OK]をクリックして確定します。

構成を削除するには

1. サーバーの行で  をクリックし、[構成の削除]を選択します。
[サーバー構成の削除]ダイアログボックスが表示されます。
2. [OK]をクリックして確定します。

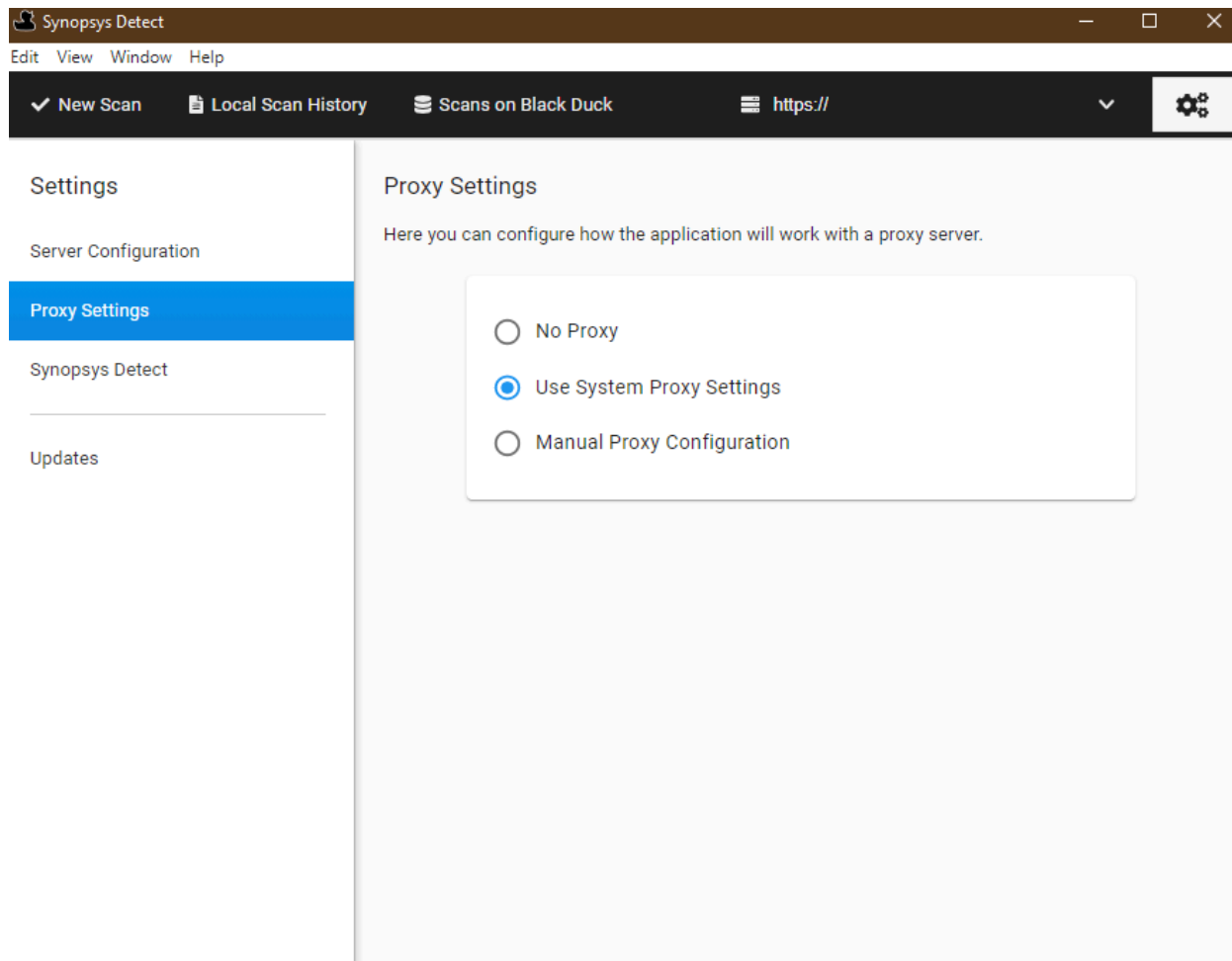
プロキシ設定

プロキシ経由でのBlack Duck Detect (Desktop)へのアクセスがサポートされています。Black Duck Detect (Desktop) は、ローカルシステムのプロキシ設定を自動的に使用します。

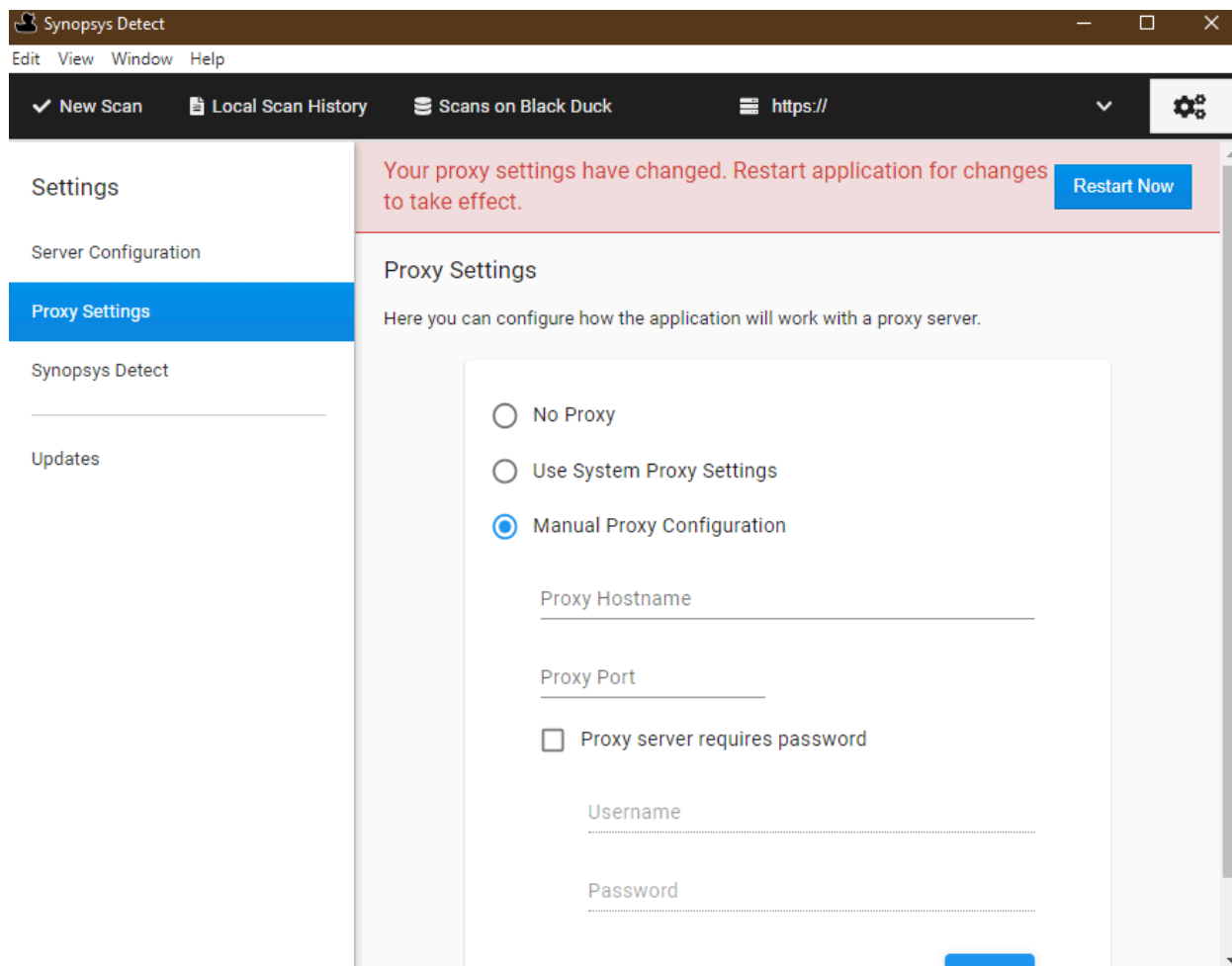
プロキシ設定を手動で入力する必要がある場合、またはプロキシを必要としない場合は、これらのデフォルト設定を変更できます。

デフォルトのプロキシ設定を変更するには、次の手順を実行します。

1. [プロキシ設定]タブを選択します。



2. [プロキシなし]または[手動プロキシ構成]を選択します。
3. 手動プロキシ構成を選択した場合は、次の手順を実行します。



- a. 次の情報を入力します。
 - ・ プロキシのホスト名。
 - ・ ポート番号。
 - ・ 認証の必要の有無。
 - ・ ユーザー名とパスワード。

プロキシが有効になっていて認証が必要な場合は、ユーザー名とパスワードを再入力する必要があります。

- b. [保存]をクリックします。

4. アプリケーションを再起動します。

Black Duck Detect設定の構成


必要に応じて、[Synopsys Detect]を選択します。また、必要に応じて、Black Duck Detect設定を定義し、使用しないビルドツールをクリアするか、ビルドツールへのパスを手動で設定します。


更新の確認

[更新]タブを選択し、Black Duck Detect(Desktop)の更新があるかどうかを確認できます。このページには、最後に更新を確認した日時が表示されます。新しいバージョンがあるかどうかを確認するには、[更新の確認]をクリックします。このオプションは、WindowsおよびMacOSシステムでのみ使用できます。

証明書


Black Duckに接続する際には、無効または安全でないSSL証明書を無視できます。

1. 右上隅にあるをクリックすると、[設定]ページが表示されます。
2. [サーバー構成]タブを選択します。
3. [無効な、または安全でないSSL証明書を無視]チェックボックスをオンにします。
4. アプリケーションを再起動します。

 **注意:** この操作は安全でない可能性があります。使用するの、安全でない証明書または自己署名証明書があるシステムへの接続が必要な場合に限定してください。

または、自己署名証明書をインポートする場合は、この操作をJREの標準keytoolインポートプロセスに従って実行できます。

Black Duck Detectが使用しているJREの場所を特定します。


1. 右上隅のをクリックすると、[設定]ページが表示されます。
2. [Black Duck Detect]タブを選択します。
3. [プロパティ]メニューから[パス]を選択します。または、[検索プロパティ]検索フィールドに「パス」を入力して、表示されるオプションを絞り込みます。
4. [Java実行可能ファイル]フィールドに値がない場合、Black Duck Detectでは、システム環境変数で設定された\$JAVA_HOMEの下にインストールされたJREが使用されます。

Black Duck Detectが使用しているJREの場所がわかったので、証明書に関連のcacertsファイル(通常はlib/securityフォルダ内にあります)にインポートする必要があります。

1. ターミナルセッション内で、(パスを適切なものに変更して)次のコマンドを実行します。

```
keytool -import -trustcacerts -keystore <path_to_keystore> -file <path_to_certificate> -alias <alias_for_cert>
```

2. パスワードが求められます。入力し、Enterキーを押します。
3. 証明書を信頼するかどうかを求められます。内容を確認し、必要に応じて受け入れます。

 **注:** チェーンに関連付けられている中間証明書もインポートする必要がある場合があります。インポートプロセスで問題が発生した場合は、IT部門にお問い合わせください。

スキャンオプション

Black Duck Detect(Desktop)により、以下のスキャンが容易になります。

- ・ ソースディレクトリ
- ・ バイナリまたは実行可能ファイル
- ・ Dockerイメージまたはディストリビューション


デフォルトでは、すべてのスキャンがBlack Duckサーバーにアップロードされ、プロジェクト バージョンにマップされます。ただし、[ここ](#)で説明するようにスキャンファイルを作成して、後でBlack Duckにアップロードできるファイルにスキャンを出力できます。

プロジェクト名やバージョン名を指定するには:

1. [プロジェクト設定]の横にある[追加]をクリックします。
2. [プロジェクト名]または[バージョン名]、あるいはその両方を選択します。UIにフィールドが表示されます。
3. フィールドの値を指定します。


ソースディレクトリのスキャン

ソースディレクトリをスキャンするには、次の手順を実行します。

1. [新規スキャン]をクリックします。
2. [スキャンのタイプ]リストから、[ソースディレクトリ]を選択します。
3.  をクリックして、スキャンするディレクトリを選択します。
4. 必要に応じて、[追加]をクリックして設定を選択し、プロジェクトまたはスキャン設定を変更または構成します。
スニペットスキャンライセンスを購入された場合は、スニペットスキャンを有効にするには、[スキャン設定]オプションから[スニペットマッチング]を選択して有効にします。
5. [スキャン]をクリックします。
スキャンのステータスが、スキャンをキャンセルするオプションとともに表示されます。
6. スキャンが完了したら、[ローカルスキャン履歴]タブを選択して、完了したスキャンに関する情報を表示します。
このタブでは、[スキャンを管理](#)できます。[スキャン]タブを使用して、アップロードされたスキャンを表示することもできます。


バイナリ/実行可能ファイルのスキャン

単一のバイナリまたは実行可能ファイルをスキャンするには、次の手順を実行します。

1. [新規スキャン]をクリックします。
2. [スキャンのタイプ]リストから、[バイナリ/実行可能ファイル]を選択します。
3.  をクリックして、スキャンするバイナリ、または実行可能ファイルを選択します。
4. 必要に応じて、[追加]をクリックして設定を選択し、プロジェクトの設定を変更または構成します。
5. [スキャン]をクリックします。
スキャンのステータスが、スキャンをキャンセルするオプションとともに表示されます。
6. スキャンが完了したら、[ローカルスキャン履歴]タブを選択して、完了したスキャンに関する情報を表示します。
このタブでは、[スキャンを管理](#)できます。[スキャン]タブを使用して、アップロードされたスキャンを表示することもできます。

Dockerイメージまたはディストリビューションのスキャン

Dockerイメージまたはディストリビューション(.tarファイル)をスキャンするには、次の手順を実行します。


1. [新規スキャン]をクリックします。
2. [スキャンのタイプ]リストから、[Docker]を選択します。
3. 次のいずれかを実行します。
 - ・ Dockerイメージ名を入力します。
 - ・ [Dockerアーカイブ(.tar)の選択]を選択し、 をクリックして、スキャンするディレクトリを選択します。

3. コードのスキャン・使用: Black Duck Detect (Desktop)

4. 必要に応じて、[追加]をクリックして設定を選択し、プロジェクトの設定を変更または構成します。
5. [スキャン]をクリックします。
スキャンのステータスが、スキャンをキャンセルするオプションとともに表示されます。
6. スキャンが完了したら、[ローカルスキャン履歴]タブを選択して、完了したスキャンに関する情報を表示します。
このタブでは、[スキャンを管理](#)できます。[スキャン]タブを使用して、アップロードされたスキャンを表示することもできます。

スキャンファイルの作成

Black Duck Detect (Desktop)を使用してスキャン結果をファイルに出力し、Black Duck (以下の説明を参照)、[コマンドライン](#)、または[Black Duck UI](#)を使用して、後からファイルをBlack Duck Detect (Desktop)にアップロードすることができます。

 注: Black Duckサーバーと通信する必要があるため、スニペットスキャンをオフラインにすることはできません。

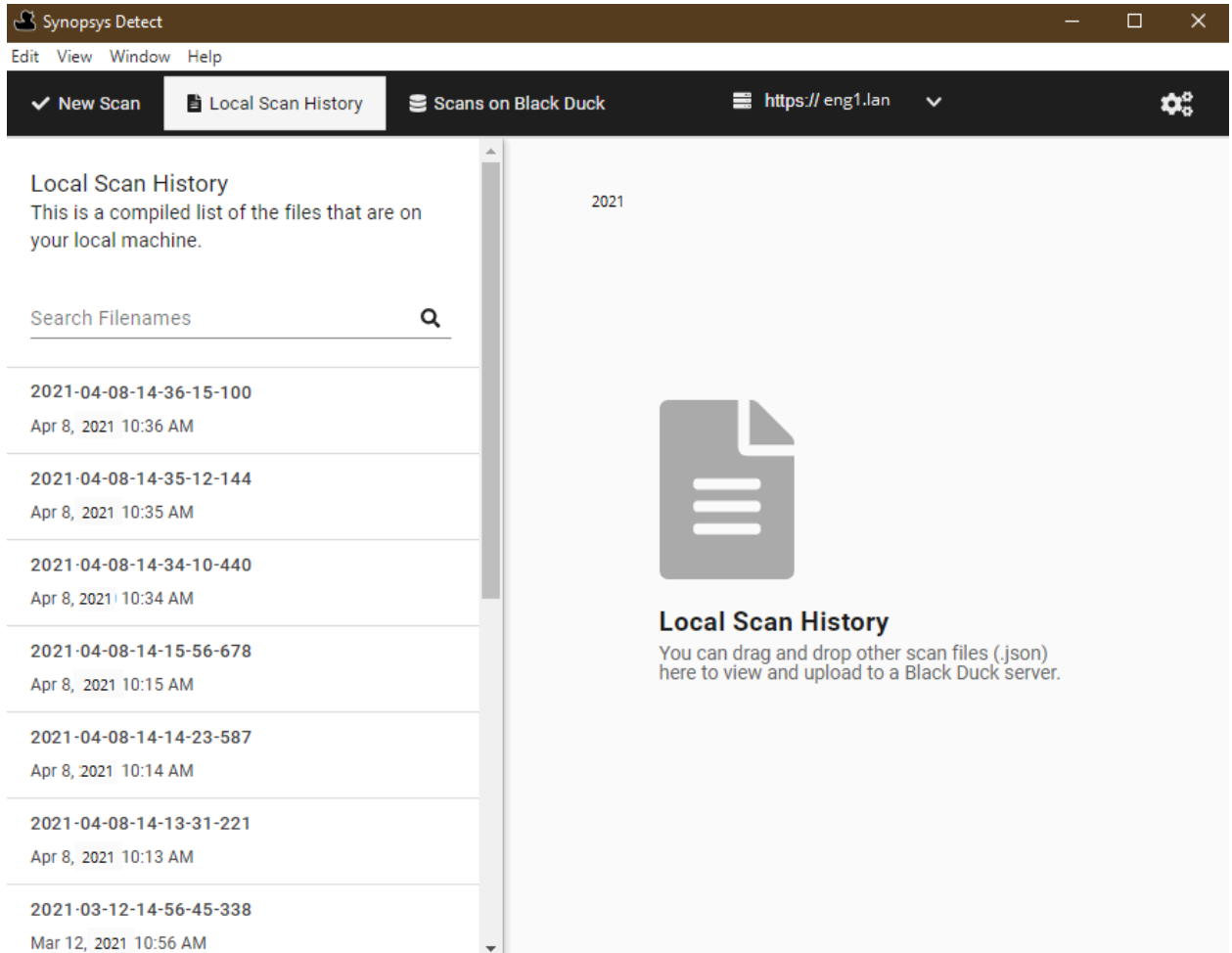
スキャンファイルを作成するには、次の手順に従います。

1. [新規スキャン]をクリックします。
2. スキャンのタイプ([ソースディレクトリ]、[バイナリ/実行可能ファイル]、または[Docker])を選択します。
3. 必要に応じて、任意のプロジェクトを変更または構成します。または、ソースディレクトリのスキャンの場合は、[追加]をクリックして設定を選択し、設定をスキャンします。
4. [オフラインモード]を選択します。
5. [スキャン]をクリックします。
スキャンのステータスが、スキャンをキャンセルするオプションとともに表示されます。
6. スキャンが完了したら、[ローカルスキャン履歴]タブを選択して、完了したスキャンに関する情報を表示します。

スキャンの管理

[ローカルスキャン履歴]タブを使用して、スキャンを管理します。

1. [ローカルスキャン履歴]をクリックします。
タブの左側のカラムに、ローカルシステム上のスキャンのリストが表示されます。

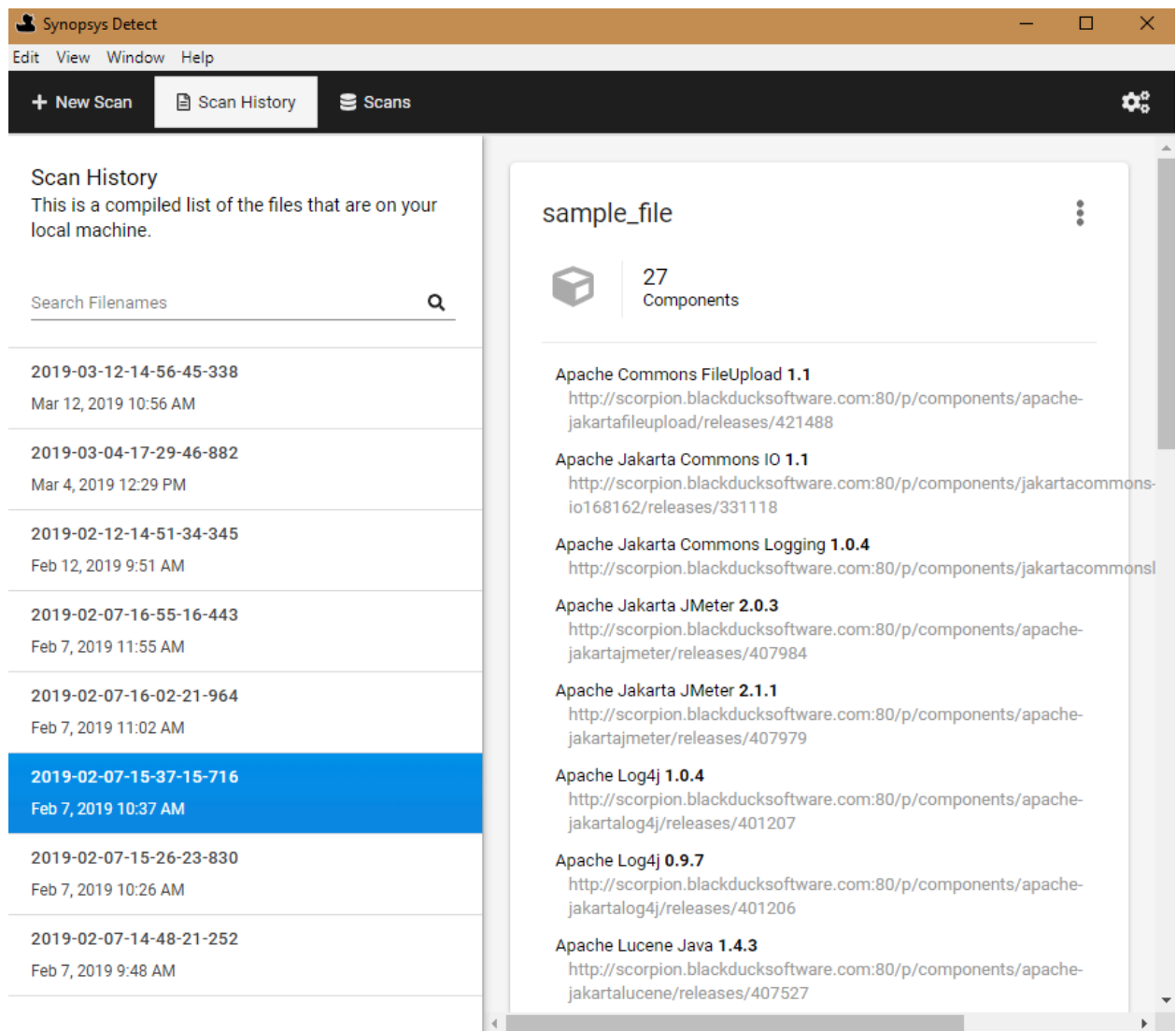



ローカルマシンからこのタブにスキャンをドラッグアンドドロップして管理します。

このタブでは、スキャンを選択して次の操作を実行できます。

- ・ スキャンの内容に関する情報を表示する。

3. コードのスキャン・使用: Black Duck Detect (Desktop)

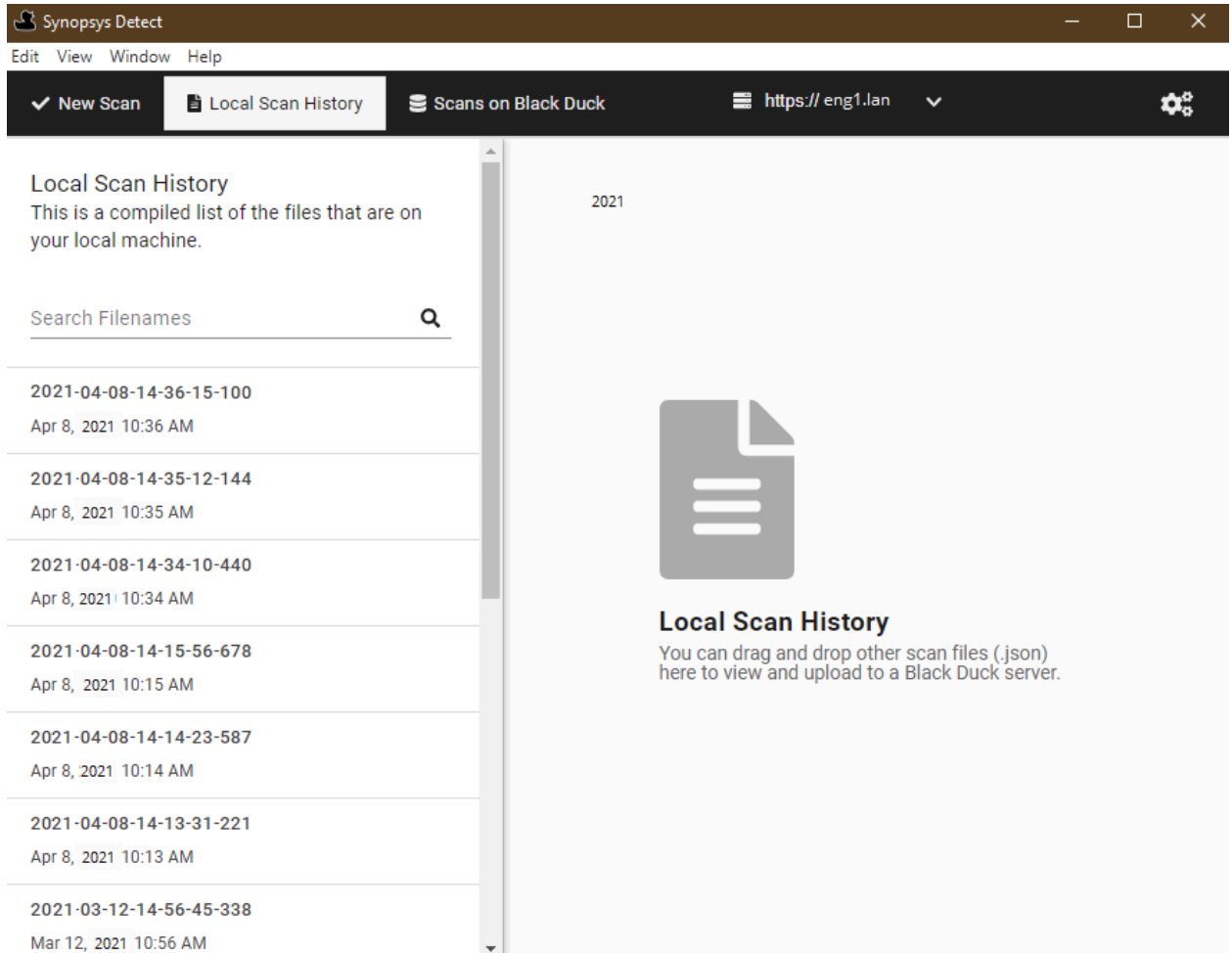



- ・  をクリックして、[ファイルの表示]を選択して、システム上のファイルの場所を表示する。
- ・ ファイルをアップロードする(次のセクションを参照)。
- ・ 左側の列のスキャン名にカーソルを合わせ、[削除]をクリックしてスキャンを削除します。[はい]をクリックして確定します。

スキャンファイルのアップロード: Black Duck

Black Duck Detect (Desktop)を使用して、スキャンファイルをBlack Duckにアップロードすることができます。

1. [ローカルスキャン履歴]をクリックします。

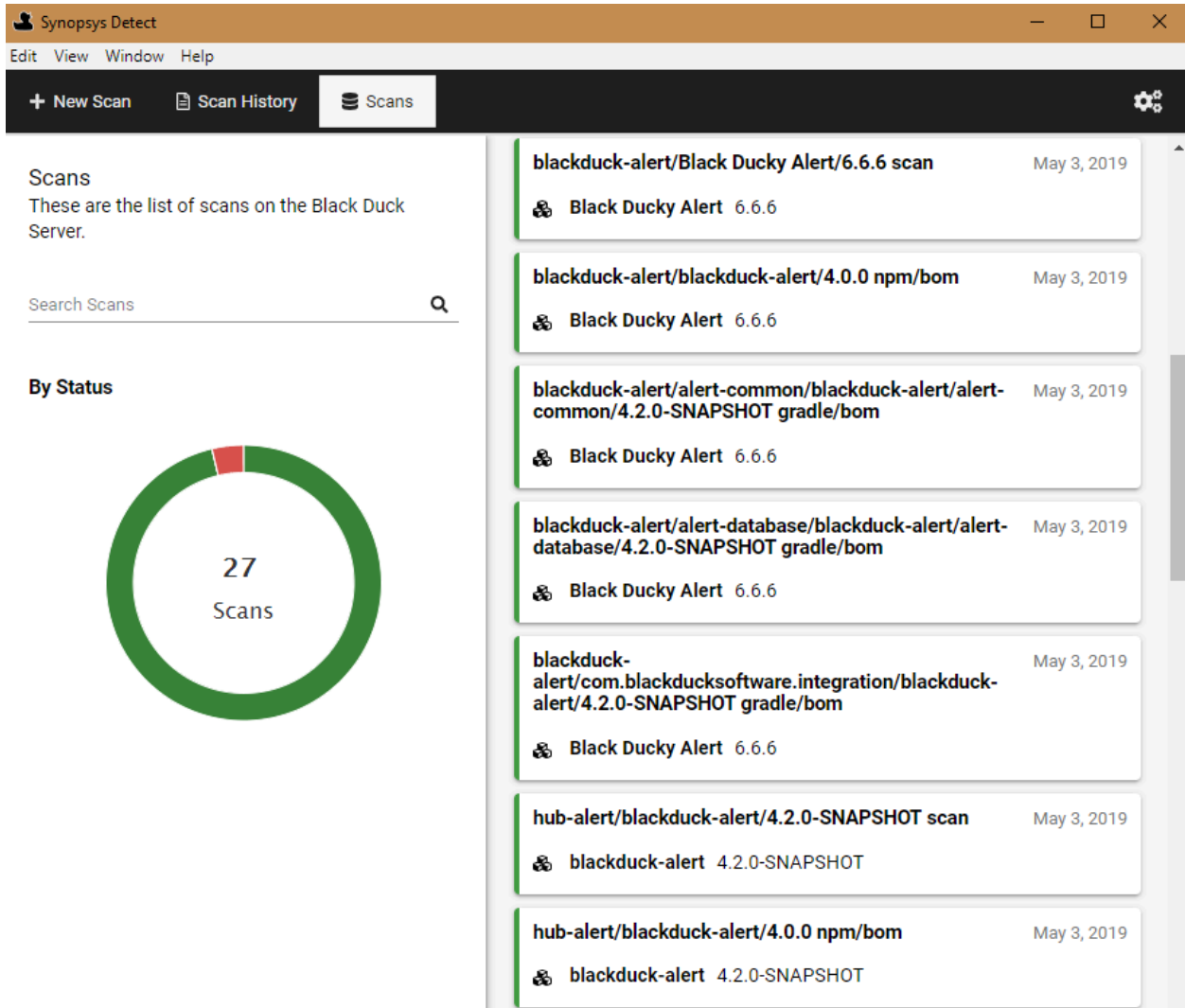


2. ファイルがローカルシステム上にある場合は、スキャンファイルをローカルマシンから[スキャン履歴]タブにドラッグ&ドロップできます。
3. アップロードするファイルを選択し、右上隅にある  をクリックすると、ファイルオプションが表示されます。
4. [スキャンファイルをBlack Duckにアップロードする]をクリックします。[アップロードの進行状況]ウィンドウが表示され、アップロードのステータスが示されます。プロセスが完了したら、ウィンドウを閉じます。
スキャンファイルがアップロードされたことを確認するには、[スキャン]をクリックして、アップロード済みのファイルを確認します。

アップロードしたスキャンの表示

Black DuckのUIにアップロードされたスキャンを表示するには、[Black Duckでスキャン]をクリックします。


3. コードのスキャン・使用: Black Duck Detect (Desktop)



このタブには、次の情報が表示されます。

- ・ タブの左側には、アップロードされたスキャンのステータス（進行中、完了、エラー）が表示されます。検索フィールドを使用してスキャンを検索するか、表示されるスキャンを制限します。
- ・ ページの右側には、スキャンが一覧表示され、それぞれのスキャンに関する次の情報が表示されます。
 - ・ 名前
 - ・ スキャンがマッピングされたプロジェクトおよびプロジェクトのバージョン。または、スキャンがプロジェクトにマッピングされていないことが示されます。
 - ・ スキャンがBlack Duckにアップロードされた日付。


スキャンを選択し、選択したスキャンのBlack Duckの[スキャン名]ページを開きます。

 注：Black Duck Detect (Desktop)に表示されるスキャンバイト数が、Black Duckに表示されるスキャンバイト数と異なる場合があります。これは、Black Duckが使用バイト数を計算する方法に起因します。正常な動作であり、一部のスキャンで発生することが予想されます。

プロジェクトの作成


プロジェクトは、Black Duckのベース単位です。プロジェクトは、スタンドアロンの開発プロジェクトとしても、別のプロジェクトの一部としても使用できます。たとえば、Apache Tomcatは、それだけでプロジェクトになりますが、他のより大きなプロジェクトの一部にすることもできます。組織内の他の開発者による検索を可能にするプロジェクトを作成する必要があります。

プロジェクトまたはアプリケーションは、10 GB以内のマネージド コード ベースに制限されます。

 注： [SCM統合](#) が有効になっている環境でSCMプロジェクトを作成する場合は、[SCMプロジェクトの作成](#)を参照してください。

プロジェクトを作成するには、次の手順を実行します。

1. Black Duckにログインします。
2. 任意のページの上で、[+プロジェクトの作成]をクリックします。[SCM統合](#) が有効になっている環境の場合は、メニューから[標準プロジェクト]を選択します。[プロジェクトの詳細]ページが表示されます。

 Create Project

Project Details

Project Group

Black Duck Project Groups × ▾

Project Name *

SCM Repository

Description

Version Details

Version Name *

SCM Branch

License

Start typing to select a license... ▾

Phase *

In Planning ▾

Distribution *


External ▾

Cancel

Save

- プロジェクト名を入力します。この名前はBlack Duck内のプロジェクト間で一意である必要があります。ただし、Black Duck KB内のプロジェクトと同じ名前であってもかまいません。

- ヒント：** ベストプラクティスとして、プロジェクト名の作成時に、他のユーザーがプロジェクトを検索する方法について考慮する必要があります。たとえば、プロジェクトが3Dグラフィックに関連する場合に「3DGraphics」という名前を付けると、ユーザーがプロジェクトを検索するためにプロジェクト名全体を入力する必要があります。名前でスペースまたは下線を使用すると（たとえば、「3D Graphics」や「3D_Graphics」）、追加した区切り文字により、ユーザーは、検索語句「3D」を使用してプロジェクトを見つけることができます。
- 必要に応じて、次のような追加情報を入力します。
 - SCMリポジトリ: コードが存在しているソースコード管理(SCM)リポジトリのURL。このフィールドは、環境でこの機能が有効になっている場合にのみ表示されます。パッケージマネージャスキャンの完了後にDetectを使用して、手動で編集したり自動的に入力したりすることができます。URLが一致しない場合、SCMリポジトリURLを手動で変更すると、既存のスキャンが中断される可能性があります。この機能はDetect 8.xでのみ使用できます。
 - 説明: ベストプラクティスとして、プロジェクトの説明の作成時に、他のユーザーがプロジェクトを検索する方法について考慮する必要があります。この説明は、他の同様のプロジェクトと簡単に区別できるように、プロジェクトで行われること、プロジェクトの独自性について具体的であることが必要です。
 - [バージョン名]フィールドに、このプロジェクトのバージョンを入力します。
 - デフォルトでは、このプロジェクトのバージョンへの編集は**このプロジェクトのすべてのバージョンに適用**されます（アーカイブされたバージョンと手動で追加したコンポーネントを除きます）。編集を特定のバージョンにのみ適用する場合は、このオプションをオフにします。
 - [保存]をクリックします。
Black Duck に[プロジェクト名]ページが表示されます。



Black Duck Project Groups
Sample Project

Project
★ Watching Project
Versions: 2
Owner: System Administrator
Overview
Settings

Description
 No description

Created
 Nov 28, 2022 by sysadmin

Tags
 No Tags

Custom Fields
 No custom fields

Updated
 Nov 28, 2022 by sysadmin

+ Create Version
+ Filter

Version	Phase	Last Updated	Last Scanned	License	Security Risk	License Risk	Operational Risk
1.0	In Planning	12:32 PM	Never	Unknown License			
1.1	In Planning	12:32 PM	Never	Unknown License			

Displaying 1-2 of 2

プロジェクトへのスキャンのマッピング

スキャンをマッピングすると、プロジェクトバージョンの構成表にスキャンデータが追加されます。

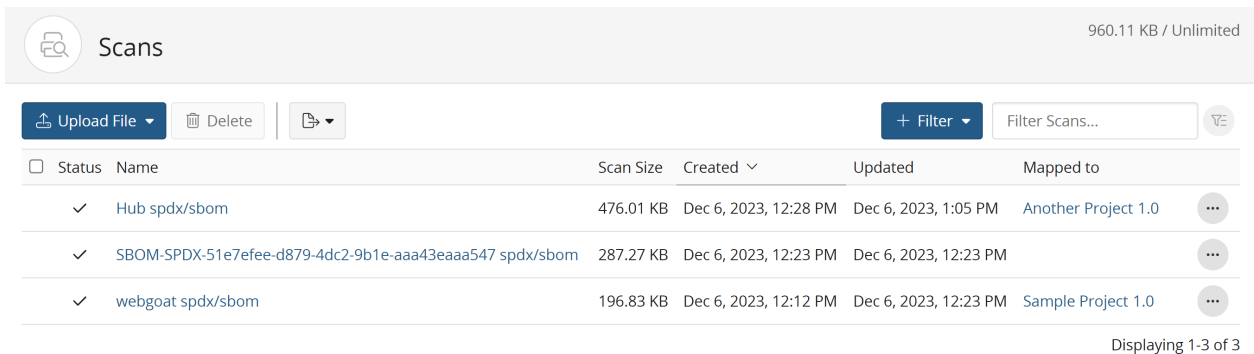
- 注：** Dockerイメージまたはファイルのディレクトリの場所およびアーカイブのスキャンは複数回できますが、プロジェクトバージョンへのマッピングは1回で済みます。ホストとパスは変更できますが、コードの場所の名前が同じであれば、Black Duckでは、以降のスキャンで検出された新しい情報でプロジェクトの構成表が自動的に更新されます。

スキャンをプロジェクトにマッピングするには、次の手順を実行します。

3. コードのスキャン・プロジェクトへのスキャンのマッピング

1. Black Duckにログインします。

2.  をクリックします。




Scans 960.11 KB / Unlimited

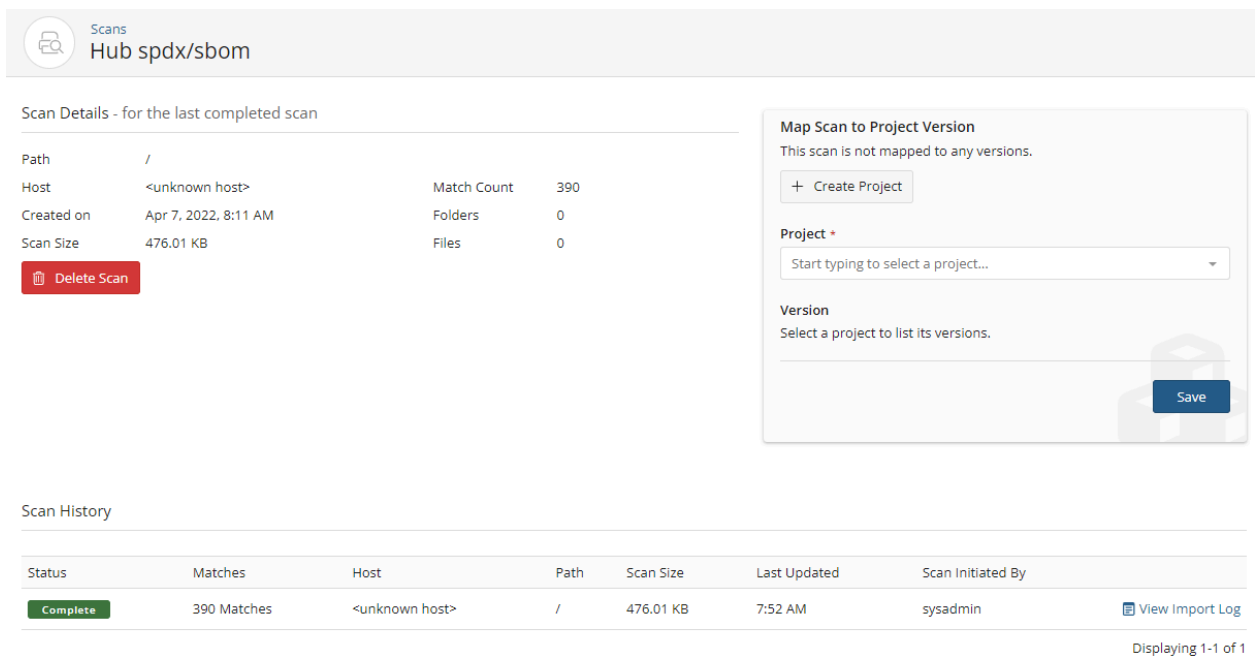
Upload File Delete Filter Scans...

Status	Name	Scan Size	Created	Updated	Mapped to
✓	Hub spdx/sbom	476.01 KB	Dec 6, 2023, 12:28 PM	Dec 6, 2023, 1:05 PM	Another Project 1.0
✓	SBOM-SPDX-51e7efee-d879-4dc2-9b1e-aaa43eaaa547 spdx/sbom	287.27 KB	Dec 6, 2023, 12:23 PM	Dec 6, 2023, 12:23 PM	
✓	webgoat spdx/sbom	196.83 KB	Dec 6, 2023, 12:12 PM	Dec 6, 2023, 12:23 PM	Sample Project 1.0

Displaying 1-3 of 3

3. 次のいずれかを実行します。

-  をクリックし、マッピングするスキャンの行の[プロジェクトへのマッピング]を選択します。
- マッピングするスキャンのパスを選択し、[スキャン名]ページを開きます。



Scans Hub spdx/sbom

Scan Details - for the last completed scan

Path /

Host <unknown host> Match Count 390

Created on Apr 7, 2022, 8:11 AM Folders 0

Scan Size 476.01 KB Files 0

Delete Scan

Map Scan to Project Version

This scan is not mapped to any versions.

+ Create Project

Project *

Start typing to select a project...

Version

Select a project to list its versions.

Save

Scan History

Status	Matches	Host	Path	Scan Size	Last Updated	Scan Initiated By
Complete	390 Matches	<unknown host>	/	476.01 KB	7:52 AM	sysadmin


View Import Log

Displaying 1-1 of 1

4. プロジェクトの名前の入力を始めて、[プロジェクト]フィールドにマッチを段階的に表示します。
必要に応じて、[プロジェクトの作成]を選択して、新規プロジェクトおよびバージョンを作成します。
5. コンポーネントスキャンをマッピングするプロジェクトバージョンを選択します。
必要に応じて、[バージョンの作成]を選択し、プロジェクトに新しいバージョンを作成します。
6. [保存]をクリックします。

Black Duck に、コンポーネントスキャンのマッピング先にしたプロジェクトの名前とバージョンが表示されます。リンクを選択して[構成表](#)ページを開きます。

3. コードのスキャン・プロジェクトへのスキャンのマッピング

 注：Black Duck により、集約されたプロジェクトバージョンの構成表が表示されます。アーカイブにコンポーネントバージョンが複数回出現した場合、構成表には1回のみ表示されます。

4. リスクの表示: Black Duck

Black Duck は、プロジェクトにわたってリスクのタイプと重大度をいくつかの詳細レベルで理解するのに役立ちます。リスクを計算するために使用されるデータは、Black Duck KBによって提供されます。


以下のページは、プロジェクト内のリスクの判定と管理に使用します。

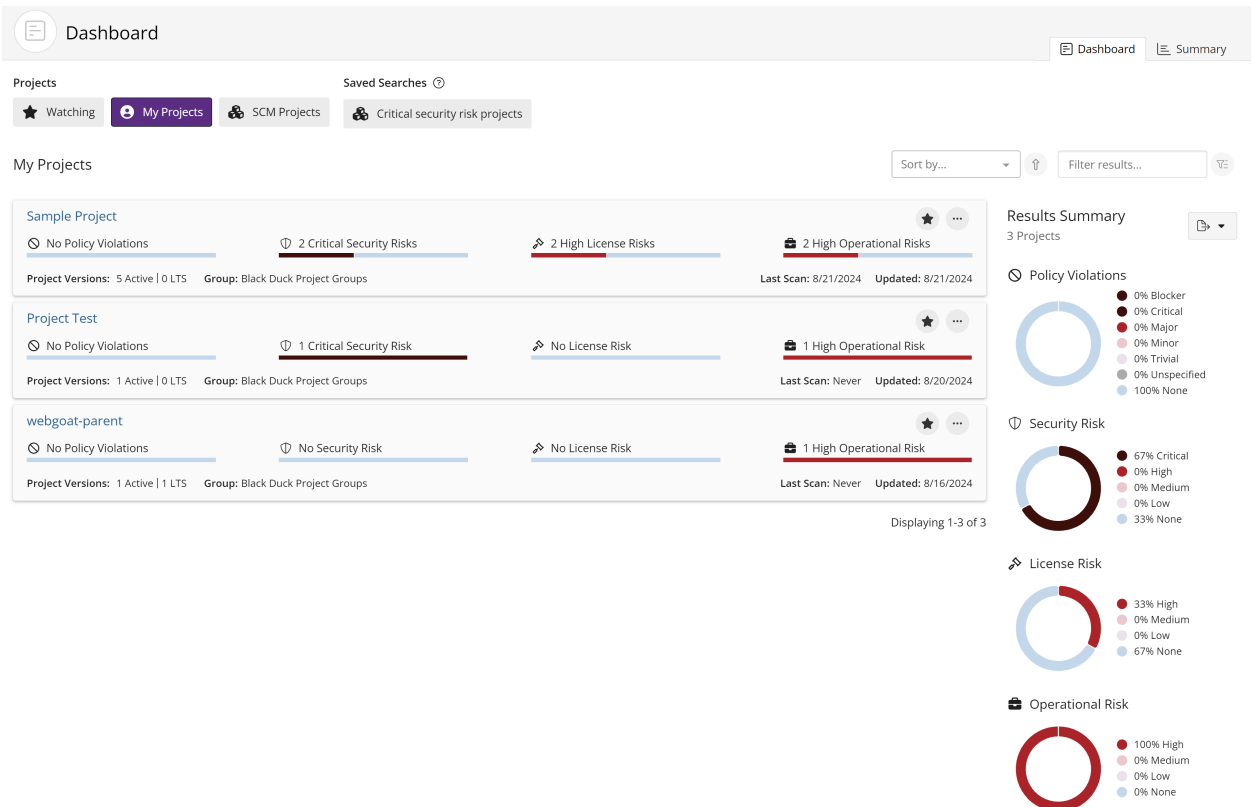
- ・ ダッシュボードのページ
- ・ プロジェクトバージョンページ/[コンポーネント]タブ
- ・ プロジェクトバージョンページ/[セキュリティ]タブ

表示されるセキュリティリスク値は、[選択したセキュリティリスク計算](#)に応じて、CVSS v2またはCVSS v3.xスコアを使用していることに注意してください。デフォルトでは、CVSS v3.xスコアが表示されます。CVSS v2を選択した場合、セキュリティ上のリスクグラフの緊急リスクカテゴリには0の値が表示されます。

ダッシュボード

ダッシュボードには、次のような視点による、リスクの大まかな概要が表示されます。

-  注: ダッシュボードにプロジェクトやコンポーネント情報が表示されるのは、[プロジェクトを作成](#)した後、プロジェクトに[スキャンをマッピング](#)するか構成表に[コンポーネントを手動で追加](#)するまでです。プロジェクトバージョンの構成表にあるコンポーネントのリスク情報は、ダッシュボードのページに表示されます。
- ・ [\[ウォッチ\]または\[マイプロジェクト\]ダッシュボード](#)を使用して目的のプロジェクトを表示したり、[プロジェクトの検索結果を保存](#)してカスタムダッシュボードを作成したりできます。



1つ以上のプロジェクトで使用されている興味のあるコンポーネントを表示するには、保存済み**コンポーネント検索**を作成してください。

Component - Apache Commons

Component	Version	Used By	First Detected	Release Date	Newer Versions	Last Vuln	Risk Level
Apache Commons BeanUtils	1.9.4	1 Project Version	5/31/2024	8/3/2019	1	Never	No License Risk
Apache Commons Codec	1.13	1 Project Version	5/8/2024	7/20/2019	17	Never	No License Risk
Apache Commons Codec	1.15	2 Project Versions	5/30/2024	9/1/2020	10	Never	No License Risk
Apache Commons Collections	3.2.2	2 Project Versions	5/30/2024	11/15/2015	33	Never	No License Risk
Apache Commons Collections	4.1	2 Project Versions	5/8/2024	11/28/2015	32	Never	No License Risk
Apache Commons Collections	4.4	1 Project Version	5/30/2024	7/9/2019	6	Never	No License Risk

Results Summary
42 Components
Results updated at Jun 12, 2024, 7:42 AM
Saved Search Settings

Security Risk

- 1% Critical
- 3% High
- 4% Medium
- 0% Low
- 92% None

License Risk

- 17% High
- 12% Medium
- 0% Low
- 71% None

Operational Risk

- 29% High
- 21% Medium
- 15% Low
- 35% None

保存済み**脆弱性検索**を作成して、関心のある脆弱性を表示します。

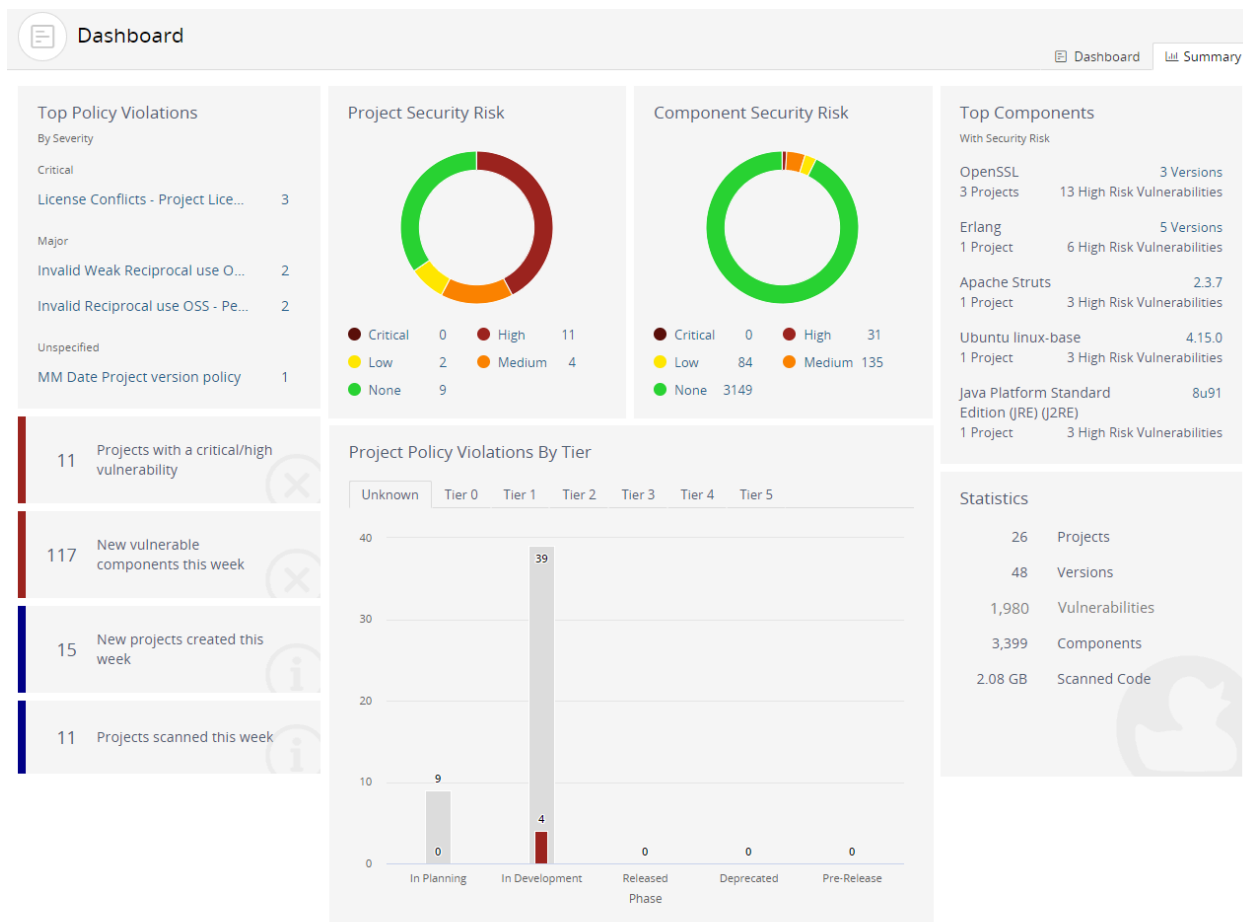
Vulnerability - Critical

Vulnerability ID	Used By	First Detected	Published	Last Modified	Overall Risk	Solution	Workaround	Exploit
BDSA-2015-0068	Project Versions	Never	11/14/2017	11/14/2017	9.2 Critical	✓ Solution	No Workaround	Exploit CWE-79
BDSA-2015-0080	Project Versions	Never	11/15/2017	11/15/2017	9.2 Critical	✓ Solution	No Workaround	Exploit CWE-79
BDSA-2010-0003	Project Versions	Never	11/28/2017	9/2/2018	9.1 Critical	No Solution	No Workaround	No Exploit CWE-20, CWE-712
BDSA-2011-0017	Project Versions	Never	5/9/2018	5/17/2022	9.2 Critical	✓ Solution	No Workaround	Exploit CWE-80


Results Summary
24,562 Vulnerabilities
Results updated at Jun 12, 2024, 7:42 AM
Saved Search Settings

概要ダッシュボードは、表示する権限があるプロジェクトの全体的な健全性を確認し、問題のある領域を判定するために使用します。

4. リスクの表示: Black Duck・プロジェクトバージョンのページ



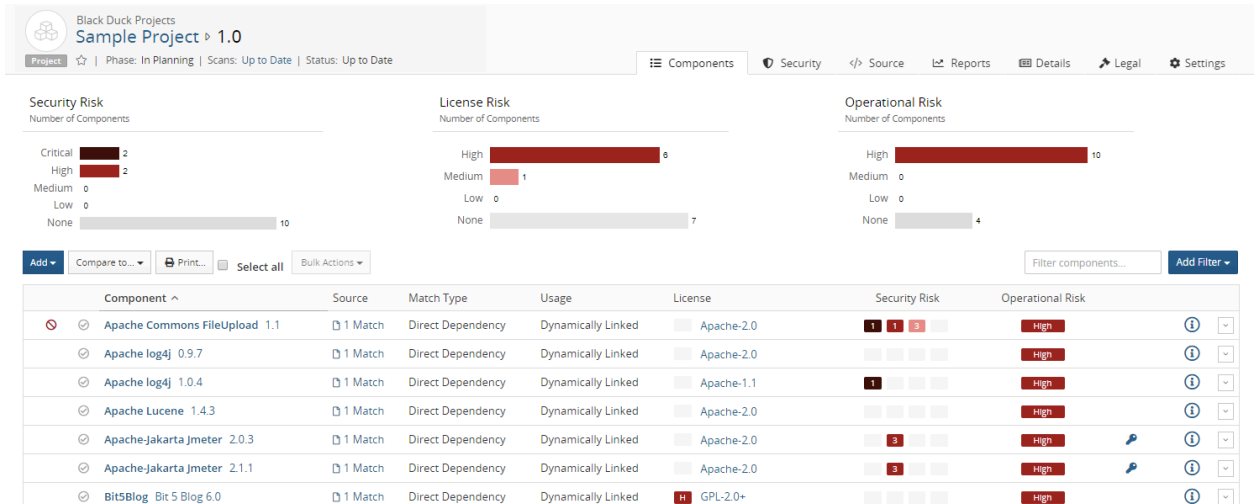
注:

- ログイン時に表示される[ダッシュボード]ページは、前回ログアウトする前に最後に表示したメインダッシュボード(ダッシュボードまたは概要)によって異なります。
-  またはナビゲーションバーの左上隅にあるロゴをクリックして、最後に表示したダッシュボード([ダッシュボード]または[概要])を表示します。

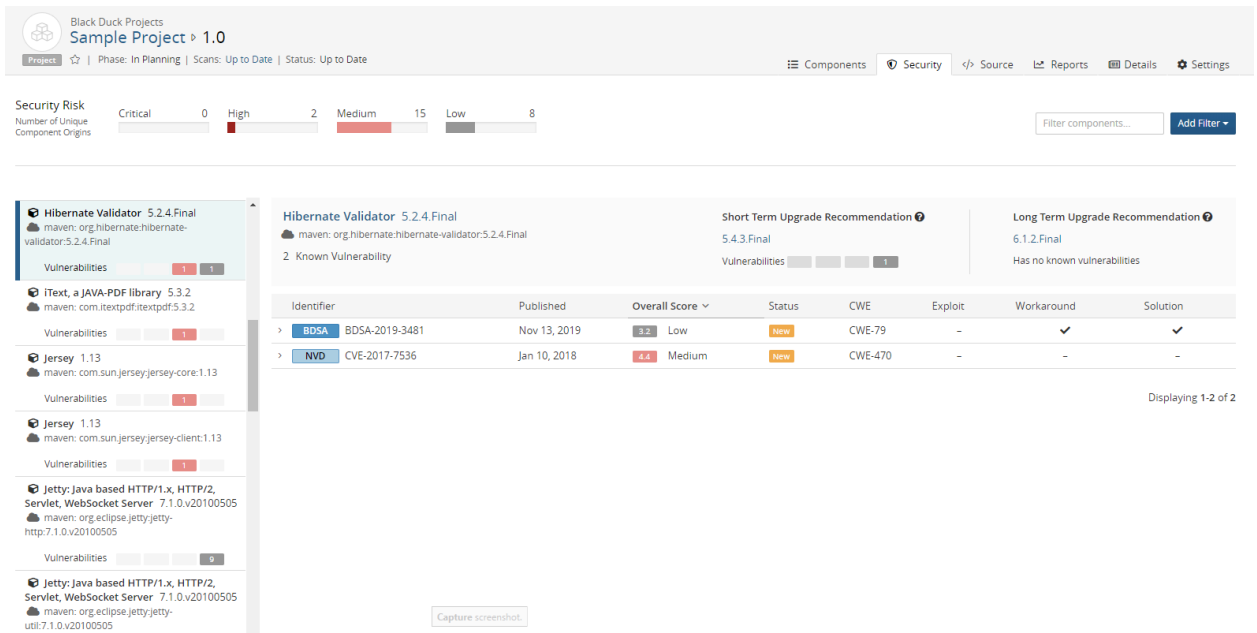
プロジェクトバージョンのページ

- [プロジェクトバージョンページ/\[コンポーネント\]タブ](#)は、プロジェクトバージョンの構成表とも呼ばれますが、セキュリティ上、ライセンス上、および運用上のリスクがあるコンポーネント(これはプロジェクトバージョン固有です)を表示するために使用します。

4. リスクの表示: Black Duck・ダッシュボードの表示



プロジェクトバージョンページ/[セキュリティ]タブは、プロジェクトバージョンで使用されているコンポーネントに関連付けられている各重大度のセキュリティ脆弱性を表示するために使用します。



ダッシュボードの表示

ダッシュボードを使用して、プロジェクトの1つ以上のバージョンに含まれるコンポーネントに関連付けられている、リスクのタイプと重大度およびポリシー違反を表示します。ダッシュボードは、プロジェクト、コンポーネント、および脆弱性を対象とする、全体的なビューです。

重要なプロジェクトとプロジェクトのバージョンを表示できるように、Black Duckでは、2つのデフォルトダッシュボードと、数に制限なくカスタムダッシュボードを作成する機能が用意されています。

Black Duck は以下の2つのデフォルトダッシュボードを表示します。

- ウォッチ。ウォッチするプロジェクト。
- マイプロジェクト。ウォッチしていないプロジェクトを含むすべてのプロジェクト。

4. リスクの表示: Black Duck・ダッシュボードの表示

これらのダッシュボードでは、プロジェクトレベルのダッシュボードページに情報が表示されます。

さらに、重要なプロジェクトバージョン、コンポーネントバージョン、および脆弱性をすばやく表示できるように、カスタムダッシュボードを作成することもできます。[プロジェクト](#)、[コンポーネント](#)、および/または[脆弱性を検索](#)してから、[検索を保存](#)します。[ダッシュボード]ページを使用して、保存済みの検索から情報を表示します。

ダッシュボードの表示

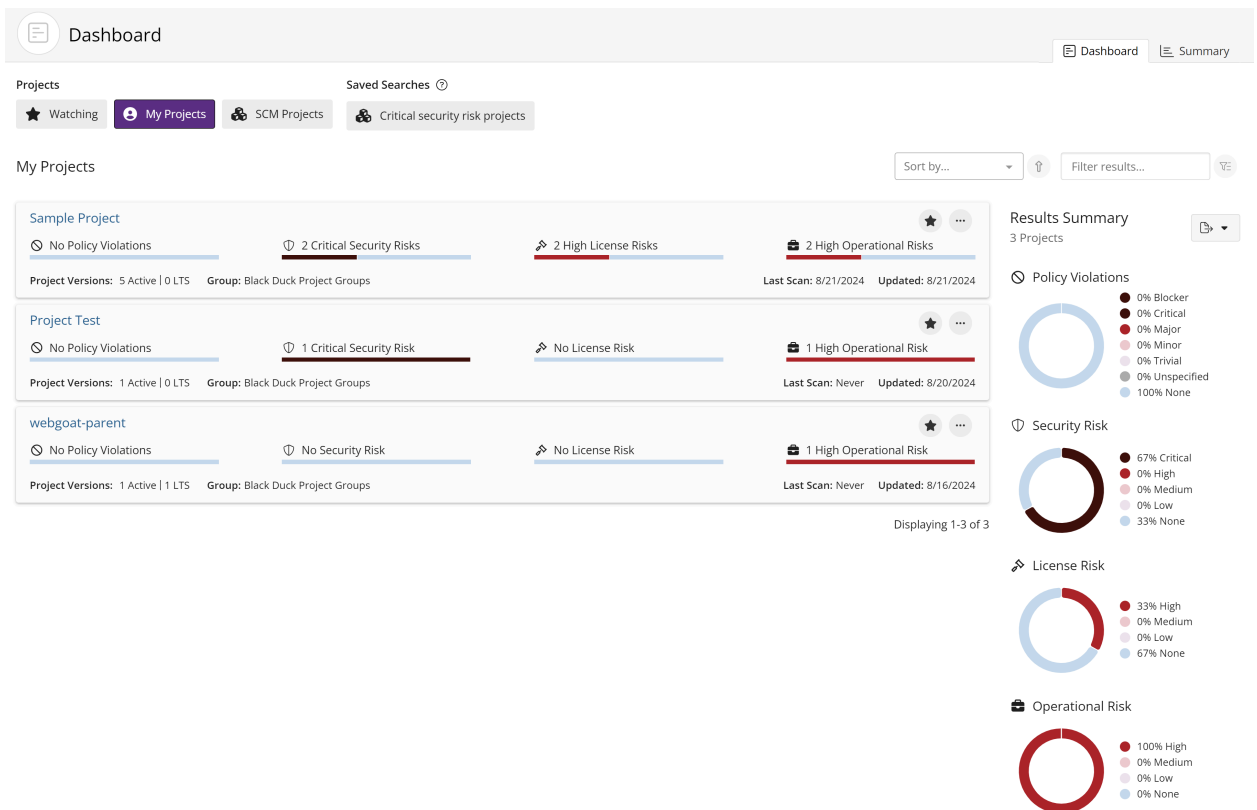
ダッシュボードを表示するには、次の手順を実行します。

1.



をクリックして、ダッシュボードを表示します。

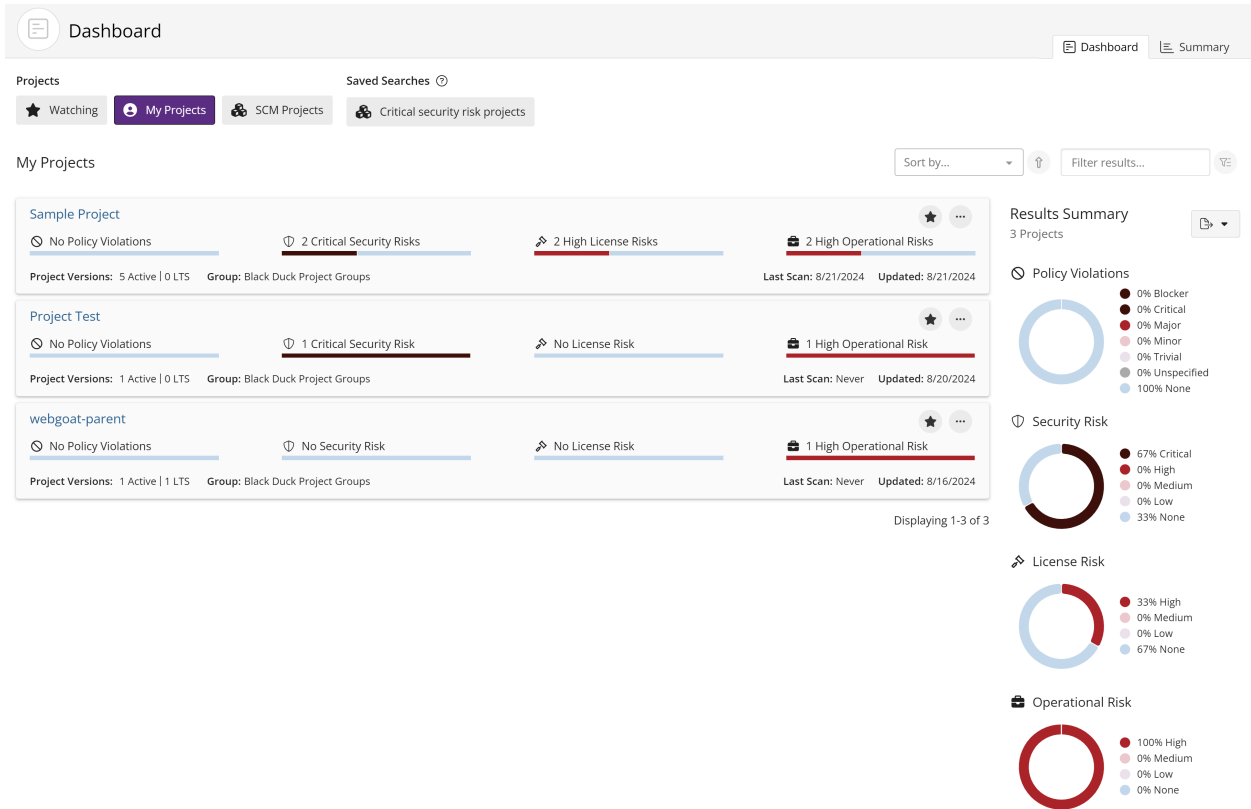
表示されるダッシュボードページは、以前に表示した最後のダッシュボード(特定のダッシュボードページまたは[概要ダッシュボード](#))によって異なります。表示されていない場合は、[ダッシュボード]を選択してダッシュボードを表示します。



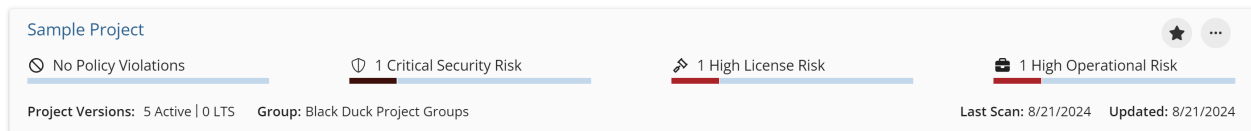
[ウォッチ]ダッシュボードと[マイプロジェクト]ダッシュボードについて


[ウォッチ]または[マイプロジェクト]ダッシュボードを使用して、リスクおよびポリシー違反情報をプロジェクトレベルで表示します。

4. リスクの表示: Black Duck・ダッシュボードの表示



プロジェクトごとに次の情報が表示されます。



- 特定のプロジェクトのポリシー違反情報を表示するには、次の手順を実行します。
 - バーを使用して、ポリシーの重大度レベルの最も高いプロジェクトバージョンの数を表示します。
-  注：テキストには、このプロジェクトに影響を与えるすべてのポリシーの重大度レベルではなく、ポリシーの重大度レベルの最も高いプロジェクトバージョンの数が記載されています。
- バーにカーソルを合わせると、ポリシー違反の重大度が最も高いプロジェクトバージョンの数が表示されます。

4. リスクの表示: Black Duck・ダッシュボードの表示

Policy Violations

by Project Version

1	Blocker	0	Minor
3	Critical	0	Trivial
0	Major	0	Unspecified

* Each project version is counted once by its highest severity risk

上記の例では、ポリシー違反がある4つのプロジェクトバージョンがあります。1つのバージョンには、最も高い重大度レベルが[ブロッカー]のポリシー違反があり、他の3つのバージョンには、最も高い重大度レベルが[緊急]のポリシー違反があります。これは、これらのバージョンのポリシー違反の数を示すものではなく、各バージョンの最も高い重大度レベルを示していることに注意してください。

- ・ リスク情報を表示するには、次の手順を実行します。
 - ・ リスクバーを使用して、リスクレベルが最も高いプロジェクトバージョンの数を表示します。

セキュリティリスク:


4 High Vulnerabilities

ライセンスリスク:

1 High License Risk

運用リスク:

4 High Operational Risks

 注: テキストには、バージョンに影響を与えるすべてのリスクレベルではなく、リスクレベルの最も高いプロジェクトバージョンの数が記載されています。

- ・ リスクバーにカーソルを合わせると、このプロジェクトの最も高いレベルのバージョンの数が表示されます。

Security Risk

by Project Version

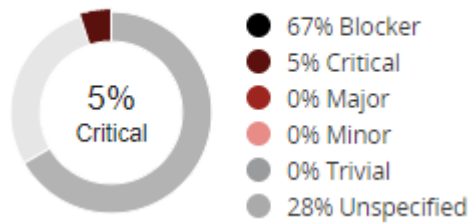
0	Critical	0	Medium
4	High	0	Low

* Each project version is counted once by its highest severity risk

プロジェクトバージョンにリスクがある場合、バージョンは1回だけカウントされ、その最も高いリスクレベルのみが表示されます。

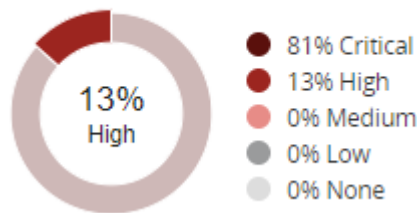
- ・ グラフを使用して、このダッシュボードのすべてのプロジェクトの概要情報を表示します。
 - ・ リスクグラフには、ポリシー違反が発生しているこのダッシュボード内のプロジェクトの割合が重大度別に表示されます。グラフ内の領域にカーソルを合わせると、次の情報を表示することもできます。




🔒 Policy Violations



- ・ リスクグラフには、このレベルのセキュリティ、ライセンス、または運用リスクを伴う、このダッシュボード内のプロジェクトの割合が表示されます。グラフ内の領域にカーソルを合わせると、次の情報を表示することもできます。

🛡️ Security Risk



- ・ 凡例の値にカーソルを合わせると、グラフ内で値が強調表示されます。
- ・ 各プロジェクトの追加情報を表示します。以下の情報が含まれます。
 - ・ バージョンの数。
 - ・ 最終スキャン日。
 - ・ 手動または新しいスキャンによって任意のプロジェクトバージョンにマッピングされているスキャンが最後に実行された日時や、任意のプロジェクトバージョンの構成表が最後に更新された日時など、このプロジェクトが最後に更新された日付。
- ・ プロジェクト名を選択すると、このプロジェクトのすべてのバージョンを一覧表示する[プロジェクト名]ページが表示されます。
- ・ 次のようにして、これらのダッシュボードでのプロジェクトの表示方法を管理します。
 - ・ [並び替え基準]フィールドを使用して、並び替え基準となる属性を選択し、矢印をクリックして並び替え順序  (昇順) または  (降順) を選択します。
 - ・ [プロジェクトのフィルタ]フィールドを使用して、いずれかのダッシュボードに表示されているプロジェクトにフィルタをかけます。
- ・ アイコン  を使用して、[監視中のプロジェクトを管理](#)するか、[プロジェクトを削除](#)します。

保存された検索のダッシュボードについて

保存済みの検索を使用して、重要なプロジェクトバージョン、コンポーネントバージョン、および脆弱性を表示します。


保存済みの検索ごとに、Black Duckはこの検索が最後に更新された日時を一覧表示します。

4. リスクの表示: Black Duck・ダッシュボードの表示

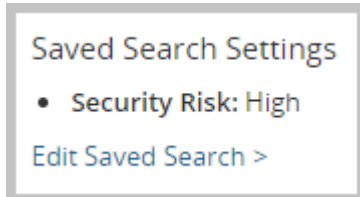
Results Summary

9 Components

Results updated at Feb 8, 2021 10:03 AM

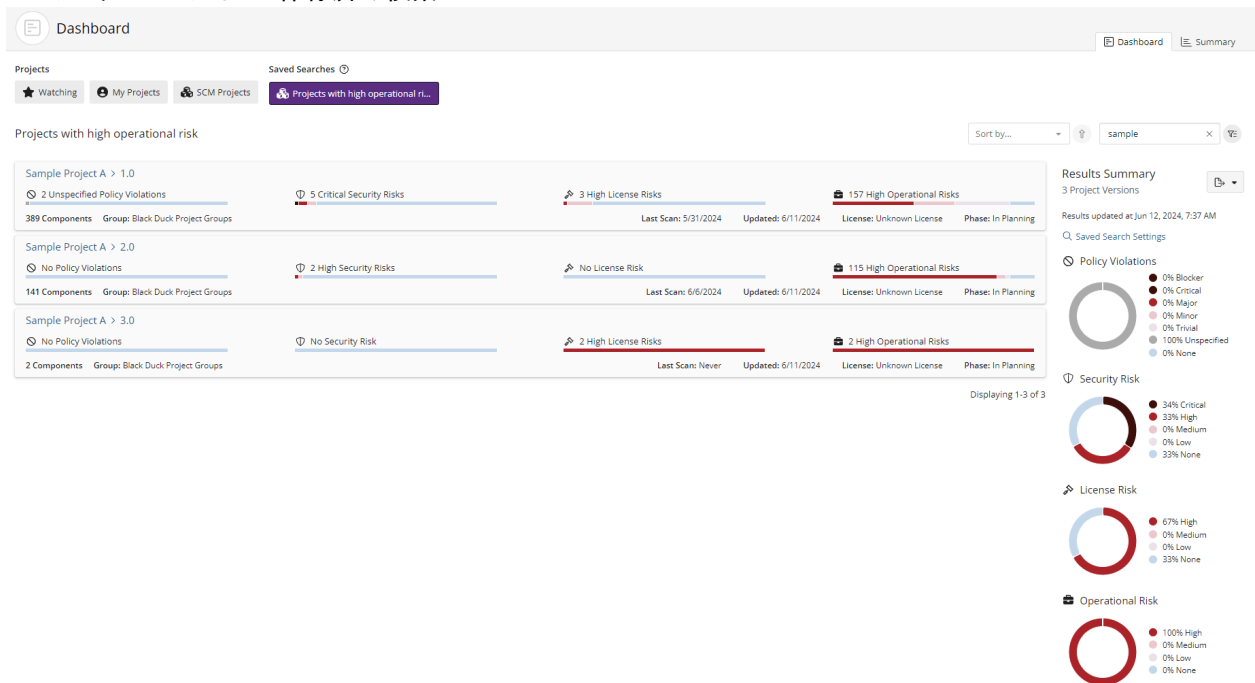
 Saved Search Settings

この保存済み検索のフィルタを表示するには、[保存済みの検索設定]を選択します。

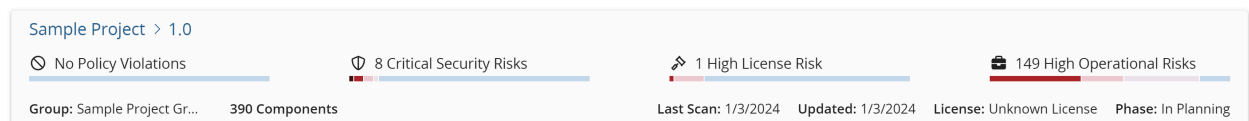



[保存済みの検索の編集]を選択して、保存済みの検索を表示する[検索]ページを開きます。このページを使用して、この変更された保存済み検索を編集および保存します。

プロジェクトバージョンの保存済み検索



プロジェクトバージョンごとに次の情報が表示されます。



-  が保存済み検索名の前に表示され、その名前がプロジェクトの保存済み検索内容であることを示します。
- 特定のプロジェクトバージョンのポリシー違反情報を表示するには、次の手順を実行します。

- ・ バーを使用して、このプロジェクトバージョンのポリシーの重大度レベルが最も高いコンポーネントの数を表示します。

たとえば、次の例は、重大度レベルが低いコンポーネントがあること、およびこのプロジェクトバージョンの最も高いポリシーの重大度レベルがブロッカーで、そのポリシーの重大度レベルとしてブロッカーを持つコンポーネントが5つあることを示しています。

5 Blocker Policy Violations

- 注: テキストには、このプロジェクトバージョンに影響を与えるすべてのポリシーの重大度レベルではなく、このプロジェクトバージョンのポリシーの重大度レベルが最も高いコンポーネントの数が記載されています。

- ・ バーにカーソルを合わせると、ポリシー違反のあるコンポーネントの数が、最も高いポリシーの重大度レベル別に表示されます。

Policy Violations

by Component

5	Blocker	1	Minor
1	Critical	0	Trivial
0	Major	0	Unspecified

* Each component is counted once by its highest severity risk

コンポーネントにポリシー違反がある場合、そのコンポーネントは1回だけカウントされ、その最も高いポリシーの重大度レベルだけが表示されます。

- ・ リスク情報を表示するには、次の手順を実行します。
- ・ リスクバーを使用すると、セキュリティ、ライセンス、または運用リスクが最も高いレベルのコンポーネントの数をすばやく表示できます。

セキュリティリスク:

1 High Vulnerability

ライセンスリスク:

2 High License Risks

運用リスク:

5 High Operational Risks

たとえば、次の例では、リスクが低いコンポーネントがある一方で、このプロジェクトバージョンの最も高いセキュリティリスクが高で、このプロジェクトバージョン内の1つのコンポーネントに、その最も高いリスクレベルとして高レベルのセキュリティリスクがあることを示しています。

1 High Vulnerability

- ・ バーにカーソルを合わせると、リスクカテゴリごとのコンポーネントの数が表示されます。

4. リスクの表示: Black Duck・ダッシュボードの表示


Security Risk

by Component



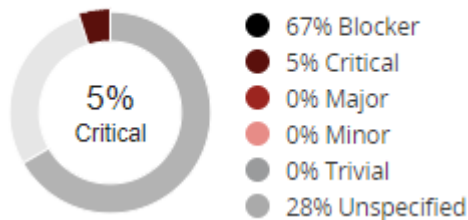
* Each component is counted once by its highest severity risk

この例では、最も高いリスクとして高リスクレベルを持つ1個のコンポーネント、最も高いリスクレベルとして中リスクを持つ10個のコンポーネント、最も高いリスクレベルとして低リスクを持つ6個のコンポーネントがあります。

 注: 各コンポーネントは1回だけカウントされ、最も高いリスクレベルで表示されます。

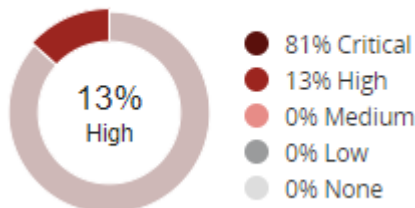
- ・ グラフを使用して、ポリシーの重大度とリスクレベル別に分類された、このダッシュボードのすべてのプロジェクトバージョンの概要情報を表示します。グラフには、レベルごとの割合が一覧表示されます。また、次の操作も可能です。
- ・ グラフにカーソルを合わせると、ポリシーの重大度レベルごとのポリシー違反があるプロジェクトバージョンの割合が表示されます。

Policy Violations





- ・ グラフにカーソルを合わせると、リスクレベルごとのこのダッシュボード内のプロジェクトバージョンの割合が表示されます。

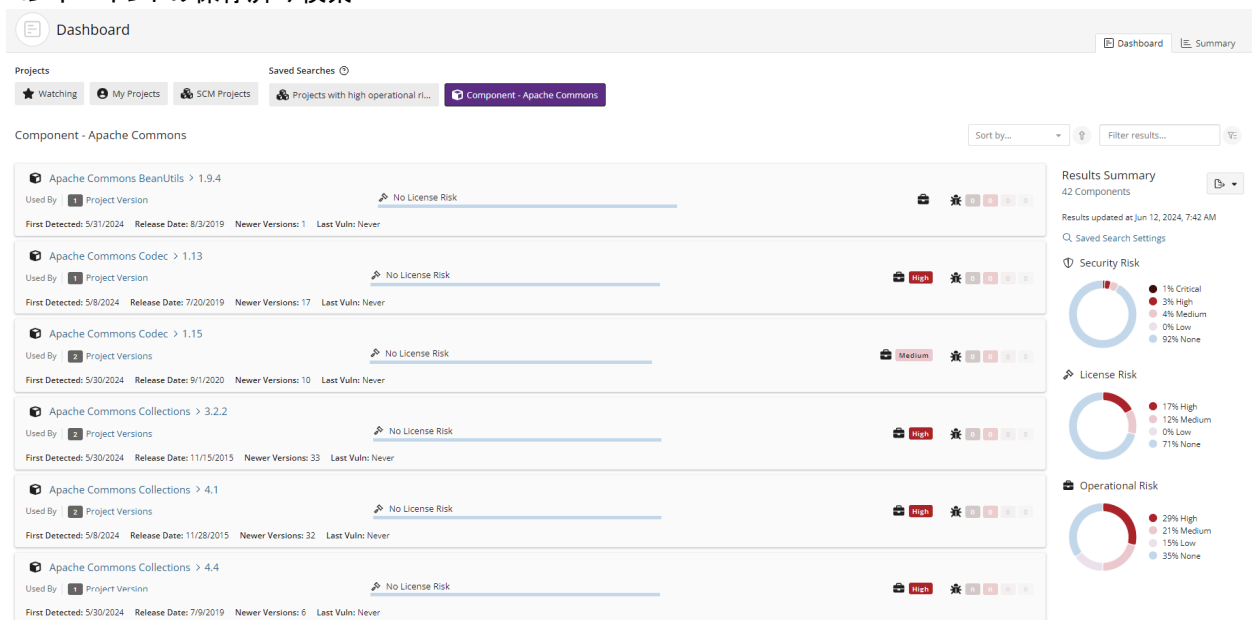
Security Risk



- ・ 凡例の値にカーソルを合わせると、グラフ内で値が強調表示されます。
- ・ プロジェクトバージョンごとに、ダッシュボードに次の情報も表示されます。
 - ・ このプロジェクトバージョンのコンポーネントの数。
 - ・ 最終スキャン日。
 - ・ 手動または新しいスキャンによってこのプロジェクトバージョンにマッピングされているスキャンが最後に実行された日時または、このプロジェクトバージョンの構成表が最後に更新された日時などの、このプロジェクトバージョンが最後に更新された日付。

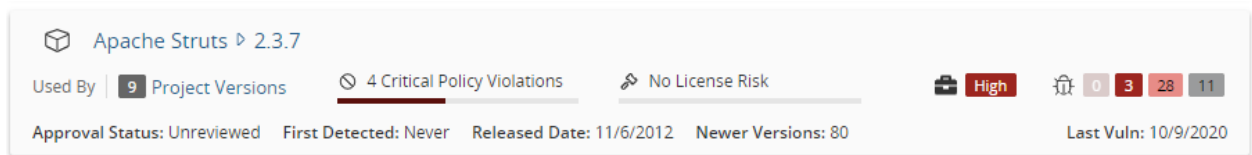
- ・ このプロジェクトバージョンのライセンス。
- ・ このプロジェクトバージョンのフェーズ。
- ・ このプロジェクトバージョンの配布。
- ・ プロジェクトまたはバージョン名を選択して、構成表を表示します。
- ・ 次のようにして、これらのダッシュボードでのプロジェクトの表示方法を管理します。
 - ・ [並び替え基準]フィールドを使用して、並び替え基準となる属性を選択し、矢印をクリックして並び替え順序  (昇順) または  (降順) を選択します。
 - ・ [プロジェクトにフィルタを適用]フィールドを使用して、ダッシュボードに表示されているプロジェクトをフィルタします。

コンポーネントの保存済み検索




The screenshot shows the Black Duck dashboard interface. At the top, there's a 'Dashboard' tab and a 'Summary' tab. Below that, a search filter 'Component - Apache Commons' is selected. The main area displays a list of components with details such as 'Used By', 'Project Version', 'First Detected', 'Release Date', 'Newer Versions', and 'Last Vuln'. Each component entry also shows a risk level (e.g., 'No License Risk', 'High', 'Medium'). On the right side, there are three donut charts representing 'Security Risk', 'License Risk', and 'Operational Risk' with corresponding legends.

コンポーネントごとに次の情報が表示されます。



This screenshot shows a detailed view of a component, 'Apache Struts 2.3.7'. It includes a 'Used By' section showing '9 Project Versions'. Below that, it lists '4 Critical Policy Violations' and 'No License Risk'. At the bottom, there's a summary bar with 'Approval Status: Unreviewed', 'First Detected: Never', 'Released Date: 11/6/2012', 'Newer Versions: 80', and 'Last Vuln: 10/9/2020'.

- ・  は、保存済み検索名の前に表示され、その名前がコンポーネントの保存済み検索であることを示します。
- ・ コンポーネント名/バージョンを選択すると、[\[コンポーネント名バージョン\]ページ](#)が表示されます。
- ・ このコンポーネントバージョンを使用しているプロジェクトバージョンの数が、[使用者]の横にある値で示されます。

Used By | **2** Project Versions

[プロジェクトバージョン]を選択して、[使用した場所]ダイアログボックスを開きます。

4. リスクの表示: Black Duck・ダッシュボードの表示

Used in ×

🔗 Apache Struts - 1.2.2 is being used in 1 Project Version

Project Name	Phase	License	Review Status	Security Risk
Sample Project - 4.0	In Planning	Apache License 2.0	Not Reviewed	0 3 6 0

Close

このダイアログボックスには、コンポーネントのこのバージョンを使用しているプロジェクトバージョンが表示されます。

カラム	説明
プロジェクト名	このコンポーネントバージョンを使用しているプロジェクトおよびバージョンの名前。プロジェクト名を選択すると、プロジェクトバージョンの[コンポーネント]タブが表示されます。
フェーズ	プロジェクトフェーズ 。
ライセンス	このコンポーネントバージョンのライセンス。
レビューステータス	このコンポーネントが、このプロジェクトバージョンでレビューされたかどうか。
セキュリティ上のリスク	各重大度レベルの脆弱性を左から右に示します。緊急、高、中、低。 0 3 28 11 値を選択すると、Black Duck KB[コンポーネント名バージョン]ページの[セキュリティ]タブが開き、このコンポーネントの当該バージョンに関連付けられた脆弱性が一覧表示されます。

- ・ バーを使用して、最も高いポリシーの重大度レベルを持つコンポーネントの数をすばやく表示します。

🔗 1 Critical Policy Violation

バーを選択すると、ポリシー違反のあるコンポーネントの数が、重大度レベル別に表示されます。

Policy Violations

by Component

0	Blocker	0	Minor
1	Critical	0	Trivial
0	Major	0	Unspecified

* Each component is counted once by its highest severity risk

- 🔗 注：コンポーネントは、このコンポーネントに影響を与えるすべてのポリシー重大度レベルではなく、最高のポリシー重大度レベルで1回のみカウントされます。

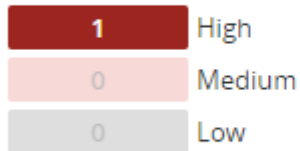
- ・ バーを使用すると、ライセンスリスクが最も高いコンポーネントの数をすばやく表示できます。

🔗 1 High License Risk

バーを選択すると、リスクカテゴリごとにコンポーネントの数が表示されます。

License Risk

by Component



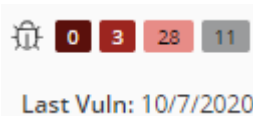
* Each component is counted once by its highest severity risk

- 当該コンポーネントバージョンの運用リスクの表示:



- このコンポーネントバージョンに関連付けられた脆弱性の数を、次の重大度別に左から右へと表示します: 緊急、高、中、低。

[最後の脆弱性]の日付は、このコンポーネントの脆弱性が、Black Duckで最後に更新された日付です (Black Duck KnowledgeBaseまたはユーザーによる更新)。



値を選択すると、Black Duck KB[コンポーネント名バージョン]ページの[セキュリティ]タブが開き、このコンポーネントの当該バージョンに関連付けられた脆弱性が一覧表示されます。

commons.apache.org
Apache Commons Collections » 3.2.1
java Versions: 62

Security Cryptography Copyrights Details Settings

Filter Vulnerabilities...

Identifier	Published	Overall Score
> BDSA BDSA-2015-0001 RCE	Apr 3, 2017	8.3 High
> BDSA BDSA-2015-0753 (CVE-2015-6420) RCE	May 3, 2019	8.3 High
> BDSA BDSA-2017-2285 (CVE-2017-15708) RCE	Dec 14, 2017	5.5 Medium
> BDSA BDSA-2015-0766 RCE	Aug 6, 2019	5.5 Medium

Displaying 1-4 of 4

- コンポーネントバージョンごとに、検索結果に次の情報も表示されます:
 - 承認済みステータス。ステータスは、このコンポーネントのバージョンがレビューされたかどうかを示します。
 - 最初に検出された日付。
 - このコンポーネントバージョンがリリースされた日付です。
 - 新しいバージョンの数。
 - コンポーネントの脆弱性が最後にBlack Duckで更新された日付 (Black Duck KnowledgeBaseから更新した場合や、ユーザーが関連する脆弱性を手動で変更した場合など)。
- 次のようにして、これらのダッシュボードでのコンポーネントの表示方法を管理します。
 - [並び替え基準]フィールドを使用して、並び替え基準となる属性を選択し、矢印をクリックして並び替え順序 (昇順) または (降順) を選択します。

4. リスクの表示: Black Duck・ダッシュボードの表示

- ・ フィルタフィールドを使用して、ダッシュボードに表示されるコンポーネントをフィルタします。

脆弱性の保存済み検索

Dashboard

Projects: Watching, My Projects, SCM Projects, Projects with high operational ri..., Component - Apache Commons, Vulnerability - Critical

Saved Searches

Vulnerability - Critical

BDSA	BDSA-2015-0068	Overall Risk	9.2	Critical	✓ Solution	No Workaround	Exploit	CWE-79
Used By	Project Versions							
First Detected:	Never	Published:	11/14/2017	Last Modified:	11/14/2017			

Results Summary: 24,562 Vulnerabilities. Results updated at: Jun 12, 2024, 7:42 AM. Saved Search Settings

BDSA	BDSA-2015-0080	Overall Risk	9.2	Critical	✓ Solution	No Workaround	Exploit	CWE-79
Used By	Project Versions							
First Detected:	Never	Published:	11/15/2017	Last Modified:	11/15/2017			

BDSA	BDSA-2010-0003	Overall Risk	8.1	Critical	No Solution	No Workaround	No Exploit	CWE-20, CWE-712
Used By	Project Versions							
First Detected:	Never	Published:	11/28/2017	Last Modified:	9/2/2018			

BDSA	BDSA-2011-0017	Overall Risk	9.2	Critical	✓ Solution	No Workaround	Exploit	CWE-80
Used By	Project Versions							
First Detected:	Never	Published:	5/9/2018	Last Modified:	5/17/2022			

脆弱性ごとに次の情報が表示されます。

BDSA BDSA-2020-1234 (CVE-2020-13430)

Used By: 0 Project Versions Overall Risk: 8.1 High ✓ Solution ✓ Workaround No Exploit CWE-79

First Detected: Never Published: 5/27/2020 Last Modified: 7/27/2020

- ・ 脆弱性IDを選択すると、追加のスコア値など、脆弱性に関する詳細情報が表示されます。CVE番号を選択してNational Vulnerability Database (NVD) 情報や、BDSA番号を選択してBlack Duck Security Advisory (BDSA) 情報を表示できます。
- ・ [使用者]の横にこの脆弱性の影響を受けたプロジェクトバージョンの数を表示します。

Used By | 2 Project Versions

[プロジェクトバージョン]を選択して、この脆弱性の影響を受けるプロジェクトのバージョンを一覧表示する、脆弱性の[影響を受けるプロジェクト]タブを開きます。

Black Duck Security Advisory

Apache HTTPClient Vulnerable to Man-In-The-Middle (MITM) Attack via SSL Hostname Verification Bypass

BDSA BDSA-2014-0126 | CVE-2014-3577 | Published May 30, 2019 | Updated Feb 7, 2020

Overview Affected Projects Technical CVE References Settings



Remediate Filter projects...

Project	Component	Component Origin	Status	Target date	Actual date
cloudfoundry-identity-parent 3.6.3	Apache HttpClient 3.1	maven/commons-httpclient:commons-httpclient:3.1	New	Never	Never
cloudfoundry-identity-parent 3.6.3	Apache HttpClient 4.3.3	maven/org.apache.httpcomponents:httpclient:4.3.3	New	Never	Never
cloudfoundry-identity-parent 3.6.3	Apache HttpComponents Core 4.3.2	maven/org.apache.httpcomponents:httpcore:4.3.2	New	Never	Never
cloudfoundry-identity-parent 3.6.3	Apache HttpComponents Core 4.3.3	maven/org.apache.httpcomponents:httpcore:4.3.3	New	Never	Never


Displaying 1-4 of 4

- ・ 全体的なリスクスコアを表示します。検索結果には、BDSA脆弱性の一時スコア、またはNVD脆弱性のベーススコアと関連するリスクレベルが表示されます。表示されるスコアとリスクレベルは、選択したセキュリティランキングによって異なることに注意してください。

スコアを選択すると、BDSAの場合は一時スコア、ベーススコア、可能性のスコア、および影響スコア、NVDの場合はベーススコア、可能性のスコア、および影響スコアなど、個々のスコアが表示されます。

- ・ ソリューション、回避策、または攻撃が利用可能かどうかを表示します。
 - ・  は、この脆弱性に対して利用可能なソリューションや回避策が存在することを示します。
 - ・  は、この脆弱性に対する攻撃があることを示します。
- ・ 脆弱性ごとに、検索結果に次の情報も表示されます。
 - ・ 最初の検出。
 - ・ 公開日。
 - ・ 最終変更日。
 - ・ このセキュリティ脆弱性の共通脆弱性タイプ一覧 (CVE) 番号。

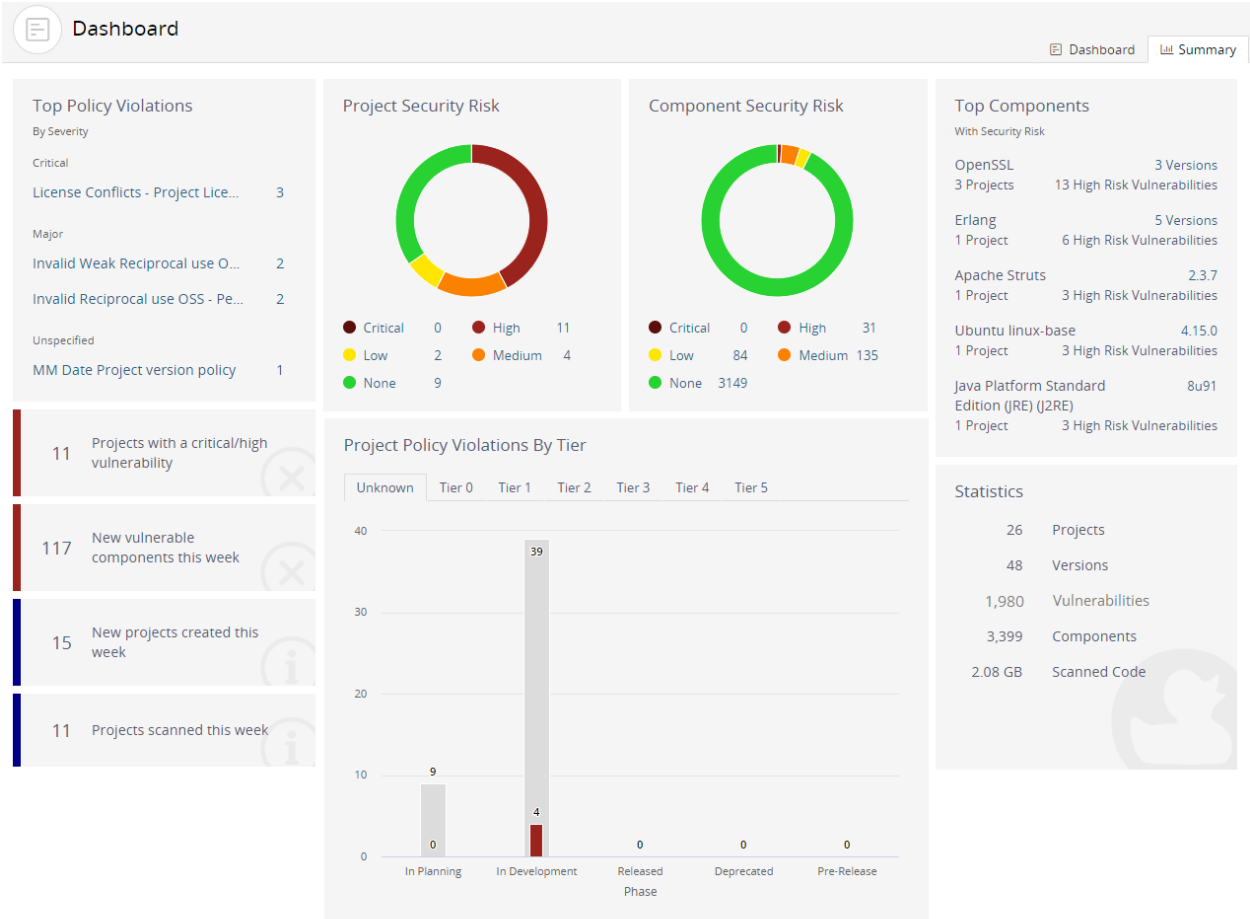
CSVへのエクスポート

ダッシュボードをCSVにエクスポートして、個々の行を表形式のデータに変換できます。これを実行するには、 ボタンをクリックし、[CSV]を選択します。

プロジェクトの健全性の表示

プロジェクト全体の健全性を確認し、問題のある領域を特定するには、[概要]タブを使用します。ページには、ビジネスに不可欠な情報を提供するウィジェットが含まれています。この情報を使用して、注意する必要がある領域をすばやく評価することができます。

4. リスクの表示: Black Duck・プロジェクトの健全性の表示

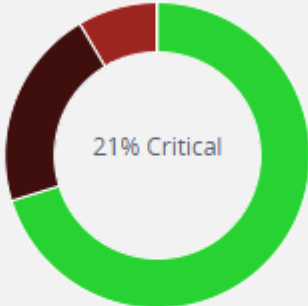
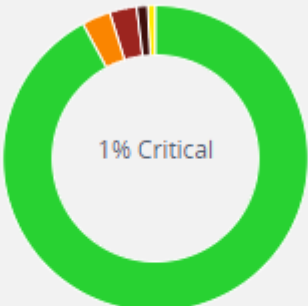


注: [概要]タブには、表示する権限があるプロジェクトの情報だけが表示されます。

次の表は、[概要]タブに表示される各ウィジェットについての説明と追加情報を表示する方法(利用可能な場合)を示しています。表示されるセキュリティリスク値は、[選択したセキュリティリスク計算](#)に応じて、CVSS v2またはCVSS v3.xスコアを使用していることに注意してください。デフォルトでは、CVSS v3.xスコアが表示されます。CVSS v2を選択した場合、グラフの緊急リスクカテゴリには値0が表示されることに注意してください。


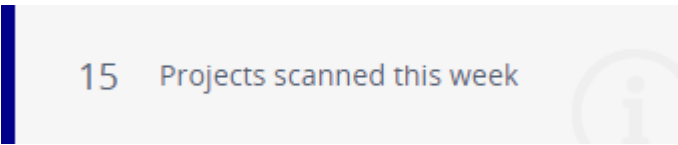
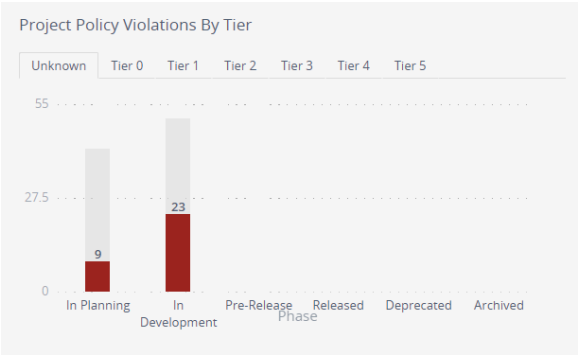
ウィジェット		説明	その他の情報
Top Policy Violations		BOM[上位ポリシー違反]ウィジェットには、表示する権限がある全プロジェクトで発生した上位のポリシー違反が最大5個表示されます。	ポリシールールを選択すると、[マイプロジェクト]タブが表示され、そのポリシールールに違反しているプロジェクトがバージョンとともに示されます。
By Severity			
Major			
High Severity	10	ポリシールールは重大度レベル別に、ポリシー違反数の多いものから降順に一覧表示されます。ポリシールールに重大度レベルが割り当てられていない場合は、ウィジェットによって上位5個のポリシー違反が違反数の多いものから降順に表示されます。	
Medium Severity	10		
Major Rule	10		
Vulnerability Count	10		
Sample Rule	10		
		<ul style="list-style-type: none"> ・ ポリシー管理モジュールがない場合、このウィジェットはページに表示されません。 ・ ポリシー管理モジュールがある一方で、ポリシールールが設定されていない場合、またはポリシー違反がない場合は、メッセージが表示されます。 	

4. リスクの表示: Black Duck・プロジェクトの健全性の表示

ウィジェット	説明	その他の情報												
<div><h3>Project Security Risk</h3><table><tr><td>Critical</td><td>10</td><td>High</td><td>4</td></tr><tr><td>Low</td><td>0</td><td>Medium</td><td>0</td></tr><tr><td>None</td><td>33</td><td></td><td></td></tr></table></div>	Critical	10	High	4	Low	0	Medium	0	None	33			<p>[プロジェクトのセキュリティ上のリスク]ウィジェットには、各レベルのセキュリティ上のリスクに対して表示する権限があるプロジェクトの数が表示されます。</p> <p>このウィジェットでは、そのプロジェクトにセキュリティ上の影響を及ぼすすべてのリスクレベルではなく、最も高いリスクレベルのみがカウントされることに注意してください。たとえば、セキュリティ上のリスクが中と低であるプロジェクトの場合、中のセキュリティリスクを持つプロジェクトとしてカウントされ、低のセキュリティリスクを持つプロジェクトには含まれません。</p>	<p>そのレベルのセキュリティ上のリスクを持つプロジェクトの数を表示するには、グラフをポイントします。</p>
Critical	10	High	4											
Low	0	Medium	0											
None	33													
<div><h3>Component Security Risk</h3><table><tr><td>Critical</td><td>29</td><td>High</td><td>73</td></tr><tr><td>Low</td><td>21</td><td>Medium</td><td>77</td></tr><tr><td>None</td><td>2331</td><td></td><td></td></tr></table></div>	Critical	29	High	73	Low	21	Medium	77	None	2331			<p>[コンポーネントのセキュリティ上のリスク]ウィジェットには、各レベルのセキュリティ上のリスクに対して表示する権限があるプロジェクト内のコンポーネントの数が表示されます。</p> <p>このウィジェットでは、コンポーネントの最も高いセキュリティ上のリスクのみがカウントされることに注意してください。たとえば、セキュリティ上のリスクが中と低であるコンポーネントは、中のセキュリティリスクを持つ1つのコンポーネントとしてカウントされます。</p>	<p>そのレベルのセキュリティ上のリスクを持つコンポーネントの数を表示するには、グラフをポイントします。</p>
Critical	29	High	73											
Low	21	Medium	77											
None	2331													

ウィジェット	説明	その他の情報																				
<div><div>Top Components</div><div>With Security Risk</div><table><tr><td>GNU C Library</td><td>2.23</td></tr><tr><td>1 Project</td><td>5 Critical Risk Vulnerabilities</td></tr><tr><td>Apache Struts</td><td>2 Versions</td></tr><tr><td>2 Projects</td><td>3 Critical Risk Vulnerabilities</td></tr><tr><td>Apache Camel</td><td>2.15.1</td></tr><tr><td>1 Project</td><td>4 Critical Risk Vulnerabilities</td></tr><tr><td>GnuTLS</td><td>3.5.16</td></tr><tr><td>1 Project</td><td>1 High Risk Vulnerabilities</td></tr><tr><td>zlib</td><td>1.1.3</td></tr><tr><td>1 Project</td><td>1 High Risk Vulnerabilities</td></tr></table></div>	GNU C Library	2.23	1 Project	5 Critical Risk Vulnerabilities	Apache Struts	2 Versions	2 Projects	3 Critical Risk Vulnerabilities	Apache Camel	2.15.1	1 Project	4 Critical Risk Vulnerabilities	GnuTLS	3.5.16	1 Project	1 High Risk Vulnerabilities	zlib	1.1.3	1 Project	1 High Risk Vulnerabilities	<p>[セキュリティ上のリスクがある上位コンポーネント]ウィジェットには、表示する権限があるプロジェクトで使用されているコンポーネントのうち、リスクの数が多いコンポーネントが最大5個表示されます。各コンポーネントについて、次の情報が表示されます。</p> <ul style="list-style-type: none">プロジェクトで使用されているコンポーネントの名前とバージョンの数。1つのバージョンのみを使用している場合は、そのバージョンがここに表示されます。このコンポーネントを含むプロジェクトの数。このコンポーネントにあるセキュリティ上のリスクの数。最も高いセキュリティ上のリスクも表示されます。 <p>コンポーネントはセキュリティ上のリスク別に表示され、最も高いリスクを持つコンポーネントが最初に表示されます。</p>	<p>特定のバージョンまたは複数のバージョンを選択して、[コンポーネントのバージョンの詳細]ページを表示します。</p>
GNU C Library	2.23																					
1 Project	5 Critical Risk Vulnerabilities																					
Apache Struts	2 Versions																					
2 Projects	3 Critical Risk Vulnerabilities																					
Apache Camel	2.15.1																					
1 Project	4 Critical Risk Vulnerabilities																					
GnuTLS	3.5.16																					
1 Project	1 High Risk Vulnerabilities																					
zlib	1.1.3																					
1 Project	1 High Risk Vulnerabilities																					
<div><div>30</div><div>Projects with a critical/high vulnerability</div></div>	<p>[緊急/高の脆弱性を含むプロジェクト]ウィジェットには、セキュリティ上のリスクが緊急または高のコンポーネントを含むバージョンを持つプロジェクトの数が表示されます。</p>	<p>N/A。</p>																				
<div><div>80</div><div>New vulnerable components this week</div></div>	<p>[今週検出された脆弱性を含むコンポーネント]ウィジェットには、今日を含む過去7日間にBlack Duck KBが脆弱性をマッピングしたコンポーネントの数が表示されます。</p>	<p>N/A。</p>																				

4. リスクの表示: Black Duck・プロジェクトの健全性の表示

ウィジェット	説明	その他の情報
	[今週作成された新しいプロジェクト]ウィジェットには、今日を含む過去7日間に作成された、表示権限を持つプロジェクトの数が表示されます。	N/A。
	[今週スキャンされたプロジェクト]ウィジェットには、今日を含む過去7日間にスキャンされたプロジェクトの数が表示されます。	N/A。
	<p>[プロジェクトポリシー違反(階層別)]ウィジェットには、ポリシー違反があったプロジェクトの合計数がフェーズ別に、階層でグループ化されて表示されます。</p> <ul style="list-style-type: none">プロジェクトで階層を使用していない場合、プロジェクトは「不明」という1個のカテゴリにグループ化されます。ポリシー管理モジュールがない場合、このウィジェットにはプロジェクトが階層別に表示されます。	各階層でバーをポイントすると、そのフェーズのプロジェクトの数、およびそのフェーズの、ポリシー違反があるプロジェクトの数が表示されます。

ウィジェット	説明	その他の情報
	<p>[統計情報]ウィジェットに N/A。は、次の情報が表示されます。</p> <ul style="list-style-type: none"> ・ [プロジェクト]には、プロジェクトの数が表示されます。 ・ [バージョン]には、プロジェクトのプロジェクトバージョン数が表示されます。 ・ [脆弱性]には、プロジェクトに含まれる脆弱性の数が表示されます。 ・ [コンポーネント]には、無視されたコンポーネントを含むプロジェクトで使用されているコンポーネントの数が表示されます。 ・ [スキャンしたコード]には、すべてのスキャンでスキャンされたギガバイト数が表示されます。 	

セキュリティ上のリスクについて

Black Duck は、セキュリティチームと開発チームがアプリケーション全体のセキュリティ上のリスクを特定できるようにします。

オープンソースソフトウェアに脆弱性をマッピングすることで、Black Duckでは、プロジェクトのセキュリティ上のリスクに関する大まかな概要情報と、セキュリティ脆弱性の調査および修正に使用できるセキュリティ脆弱性に関する詳細情報が得られます。

脆弱性は、米国国立標準技術研究所 (NIST) によって管理されている National Vulnerability Database (NVD) の共通脆弱性識別子番号 (CVE) や、Black Duck Security Advisories のライセンスを所有している場合は BDSA 番号によって、オープンソースコンポーネントにリンクされます。Black Duckでは、レポートとUIに数字と一緒に表示される点に注意してください。これは、異なるソースからの同じ脆弱性を表しているためです。

セキュリティ上のリスクのレベル

NVDとBDSAは、共通脆弱性評価システム (CVSS) を使用して、脆弱性の重大度を示す数値スコアを表示します。数値スコアはリスクレベルに変換され、セキュリティ脆弱性の評価と優先順位付けに役立ちます。

Black Duck には、CVSS v2またはCVSS v3.xスコアを表示するオプションがあります。デフォルトでは、Black DuckはCVSS v3.xスコアを表示します。

- ・ CVSS v2スコアの値は次のとおりです。
 - ・ 低リスク: 0.0~3.9

4. リスクの表示: Black Duck・セキュリティ上のリスクについて

- ・ 中リスク: 4.0~6.9
- ・ 高リスク: 7.0~10.0

Black Duckでは、0.0のスコアを持つ脆弱性をリスクなしとして示します。

CVSS v2には緊急リスクカテゴリはありませんが、Black Duck UIのセキュリティグラフには緊急リスクカテゴリが表示されます。CVSS v2については、このカテゴリに0の値が表示されます。

- ・ CVSS v3.xスコアの値は次のとおりです。

- ・ なし: 0.0
- ・ 低リスク: 0.1~3.9
- ・ 中リスク: 4.0~6.9
- ・ 高リスク: 7.0~8.9
- ・ 緊急リスク: 9.0~10.0


CVSS v3.xに表示されるスコアは、v3.0またはv3.1のスコアになる可能性があることに注意してください。

推定セキュリティリスク

この推定リスク統計は、セキュリティ脆弱性の重大度カテゴリ別にソートされたコンポーネントの全バージョンを参照し、コンポーネントバージョンごとに各重大度カテゴリの最大脆弱性数を計算することで算出されます。各重大度カテゴリの最大脆弱性数は、セキュリティリスクの構成表の[重大度カテゴリ別の推定セキュリティリスク]に表示されます。重大度が最高値になっているカテゴリ数は、複数の異なるコンポーネントバージョンを参照している可能性があります。以下に例を示します。

- ・ バージョン1.1では、重大2、高3、中15、低4になっています
- ・ バージョン1.2では、重大2、高4、中12、低1になっています
- ・ この例で、コンポーネントのバージョンが不明の場合、重大度カテゴリ別の推定セキュリティリスクは、構成表上で重大2、高4、中15、低4になります。

推定リスクではなく、正確なリスクを表示するには、アプリケーションで使用されている正確なバージョンを選択する必要があります。この推定リスク情報は、どのコンポーネントを最初にレビューすべきかの優先順位付けに役立ちます。企業のセキュリティポリシーに基づいて優先順位をさらに明確にし、コンポーネントの最初の選別が実行できるように、推定リスク情報とともにBDポリシー管理を使用することをお勧めします。

 注: 表示される情報は統計データの推定のみです。結果的に、推定セキュリティリスクにはCVEデータは含まれません。

推奨されるワークフロー

Black Duckでセキュリティ上のリスクを管理するには

1. セキュリティチームの協力を受けて、セキュリティリスクポリシーを決定します。
2. 必要に応じて、システム管理者の役割を持つユーザーは、[デフォルトのセキュリティランキングを定義](#)できます。

セキュリティランキングにより、脆弱性がレポートでどのように表示されるかも定義される点に注意してください。利用可能なデータに応じて、脆弱性は次のいずれかの形で表示されます。BDSA(NVD)またはNVD(BDSA)。たとえば、セキュリティランキングがNVD2、BDSA2、BDSA3、NVD3の場合、次のようになります。

- ・ 脆弱性Aには、NVD3のみのデータがあります。この脆弱性は、NVD-1234-5678としてレポートに記載されます。
- ・ 脆弱性Bには、NVD3およびBDSA3のデータがあります。レポートには、BDSA(NVD)として記載されます。
- ・ 脆弱性Cにはすべてのデータがあります。レポートにはNVD(BDSA)と記載されます。

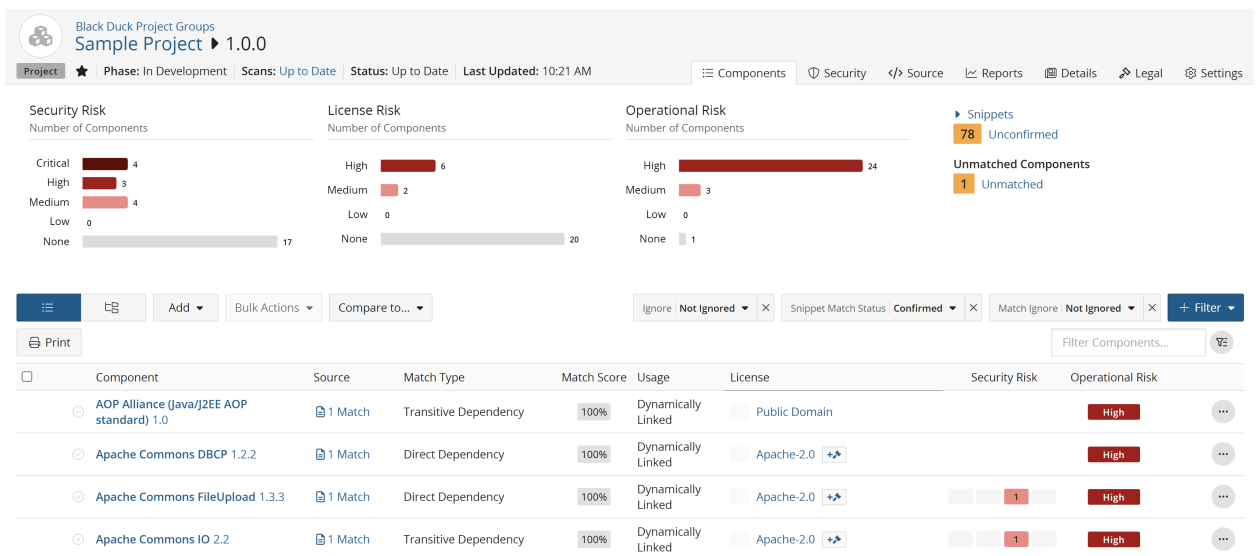
3. コンポーネントがセキュリティポリシーに準拠していない場合に違反をトリガーする[ポリシーを作成します](#)。
4. 必要に応じて、次の手順を実行します。
 - ・ プロジェクト全体の健全性を確認し、問題のある領域を特定するには、[概要ダッシュボード](#)を使用します。このページを使用して、注目する必要のある領域を迅速に評価します。
 - ・ リスクに関する概要を確認するには、次の[ダッシュボード]ページを使用します。
 - ・ [\[ウォッチ\]または\[マイプロジェクト\]ダッシュボード](#)を使用して、すべてのプロジェクトにわたるセキュリティ上のリスクを表示します。
 - ・ [保存済み検索を作成](#)して、[ダッシュボード]ページに表示される情報をカスタマイズし、関心のあるプロジェクト、コンポーネント、および脆弱性を表示します。
 - ・ プロジェクトバージョンレベルの情報を表示するには、次のページを使用します。
 - ・ [プロジェクトバージョンページ/\[コンポーネント\]タブ](#)は、プロジェクトバージョンの構成表とも呼ばれます。セキュリティ上のリスクがある、プロジェクトバージョンに固有のコンポーネントを表示します。
 - ・ [プロジェクトバージョンページ/\[セキュリティ\]タブ](#)は、プロジェクトバージョンで使用されているコンポーネントに関連付けられているセキュリティの脆弱性を、重大度ごとに表示します。
5. 脆弱性およびポリシー違反を調査します。セキュリティ脆弱性の詳細については、以下を参照してください。
 - ・ [CVEページ](#)
 - ・ [BDSAページ](#) — Black Duck Security Advisories (BDSA) のライセンスを所有している場合
6. 脆弱性の重大度を確認した後、適切な[役割](#)を持つユーザーは、セキュリティ脆弱性の[修正ステータス](#)を変更できます。
7. 新しいセキュリティ脆弱性の[通知を監視します](#)。
1つ以上のプロジェクトに含まれるコンポーネントでセキュリティ脆弱性が公開または更新された場合、通知アラートが送られてきます。

5. 構成表の表示

コンポーネントスキャンをプロジェクトバージョンにマッピングすると、結果によってプロジェクトバージョンの構成表が自動的に作成されます。

プロジェクトバージョンの構成表を表示するには、次の手順を実行します。

1. Black Duckにログインします。
2. [ウォッチ]または[マイプロジェクト]ダッシュボードを使用して、プロジェクト名を選択します。[プロジェクト名]ページが表示されます。
3. 表示するプロジェクトのバージョン名を選択します。
[コンポーネント]タブに構成表が表示されます。



デフォルトでは、見つかったすべてのコンポーネントが同じレベルにリストされているコンポーネントの「フラット」ビューが構成表に表示されます。

構成表でコンポーネントとコンポーネントバージョンを調整する

コンポーネントスキャンをプロジェクトバージョンにマッピングすると、スキャン結果によってプロジェクトバージョンの構成表が自動的に作成されます。コンポーネントスキャンでは、Black Duck KB内のコンポーネントと比較することにより、ほとんどのアーカイブファイルからのオープンソースコンポーネントとコンポーネントバージョンが自動的に検出されます。ただし、Black Duck KBにないバージョンや修正バージョンを使用している場合があります。構成表内のコンポーネントのコンポーネントとバージョンを調整することができます。

- ・ コンポーネント/バージョンがBlack Duck KBで利用可能である場合、適切な役割を持つユーザーがコンポーネントまたはコンポーネントのバージョンを調整することができます。次に説明します。
- ・ コンポーネントのコンポーネントバージョンがBlack Duck KBで使用できない場合、コンポーネントマネージャの役割を持つユーザーがカスタムバージョンを作成し、構成表に追加することができます。

構成表内でコンポーネントの代替コンポーネントマッチとバージョンマッチを選択するには、次の手順を実行します。

1. Black Duckにログインします。

5. 構成表の表示・構成表でコンポーネントとコンポーネントバージョンを調整する

- [ウォッチ]または[マイプロジェクト]ダッシュボードを使用して、プロジェクト名を選択します。[プロジェクト名]ページが表示されます。
- バージョン名を選択し、[コンポーネント]タブを開いて構成表を表示します。

Component	Source	Match Type	Match Score	Usage	License	Security Risk	Operational Risk
AOP Alliance (Java/J2EE AOP standard) 1.0	1 Match	Transitive Dependency	100%	Dynamically Linked	Public Domain	High	High
Apache Commons DBCP 1.2.2	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	High	High
Apache Commons FileUpload 1.3.3	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	High	High
Apache Commons IO 2.2	1 Match	Transitive Dependency	100%	Dynamically Linked	Apache-2.0	High	High

- 構成表のコンポーネントリストビューで をクリックして[編集]を選択し、[コンポーネントの編集]ダイアログボックスを開きます。
- [コンポーネント]フィールドにOSSコンポーネントの名前を入力し、代替マッチを選択します。
- [バージョン]一覧からコンポーネントのバージョンを選択します。このリストには、Black Duck KBで利用可能なコンポーネントのすべてのバージョンがあります。
- 必要に応じて、この調整の目的を入力し、および/または[変更]チェックボックスをオンにして、必要に応じて、フィールドにこの変更に関する情報を入力します。
- [保存]をクリックします。

構成表エントリのコンポーネントおよびバージョンが更新されます。情報インジケータ()が表の行に表示され、コンポーネントスキャンで自動的に検出されたコンポーネントおよび/またはバージョンが変更されたことを示します。

Component	Source	Match Type	Match Score	Usage	License	Security Risk	Operational Risk
AOP Alliance (Java/J2EE AOP standard) 1.0	1 Match	Transitive Dependency	100%	Dynamically Linked	Public Domain	High	High
Apache Commons DBCP 1.2.2	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	High	High
Apache Commons FileUpload 1.3.3	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	High	High
Apache Commons IO 2.2	1 Match	Transitive Dependency	100%	Dynamically Linked	Apache-2.0	High	High