Synopsys Black Duck for Red Hat OpenShift

Lab Guide

Introduction:

This workshop showcases how to scan containers deployed on Red Hat® OpenShift® with Synopsys' Software Composition Analysis tool, Black Duck in production workloads. Black Duck provides a solution for managing security, license compliance and code quality risks that come from the use of open source and third-party code in applications and containers.

This Lab will cover:

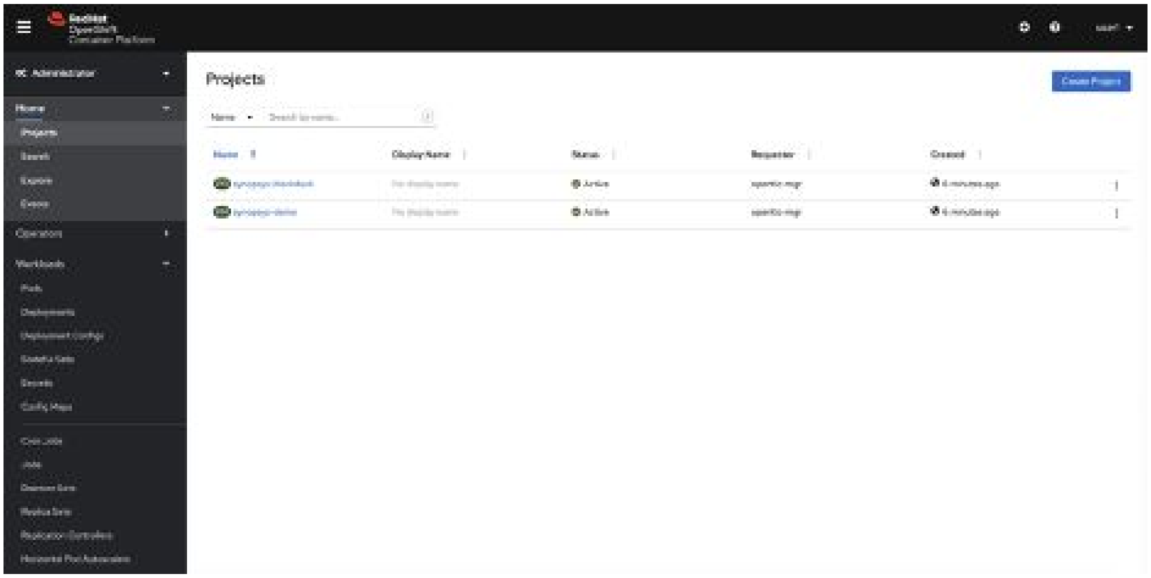
1. Black Duck for OpenShift setup.
2. Project & 'pod running' verification.
3. Demo Application details.
4. How Black Duck Scanning works.
5. An overview of Black Duck Scanning results.
6. Scanning a custom container.
7. Working with Scan Results
    a. Removing and Reviewing Components
    b. Adding a Component, making comments, andcomparing BOMs
    c. Updating Remediation Status and Reviewing Snippets
    d. Selecting and Editing Licenses

Table of Contents

Task 1: Black Duck for OpenShift Setup

A lab instructor is required to run this as a workshop. After the instructor deploys the RHPDS instance, it will create a Red Hat OpenShift cluster with two projects created, and Black Duck for OpenShift deployed. The lab instructor will provide participants access to the cluster. To view what was created by the instructor follow these steps:

1. Click on Home (Left navigation panel) > Projects > synopsys-blackduck: to view the Black Duck connector project. To see the running pods navigate to the workloads section on the top.
2. Similarly, to view the scanning demo project, repeat the above process by selecting synopsys-demo.



Projects

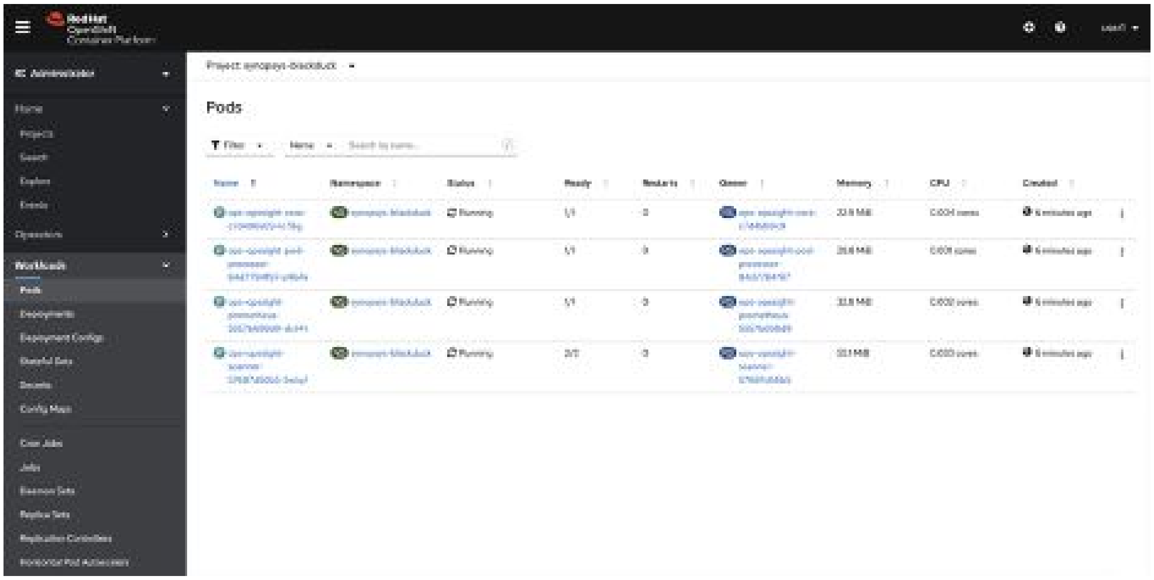
Name	Display Name	Status	Requester	Created
synopsys-blackduck	No display name	Active	opentlc-mgr	6 minutes ago
synopsys-demo	No display name	Active	opentlc-mgr	6 minutes ago

End of Task 1

Task 2: Project & Pod Verification

The two created projects are as follows - synopsys-blackduck & synopsys-demo. The synopsys-blackduck project contains 4 pods:

1. opssight-core: brains of the operation, a pod which communicates with Black Duck instance hosted at https://redhathub.blackducksoftware.com/, it maintains a list of all the scanned images and communicates with the rest of the pods.
2. opssight-pod-processor: a pod which connects with other pods and retrieves the underlying base image that runs inside the containers in OpenShift.
3. opssight-scanner: a pod which downloads the image from whichever image registry it's supposed to.
4. opssight-prometheus: a pod which monitors opssight's consumption of resources.



Project: synopsys-blackduck

Pods

Name	Namespace	Status	Ready	Restarts	Owner	Memory	CPU	Created
[illegible]	synopsys-blackduck	Running	1/1	0	[illegible]	32.9 MiB	0.004 cores	6 minutes ago
[illegible]	synopsys-blackduck	Running	1/1	0	[illegible]	28.8 MiB	0.001 cores	6 minutes ago
[illegible]	synopsys-blackduck	Running	1/1	0	[illegible]	32.8 MiB	0.002 cores	6 minutes ago
[illegible]	synopsys-blackduck	Running	2/2	0	[illegible]	32.1 MiB	0.003 cores	6 minutes ago

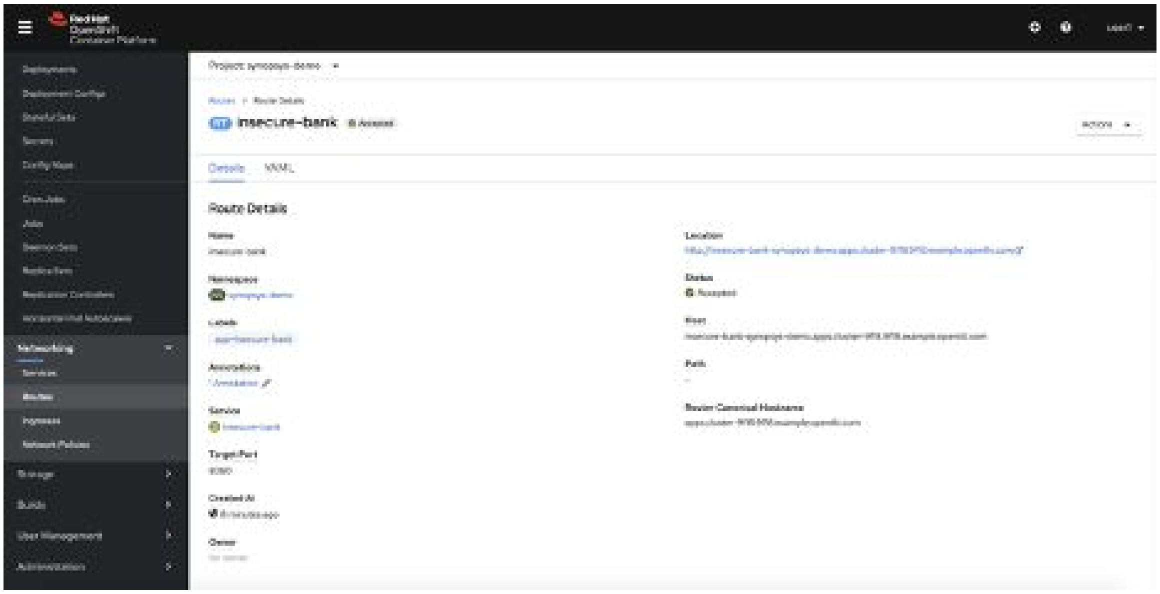
This also includes a configmap for configuring a lot of options e.g. when to look for scans to run, only run scans for specific project, etc. There are also two opaque secrets created which helps the integration with any images that may come from a private registry. All of these options are preconfigured, so workshop users do not need to worry about them.

End of Task 2

Task 3: Demo Application Details

The demo application is an insecure bank application under project the synopsys-demo where users can make dummy bank transactions. The underlying image that's running this application is located at https://quay.io/repository/opssighttestorg/insecure-bank. This underlying image will be scanned by Black Duck.

1. To see the running pod of this project navigate to Workloads (left side panel) > Pods > insecure-bank-deployment-{generated-alpha-numeric-code} pod Make sure the project (on the top) is set to synopsys-demo before doing this.
2. Next let's look at a ClusterIP service generated for this app, navigate to Networking (left side panel) > services > insecure-bank, this should validate connection to insecure-bank pod after clicking the pods column on the top.
3. This app is also externally exposed using routes to be interactable, navigate to Networking > Routes > insecure-bank. The external IP should be visible under the location column. The username and password for testing is "john@example.com" and "test" respectively.



Project: synopsys-demo

Routes / Route Details

RT insecure-bank Accepted

Route Details

Name
insecure-bank

Namespace
NS synopsys-demo

Labels
app=insecure-bank

Annotations
1 Annotation

Service
S insecure-bank

Target Port
8080

Created At
[illegible] minutes ago

Owner
No owner

Location
[illegible]

Status
Accepted

Host
[illegible]

Path
-

Router Canonical Hostname
[illegible]

End of Task 3

Task 4: How Black Duck Scanning Works

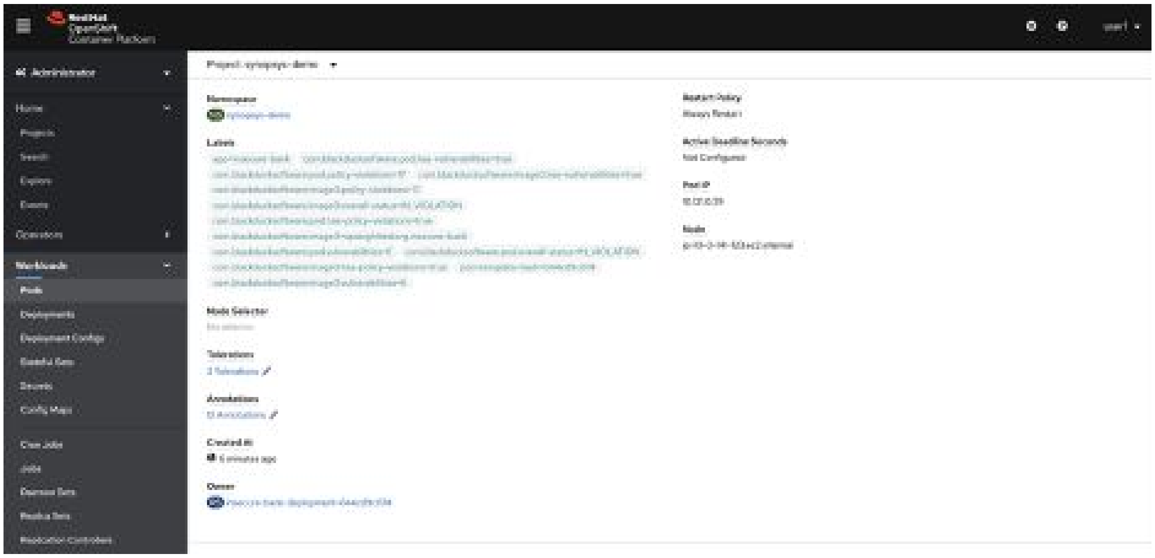
Note: For purposes of this workshop, the Black Duck scanner is only configured to scan anything deployed in the synopsys-demo workspace.

The scanning process works as place as follows:

1. The insecure-bank application is deployed in the cluster.
2. The "connector-pod-processor" pod is informed that there's a new pod in the cluster and it sends underlying image information to the "connector-core" pod.
3. The "connector-core" initiates the scanning process by delivering the information to "connector-scanner" pod while taking a note of the activity & progress.
4. The "connector-scanner" pod then initiates a Black Duck signature scan. There are two containers in the pod, the first (image-getter) container will download and temporarily store the image in memory. The second (scanner) container to invoke the Black Duck scanner.
5. If the image has not been previously scanned, then the scanner will create the project with version. If the image is present with a different version, then the scanner will only create a new version under the project. If both image and the version are present in Black Duck, then image is not sent for scanning and the results are re-used.
6. After scanning is finished, Black Duck populates the Bill of Materials (BOM) in Black Duck.
7. The "connector-core" pod retrieves the information from Black Duck and sends it back to the "connector-pod-processor" pod while taking a note of the scan completion and results received.
8. The "connector-pod-processor" pod will finally annotate the relevant pod with policy violation and vulnerability count.

More details here

To view these labels in the OpenShift UI navigate to Workloads (left side panel) > Pods > click on insecure-bank-deployment-{generated-alpha-numeric-code} pod (make sure the project is set to synopsys-demo now) and scroll down to the labels section.



Namespace
NS synopsys-demo

Labels
app=insecure-bank com.blackducksoftware.pod.has-vulnerabilities=true
com.blackducksoftware.pod.policy-violations=[illegible] com.blackducksoftware.image0.has-vulnerabilities=true
com.blackducksoftware.image0.policy-violations=[illegible]
com.blackducksoftware.image0.overall-status=IN_VIOLATION
com.blackducksoftware.pod.has-policy-violations=true
com.blackducksoftware.image0-repository=[illegible]insecure-bank
com.blackducksoftware.pod.vulnerabilities=[illegible] com.blackducksoftware.pod.overall-status=IN_VIOLATION
com.blackducksoftware.image0.has-policy-violations=true pod-template-hash=[illegible]
com.blackducksoftware.image0.vulnerabilities=[illegible]

Node Selector
No selector

Tolerations
2 Tolerations

Annotations
13 Annotations

Created At
5 minutes ago

Owner
RS insecure-bank-deployment-[illegible]

Restart Policy
Always Restart

Active Deadline Seconds
Not Configured

Pod IP
10.[illegible]

Node
ip-10-0-141-53.ec2.internal

End of Task 4

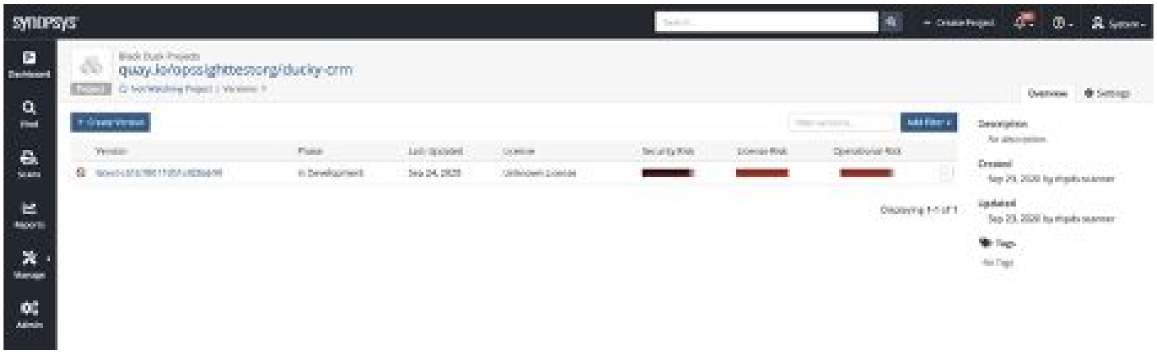
Task 5: Overview of Black Duck Scanning Results

PLEASE NOTE THAT WE'RE NOT DEMONSTRATING ALL OF BLACK DUCK'S CAPABILITIES HERE. THIS SECTION ONLY HIGHLIGHTS THE PROCESS FOLLOWED IN THIS WORKSHOP

To view the scanning results in Black Duck UI, follow these instructions:

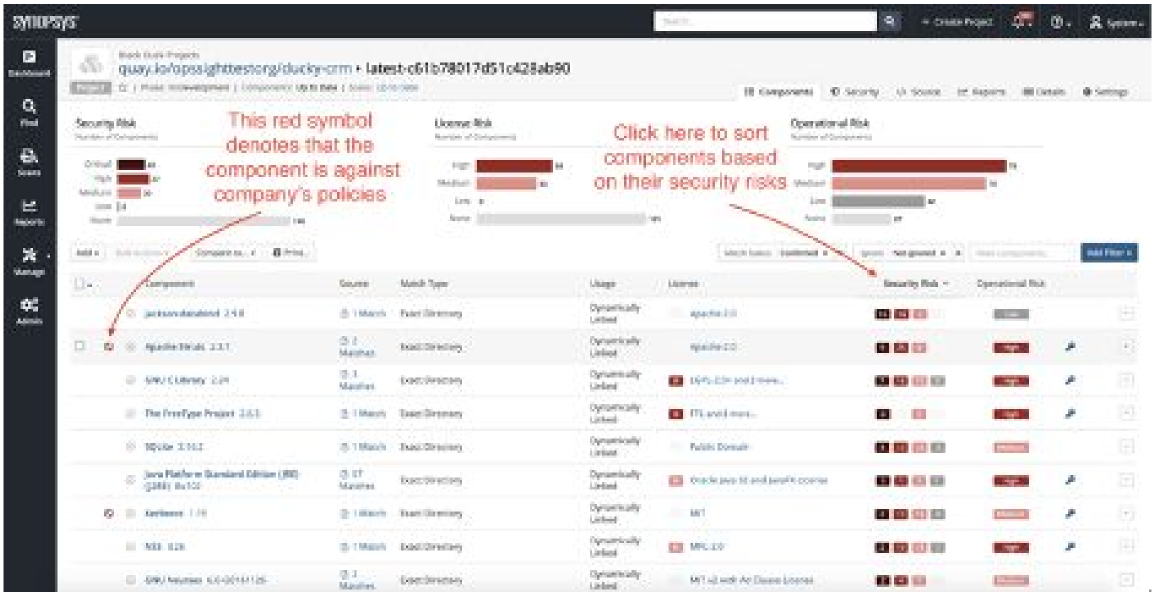
1. Open a new tab in a browser and go to this URL -> https://redhathub.blackducksoftware.com. The username and password are to be given by the instructor.

2. In the project view look for the project labelled "quay.io/opssighttestorg/ducky-crm" and click on it. The version under this project shows the SHA of the image, see screenshot below. Click on the version to proceed.



Version	Phase	Last Updated	License	Security Risk	License Risk	Operational Risk
[illegible]	In Development	Sep 24, 2020	Unknown License	▬	▬	▬

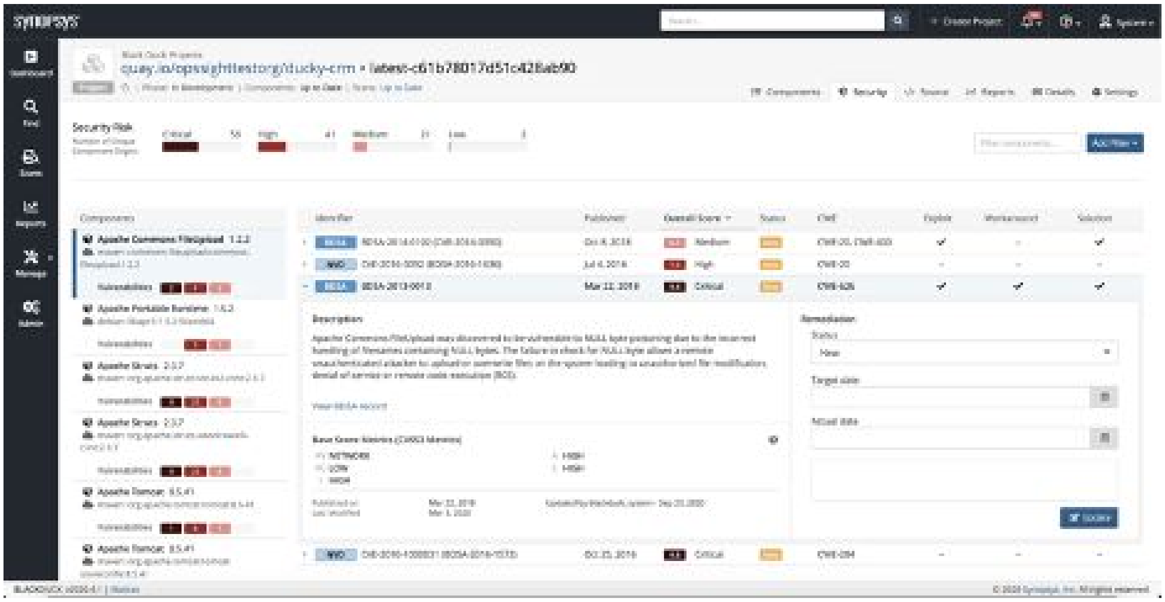
3. This will open up a Bill of Materials (BOM) view of the specific project version. The components listed are what's present inside that container, they may or may not have security vulnerabilities and policy violations. This view gives a general overview about the container.



This red symbol denotes that the component is against company's policies

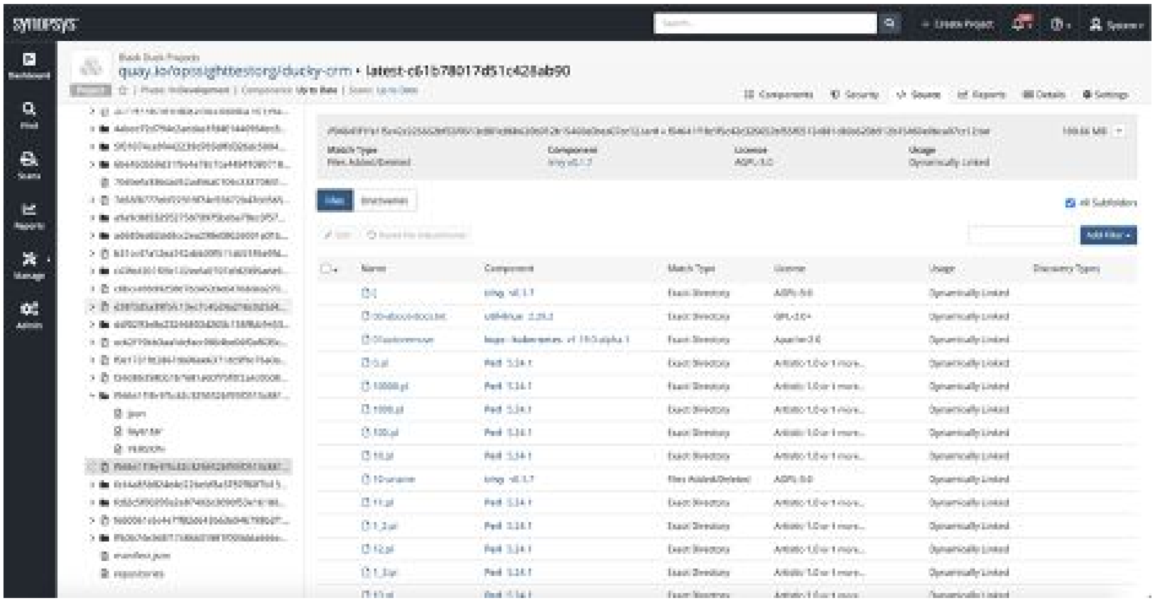
Click here to sort components based on their security risks

4. To get a more security focused view click on the security tab on the upper right side of the screen. This will showcase a more thorough view of each component and vulnerabilities associated with them. This feed of information includes Black Duck Security Advisories (BDSAs) which provide a more complete view of the vulnerabilities, their exploits and workarounds. Learn more about BDSAs here.



SYNOPSYS
quay.io/opssightestorg/ducky-crm • latest-c61b78017d51c428ab90
Security Risk
Critical
High
Medium
Low
Components
Apache Commons FileUpload 1.2.2
Apache Portable Runtime 1.6.2
Apache Struts 2.3.7
Apache Tomcat 8.5.41
Description
Remediation
Base Score Metrics (CVSS3 Metrics)

To see a more detailed view of the scanned image and layers that were scanned, view the source tab on the upper right side of the screen.



quay.io/opsisightestorg/ducky-crm › latest-c61b78017d51c428ab90

Match Type	Component	License	Usage
Files Added/Deleted	ring v0.1.7	AGPL-3.0	Dynamically Linked

Name	Component	Match Type	License	Usage	Discovery Types
1	ring v0.1.7	Exact Directory	AGPL-3.0	Dynamically Linked	
00-about-docs.txt	util-linux 2.25.2	Exact Directory	GPL-2.0+	Dynamically Linked	
01autoremove	kops - kubernetes v1.19.0-alpha.1	Exact Directory	Apache-2.0	Dynamically Linked	
0.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
10000.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
1000.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
100.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
10.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
10-uname	ring v0.1.7	Files Added/Deleted	AGPL-3.0	Dynamically Linked	
11.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
1_2.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
12.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
1_3.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	
13.pl	Perl 5.24.1	Exact Directory	Artistic-1.0 or 1 more...	Dynamically Linked	

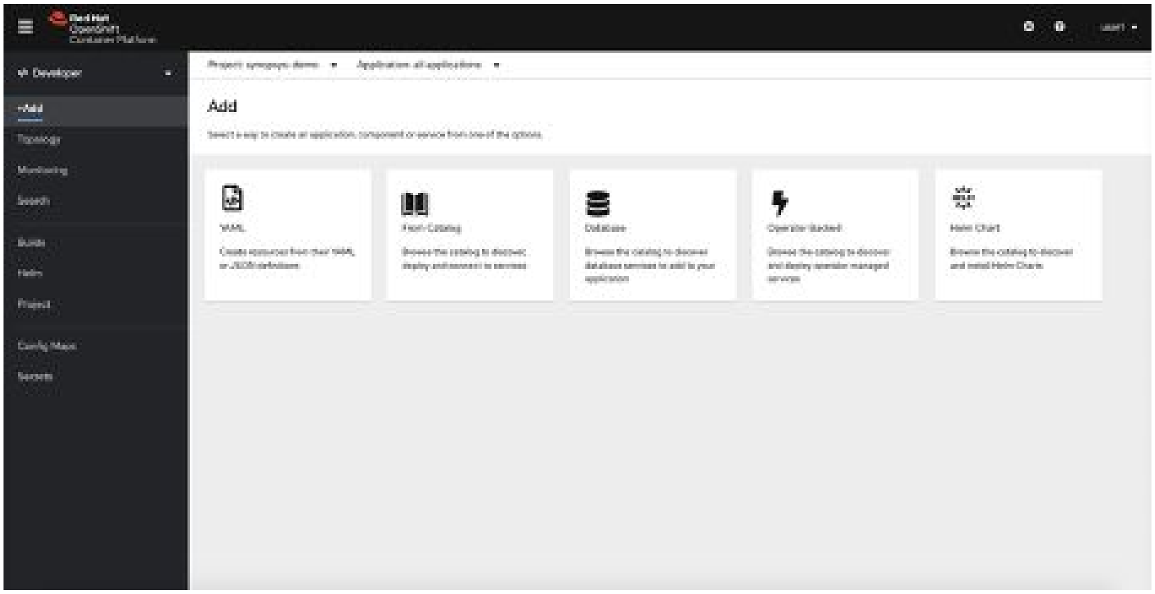
End of Task 5

Task 6: Scanning a Custom Container (Advanced)

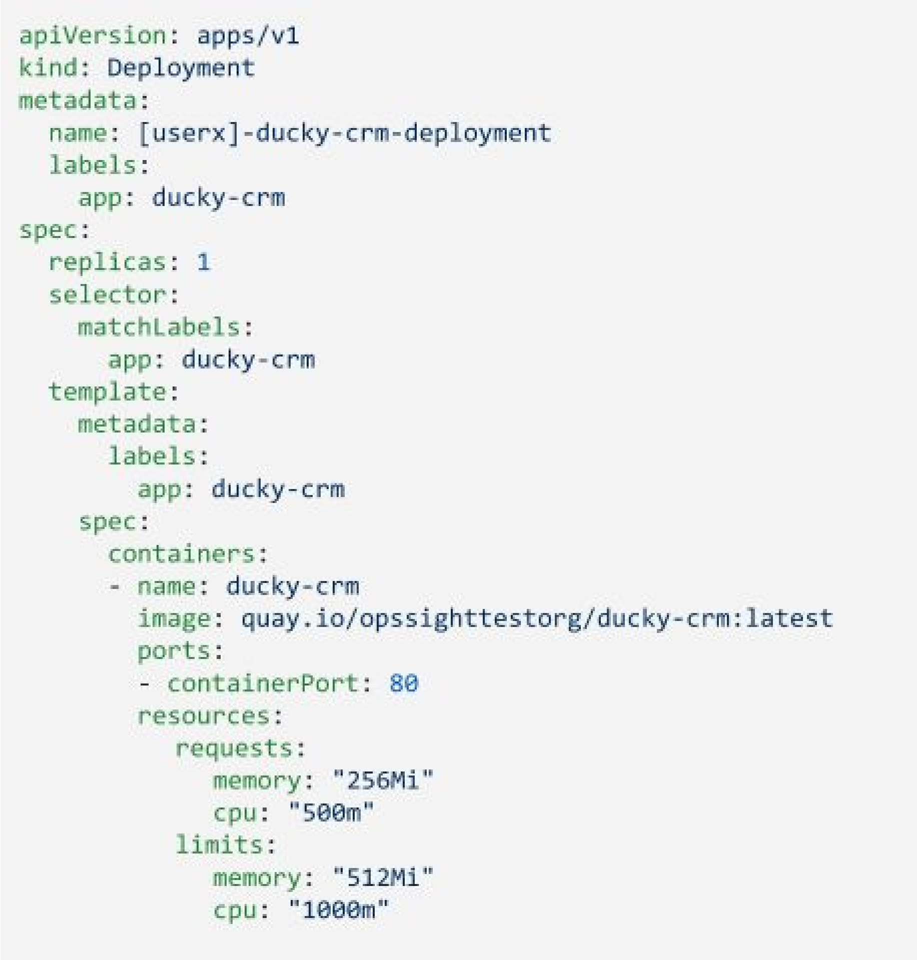
PLEASE DON'T SCAN HUGE PROJECTS, THIS BLACK DUCK INSTANCE IS UNDER AN NFR LICENSE AND HAS LIMITED CAPACITY

The objective is to deploy an application in the synopsys-demo project so that the Black Duck connector can scan it. In the steps below we'll be using the https://quay.io/repository/opssighttestorg/ducky-crm image.

1. Go to Developer section (perspective) instead of Administrator view in synopsys-demo project and select the YAML option.

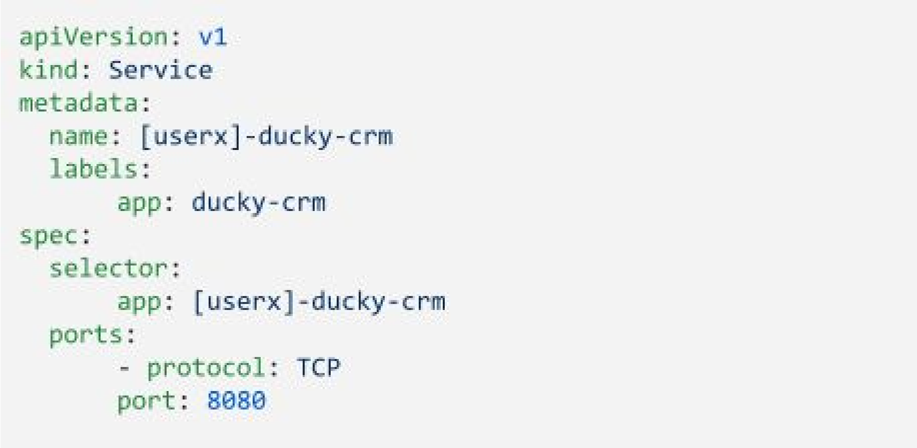

Red Hat OpenShift Container Platform
user1
Developer
+Add
Topology
Monitoring
Search
Builds
Helm
Project
Config Maps
Secrets
Project: synopsys-demo
Application: all applications
Add
Select a way to create an application, component or service from one of the options.
YAML
Create resources from their YAML or JSON definitions
From Catalog
Browse the catalog to discover, deploy and connect to services
Database
Browse the catalog to discover database services to add to your application
Operator Backed
Browse the catalog to discover and deploy operator managed services
Helm Chart
Browse the catalog to discover and install Helm Charts

2. **Note:** Other users may be creating the same application in this project, so it is important to modify the YAML below to use your lab username where [userx] is found. After updating the YAML, paste it into the editor text area and click "Create" to create the Deployment.



```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: [userx]-ducky-crm-deployment
  labels:
    app: ducky-crm
spec:
  replicas: 1
  selector:
    matchLabels:
      app: ducky-crm
  template:
    metadata:
      labels:
        app: ducky-crm
    spec:
      containers:
      - name: ducky-crm
        image: quay.io/opssighttestorg/ducky-crm:latest
        ports:
        - containerPort: 80
        resources:
           requests:
             memory: "256Mi"
             cpu: "500m"
           limits:
             memory: "512Mi"
             cpu: "1000m"
```

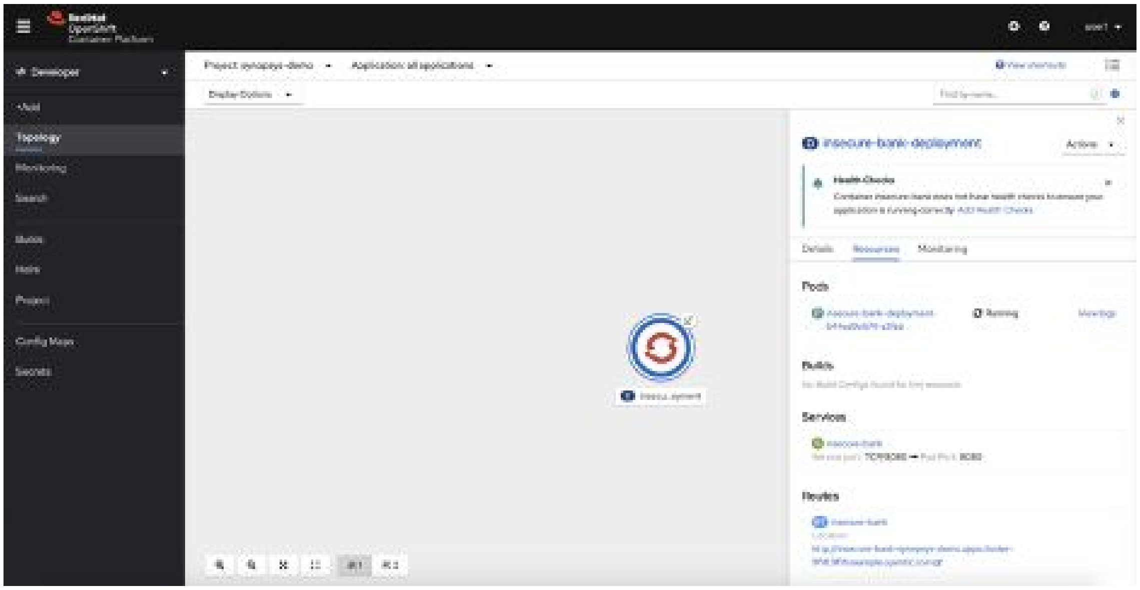
3. Click "Add again" and choose the YAML option to create the Service. Remember to modify the YAML below first with your username.



```
apiVersion: v1
kind: Service
metadata:
  name: [userx]-ducky-crm
  labels:
       app: ducky-crm
spec:
  selector:
       app: [userx]-ducky-crm
  ports:
       - protocol: TCP
       port: 8080
```

4. Verify it was successful in topology section (blue circle signifies app is running) by clicking on the new app in topology section -> go to resources tab -> and click on pods. The new labels should be

shown there shortly (sometimes it takes some time).



5. You might not be able to see the scan due to workshop blackduck restrictions, if you want to see the scan results in Black Duck please contact your lab instructor and they can give you access to Black Duck for your specific project.

End of Task 6

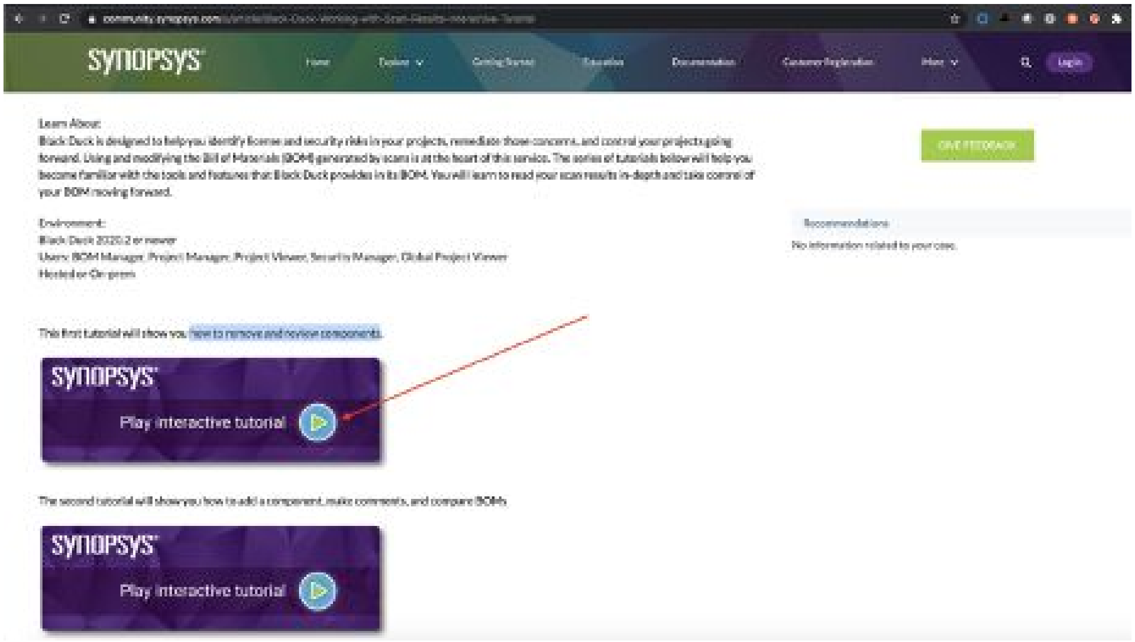
Task 7: Working with Scan Results

In this tutorial you will be logging into Synopsys e-learning URL and performing Bill Of Material (BOM) operations on the project of your choosing in https://redhathub.blackducksoftware.com.

Removing and Reviewing Components

In this section of the workshop you'll learn how to interact with the components that were discovered by Black Duck after the scanning process finished. (Components are the list of the libraries and dependencies found in the application.)

1. Visit https://community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial
2. Click on the first interactive tutorial labelled "how to remove and review components".


community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial
SYNOPSYS
Home
Explore
Getting Started
Education
Documentation
Customer Registration
More
Login
GIVE FEEDBACK
SYNOPSYS
Play interactive tutorial
SYNOPSYS
Play interactive tutorial

Learn About:
Black Duck is designed to help you identify license and security risks in your projects, remediate those concerns, and control your projects going forward. Using and modifying the Bill of Materials (BOM) generated by scans is at the heart of this service. The series of tutorials below will help you become familiar with the tools and features that Black Duck provides in its BOM. You will learn to read your scan results in-depth and take control of your BOM moving forward.

Environment:
Black Duck 2020.2 or newer
Users: BOM Manager, Project Manager, Project Viewer, Security Manager, Global Project Viewer
Hosted or On-prem

Recommendations
No information related to your case.

This first tutorial will show you how to remove and review components.

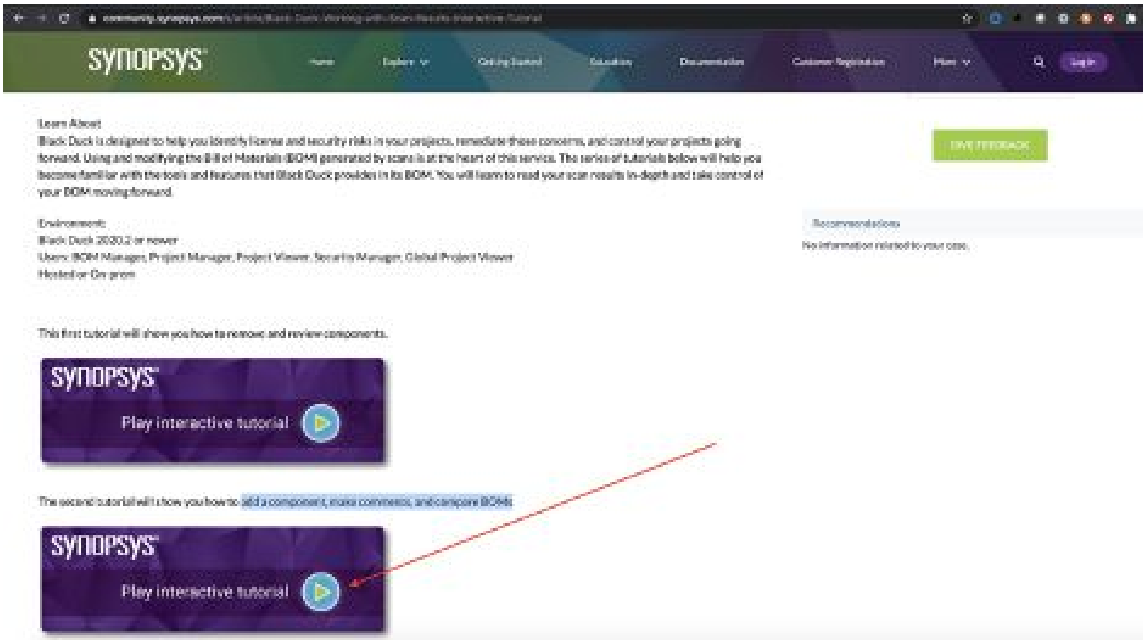
The second tutorial will show you how to add a component, make comments, and compare BOMs.

3. This will open up a new browser tab, you can interact & complete the tutorial at your own pace.

Adding a Component, Making Comments, and Comparing BOMs

In this section of the workshop you'll learn how to add custom components that were either missed by Black Duck or needs to be introduced as part of the project. This tutorial will also cover commenting and comparing Bill of Materials (BOMs) with other project to understand & verify differences between projects or project versions.

1. Visit https://community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial
2. Click on the second interactive tutorial labelled "add a component, make comments, and compare BOMs".


community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial
SYNOPSYS
Home
Explore
Getting Started
Education
Documentation
Customer Registration
More
Log In
GIVE FEEDBACK
SYNOPSYS
Play interactive tutorial
SYNOPSYS
Play interactive tutorial

Learn About
Black Duck is designed to help you identify license and security risks in your projects, remediate those concerns, and control your projects going forward. Using and modifying the Bill of Materials (BOM) generated by scans is at the heart of this service. The series of tutorials below will help you become familiar with the tools and features that Black Duck provides in its BOM. You will learn to read your scan results in-depth and take control of your BOM moving forward.

Environment:
Black Duck 2020.2 or newer
Users: BOM Manager, Project Manager, Project Viewer, Security Manager, Global Project Viewer
Hosted or On prem

Recommendations
No information related to your case.

This first tutorial will show you how to remove and review components.

The second tutorial will show you how to add a component, make comments, and compare BOMs

3. This will open up a new browser tab, you can interact & complete the tutorial in your own pace.

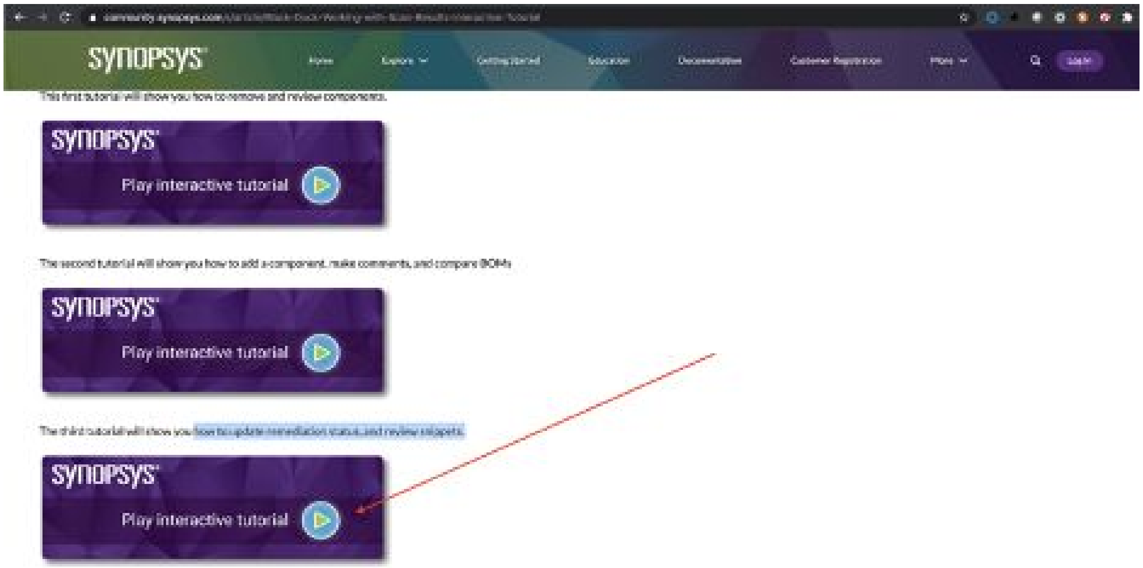
Updating Remediation Status and Reviewing Snippets

In this tutorial you will learn how to update remediation status for security vulnerabilities and review snippets detected by a snippet scan.

1. Visit https://community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-T

[utorial](https://community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial) & scroll down.

2. Click on the third interactive tutorial labelled “how to update remediation status, and review snippets”.


community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial
SYNOPSYS
Home
Explore
Getting Started
Education
Documentation
Customer Registration
More
Log In
SYNOPSYS
Play interactive tutorial
SYNOPSYS
Play interactive tutorial
SYNOPSYS
Play interactive tutorial

This first tutorial will show you how to remove and review components.

The second tutorial will show you how to add a component, make comments, and compare BOMs

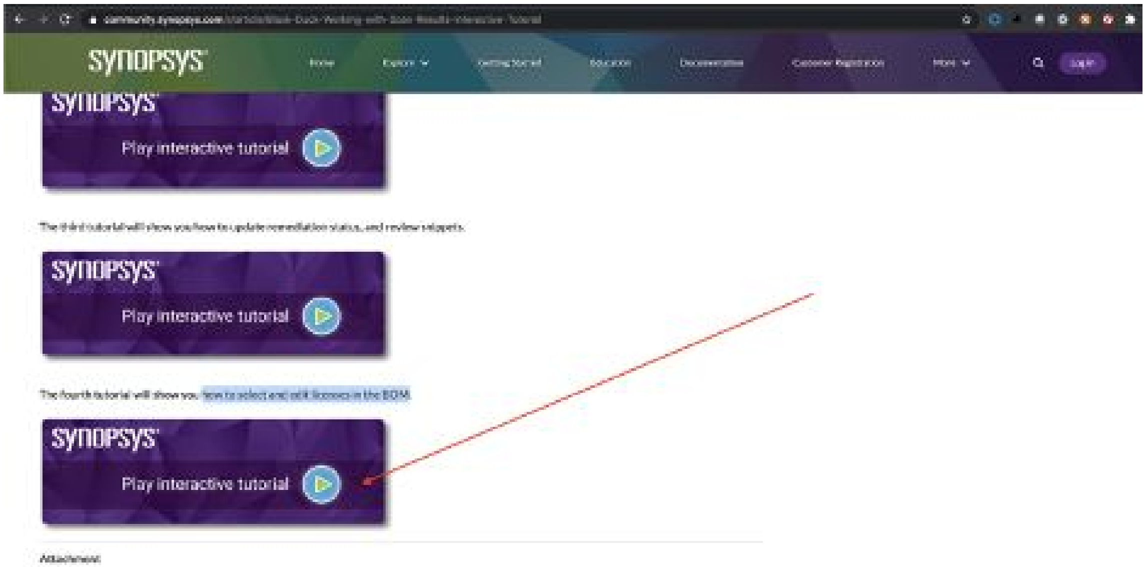
The third tutorial will show you how to update remediation status and review snippets.

3. This will open up a new browser tab, you can interact & complete the tutorial in your own pace.

Selecting and Editing Licenses

In this tutorial, you will learn how to adjust license information for BOM components.

1. Visit https://community.synopsys.com/s/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial & scroll down.
2. Click on the fourth interactive tutorial labelled “how to select and edit licenses in the BOM”.


community.synopsys.com/t5/article/Black-Duck-Working-with-Scan-Results-Interactive-Tutorial
SYNOPSYS
Home
Explore
Getting Started
Education
Documentation
Customer Registration
More
Log In
SYNOPSYS
Play interactive tutorial

The third tutorial will show you how to update remediation status, and review snippets.

SYNOPSYS
Play interactive tutorial

The fourth tutorial will show you how to select and edit licenses in the BOM.

SYNOPSYS
Play interactive tutorial

Attachment

3. This will open up a new browser tab, you can interact & complete the tutorial at your own pace.

End of Task 7

End of Workshop!

For more information on Black Duck Software Composition Analysis, click here.