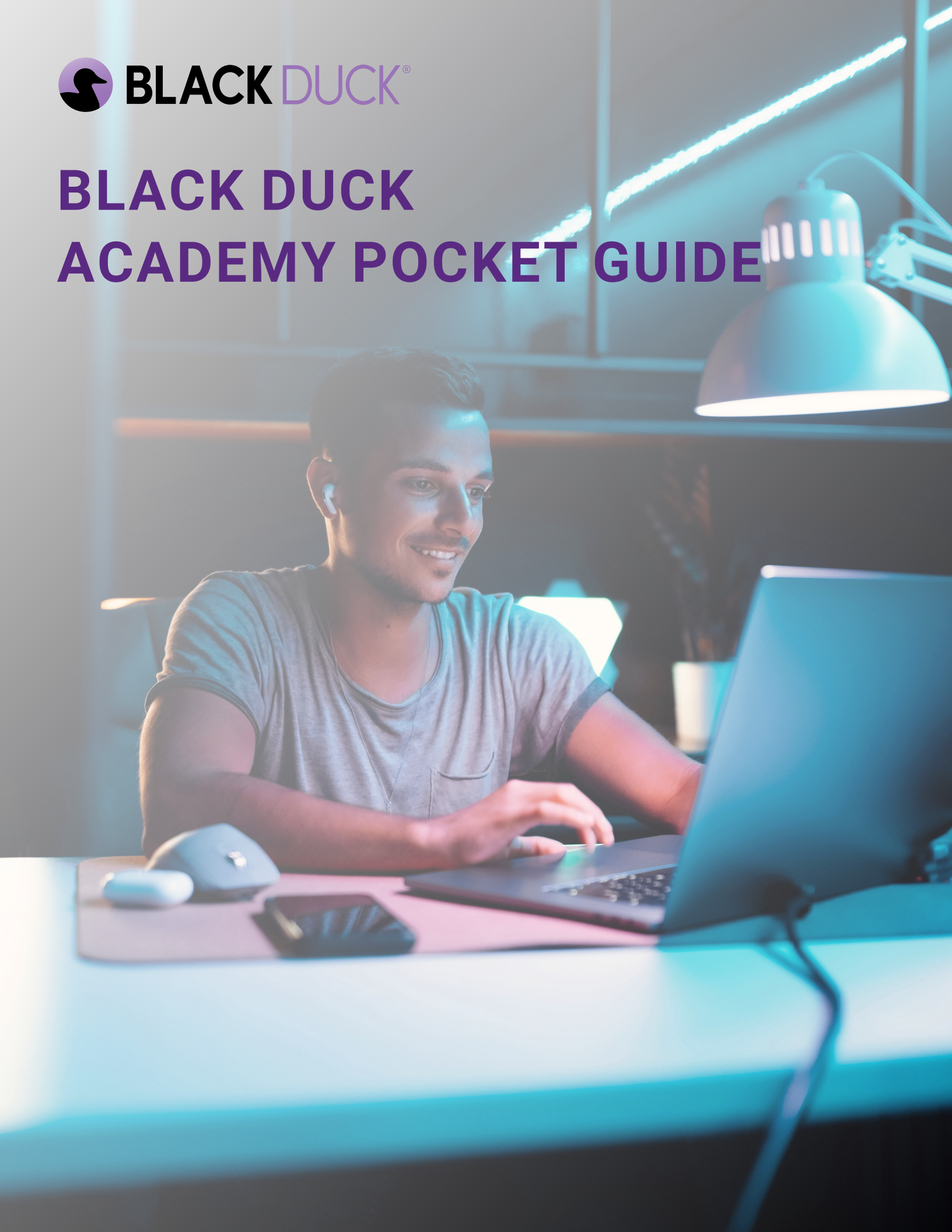
BLACK DUCK®

BLACK DUCK ACADEMY POCKET GUIDE



Introduction

Welcome to your pocket guide to the Black Duck Academy — your all-in-one resource for learning and mastering Black Duck solutions with speed, confidence, and ease.

And don't let the word Academy put you off. Who has time for long-winded, boring courses? Our bite-sized, microlearning units are designed to be short, sharp, and fun—so you can **get up and running quickly, at your own pace and on your own time.**

Whether you're a beginner, need a quick refresher, a developer integrating security into your workflow, or a security professional managing risk across your organization — **we've got your back.**

Why Integrations First?

CI/CD integrations are no longer an afterthought — they're foundational to today's development workflows. That's why we want you to be aware of our integration resources right away. By hooking Black Duck solutions into the CI/CD platforms you already use, you'll start seeing real value right away.

Now or Later — We've Got You Covered! Whether you're planning CI/CD integrations right out of the gate or saving them for later in you deployment, we want to make sure you know exactly where to find our integration resources — you'll find the integration micro-courses you need under the relevant product sections later in this guide or directly on the Academy Integrations page.

INTEGRATION	POLARIS	COVERITY	BLACK DUCK SCA
GitLab	✔	✔	✔
GitHub	✔	✔	✔
Jenkins	✔	✔	✔
Azure DevOps	✔	✔	✔

Ready to Get Started?

Welcome to our Getting Started pathways!

We know starting with new software can feel overwhelming, so we've created user-friendly Getting Started pathways just for you. These guides are organized by product and user role, offering clear, step-by-step instructions to help you understand key features and get productive quickly. Whether you're brand new or just need a refresher, we're here to make your onboarding smooth and simple.

Let's get started!

Polaris

Polaris SCA from Setup to First Results
Polaris SAST from Setup to First Results
Polaris: Administrator
Polaris: Contributing Develope
Polaris : DevOps

Coverity

Coverity from Install to First Results
Coverity for Developers (End Users)
Coverity for Managers
Coverity Getting started for Administrators
Coverity Getting Started for Build Engineers
Coverity Getting Started Server Installation and Initial Setup

Black Duck SCA

Black Duck SCA from Setup to First Results
Black Duck SCA DevSecOps
Black Duck SCA for Admins
Black Duck SCA for Developers
Black Duck SCA for End Users
Black Duck SCA for Integrations
Black Duck SCA for Managers
Black Duck SCA for Security Professionals
Black Duck SCA for the Legal Team

Defensics

Defensics: From Install to First Results
Defensics for Administrators
Defensics for Developers
Defensics for Managers
Defensics for Test Engineers
Defensics for Test Engineers Extended

Code Sight

Code Sight from Install to First Results

Your Product Success Journey

To support our customers in mastering our products, we've developed a comprehensive library of on-demand micro-courses. These bite-sized, focused modules are designed to deliver just-in-time knowledge and skills that align with the natural progression of your product journey. Whether you're just getting started or optimizing advanced capabilities, our content is structured to meet learners where they are in their adoption journey and guide them forward.

PRODUCT ADOPTION	PHASES	MATURITY LEVEL
Baseline	This phase focuses on foundational knowledge and essential setup. Courses here are ideal for new users or teams beginning their journey with our products. They cover core concepts, initial configurations, and basic usage to ensure a strong start.	
Emerging	As users gain confidence, the Emerging phase introduces intermediate topics that expand functionality and improve efficiency. These courses help learners build on their foundation by exploring more advanced features and workflows.	
Maturing	In this phase, users begin to integrate our products more deeply into their operations. Courses emphasize best practices, crossfunctional use cases, and strategic implementation to drive broader adoption and impact.	
Optimizing	This phase is designed for expert users and teams looking to maximize value. These courses focus on fine-tuning, automation, analytics, and continuous improvement strategies to achieve peak performance.	

All micro-courses are clearly labeled with their corresponding phase and sorted in sequence from Baseline to Optimizing. This organization makes it easy for users to identify where they are in their product journey and select the most relevant content to accelerate their progress. Whether you're onboarding a new team, scaling adoption across departments, or refining advanced capabilities, our microlearning collection is your roadmap to success. Dive in, explore, and grow—one bite at a time.

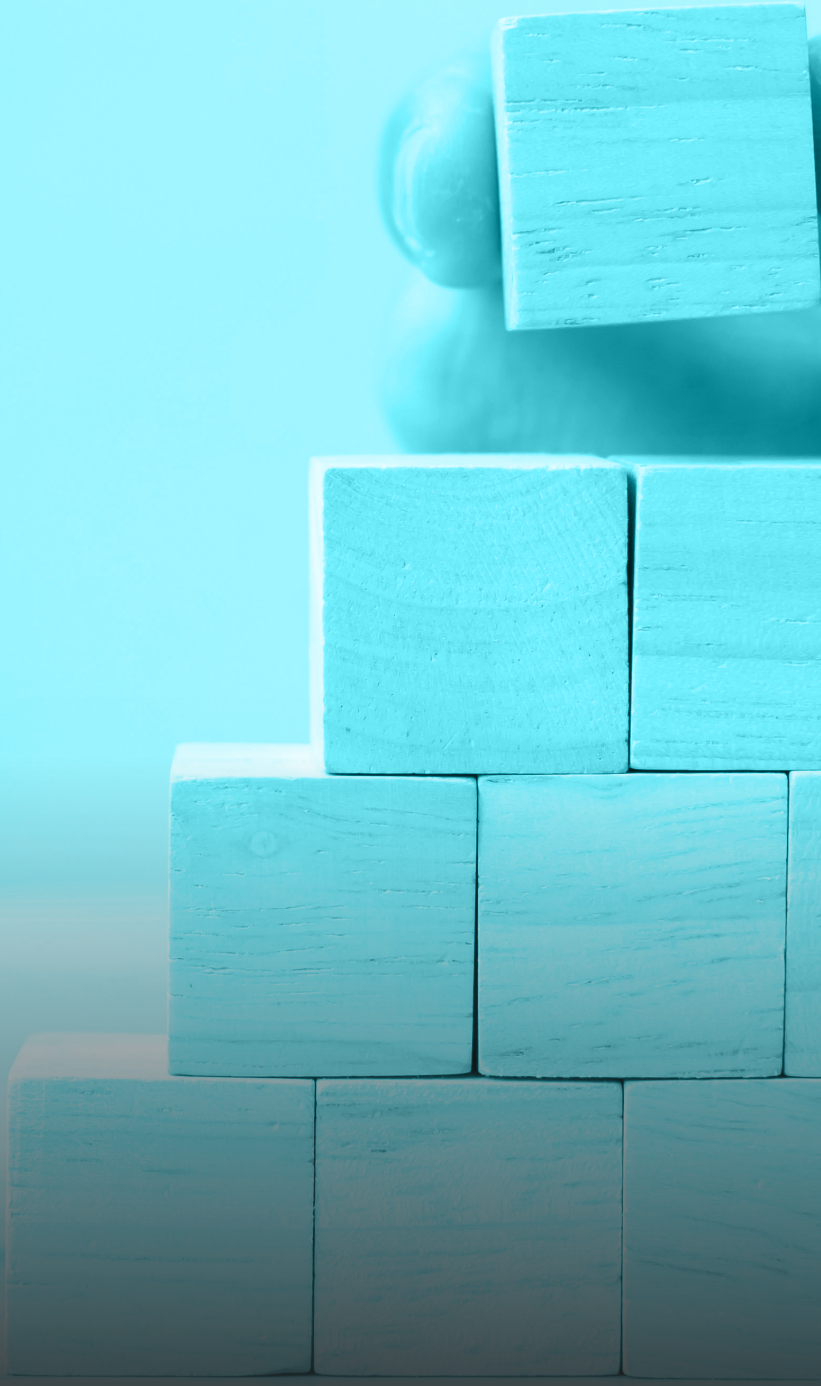
Ready to Level Up?

Looking to sharpen your skills or explore new topics? Visit **Black Duck Academy** at https://blackduck.skilljar.com.

You can browse our micro-courses, tutorials, learning paths, course summaries, and outlines without logging in. When you're ready to dive in, simply **log in** using your **Community Portal** credentials, and start leveling up.

No Login? No Problem. Just contact us at academy@blackduck.com and we'll get you fixed up.

POLARIS



Learn about Polaris Software Integrity Platform

Comprehensive application security from developer to deployment.

Baseline ■ □ □ □

- **Basic deployment** Core functionality is installed and minimally configured. Usage may be ad hoc, with little to no automation or integration. Visibility is limited to basic metrics or logs.

Emerging ■ ■ □ □

- **Ramped deployment** Key integrations with CI/CD pipelines are established. Automation begins for routine tasks like scanning or policy enforcement. Teams start aligning product use with development workflows.

Maturing ■ ■ ■ □

- **Advanced deployment** The solution is widely deployed across teams or projects. Automation is policy-driven and consistent. Integration with developer tools and environments is robust. Dashboards and reporting begin to inform decisions.

Optimizing ■ ■ ■ ■

- **Proficient "reference" deployment** Full integration across the SDLC. Analytics dashboards provide actionable insights. Feedback loops drive continuous improvement. Manual intervention is rare. Usage is proactive, with predictive capabilities and strategic alignment.

Polaris: Getting started with fAST SCA ■ □ □ □

Summary: This course will cover how to run a fAST SCA and view results. Polaris is our SaaS solution for unifying SCA, SAST and DAST scans on a single platform. This course will show you how to run a test for an SCA scan and how to view results.

URL: blackduck.skilljar.com/polaris-getting-started-with-fast-sca

Polaris: Insights and Reports ■ □ □ □

Summary: This course walks through the dashboards and the reporting interfaces in Polaris. Polaris Dashboards is a great visual help for you to see an overview of your applications and issues. This view gives you an insight on what is happening with your applications and projects. Reporting interface provides meaningful reports for you and your users.

URL: blackduck.skilljar.com/polaris-insights-and-reports

Polaris: Creating an Access Token ■ □ □ □

Summary: In this lesson we'll learn how to create an Access Token in Polaris.Once you know where to look in the Polaris web UI, access tokens are easy to generate. In this lesson we'll review the steps needed to make an access token.

URL: blackduck.skilljar.com/polaris-creating-an-access-token-1

Polaris: Ways to Triage Issues ■ □ □ □

Summary: There are several ways to triage your findings in Polaris, in this lesson we'll list and discuss the options available to you. You'll learn that triaging your findings in Polaris is fairly straight forward. However since there are several ways to do this, this lesson is designed to make you aware of the options you have available to you and show you how to use those tools.

URL: blackduck.skilljar.com/polaris-ways-to-triage-issues

Polaris: Using the Bridge CLI ■ □ □ □

Summary: In this micro course you will learn how to use the Bridge CLI to capture code for a Polaris scan. This micro-course provides a quick overview of the Bridge CLI and how you can use it run Polaris testing in your CI/CD pipeline, allowing you to perform any needed heavy computation analysis on Polaris cloud servers. It will show you how to run scans and receive results from the command line, either by scripting or running the commands manually.

URL: blackduck.skilljar.com/polaris-using-the-synopsys-bridge

Polaris: A Video Introduction

Summary: This video will give you a brief introduction to Polaris

URL: blackduck.skilljar.com/polaris-a-video-introduction

Polaris: Getting started with fAST Dynamic

Summary: This course will cover how to run a fAST Dynamic test and view results. Polaris is our SaaS solution unifying DAST, SAST and SCA scans on a single platform. This course will show you how to run a DAST scan on a site and how to view the results

URL: blackduck.skilljar.com/polaris-getting-started-with-fast-dynamic

Polaris: Getting started with fAST STATIC

Summary: This course will cover how to run a fAST Static test and view results. Polaris is our SaaS solution unifying SAST, SCA and DAST scans on a single platform. This course will show you how to run a static analysis test on source code and how to view the results.

URL: blackduck.skilljar.com/polaris-getting-started-with-fast-static

Polaris: Reviewing Scan Results

Summary: In this lesson we'll learn about the Polaris Portfolio Project Page Interface and how to review scan results. The Portfolio Project Page allows you to view, triage, and export a project's issues, and view a project's components (bill of materials) and licenses. Familiarizing yourself with the Project Page will allow you to maneuver your way through issues quickly and efficiently.

URL: blackduck.skilljar.com/polaris-reviewing-scan-results

Polaris: Create Application

Summary: This video will give you a brief overview to creating an Application, Project, and Branch in Polaris.

URL: blackduck.skilljar.com/polaris-create-application

Polaris: My Organization Settings, Groups and Roles

Summary: This course will look at configuring user roles in Polaris. This course will look at configuring user roles in Polaris. We will take a look at how to create and manage your application roles, then look at how we can apply them to projects.

URL: blackduck.skilljar.com/polaris-my-organization-settings-groups-and-roles

Polaris: Create and Manage Labels

Summary: For organizations looking to classify their applications, projects or branches, Polaris offers Organization Administrators the capability to create Labels.

URL: blackduck.skilljar.com/polaris-create-and-manage-labels

Polaris: GitLab Integration (Integration)

Summary: Integrate Polaris with GitLab using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Polaris with GitLab. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/polaris-gitlab-integration

Polaris Jira Integration

Summary: This micro-course walks you through how to integrate Jira with Polaris. This micro-course walks you through how to integrate Jira with Polaris. It covers ever step needed to enable the export of individual issues to your Jira Cloud.

URL: blackduck.skilljar.com/polaris-jira-integration

Polaris Single Sign-on (SSO) Configuration with SAML 2.0

Summary: Polaris supports SAML 2.0 single sign-on (SSO). Customers are able to establish SAML 2.0-based SSO authentication, enabling their users to seamlessly sign into Polaris. This allows users to log into Polaris using an SSO authentication service, such as OKTA. Typically, DevOps staff configure SAML authentication. SAML is a standard authentication protocol between a service provider (SP), in this case Polaris, and an identity provider (IdP) like OKTA.

URL: blackduck.skilljar.com/polaris-single-sign-on-sso-configuration-with-saml-20

Polaris: Running a Signature Analysis

Summary: Learn how to run a Signature Analysis in Polaris. Black Duck allows for the creation of an SBOM within the user interface. SBOM is a standard format for tracking OSS in your software projects. Black Duck makes it very quick and easy to generate a Bill of Materials in this format. Polaris offers both Package Manager and Signature Scan methodology for thorough coverage in Software Composition Analysis. This course will cover how to run a signature analysis which discovers components by their directory structure signature.

URL: blackduck.skilljar.com/polaris-running-a-signature-analysis

Polaris: Azure DevOps Bug Tracking Integration

Summary: This micro-course walks you through how to integrate Azure DevOps bug tracking with Polaris. It covers the steps needed to enable the export of individual issues to Azure showing both the admin setup and the project based setup. Detailed technical requirements can be found [3]here in the Documentation

URL: blackduck.skilljar.com/polaris-azure-devops-bug-tracking-integration

Polaris: Creating an SBOM Report

Summary: This micro-course provides a quick overview of creating an SBOM report in Polaris. Users will see what options are available and how to see the details of the report generation.

URL: blackduck.skilljar.com/polaris-creating-an-sbom-report

Polaris: Azure DevOps Integration **(Integration)**

Summary: This course describes how to use our Security Scan extension for Azure DevOps with Polaris allowing you to easily integrate security testing into your CI pipeline. It will walk you through adding the Security Scan Action to your pipeline allowing you to automate SAST and SCA scans on every push.

URL: blackduck.skilljar.com/polaris-azure-devops-integration

Polaris: Using the Black Duck Security Scan Action for GitHub **(Integration)**

Summary: This micro-course describes how to use our Security Scan Action for GitHub with Polaris allowing you to easily integrate security testing into your CI pipeline. It will walk you though adding the Security Scan Action to your GitHub workflow.yml file allowing you to automate SAST and SCA scans on every push. You can find more information on our Security Scan Action in the GitHub marketplace at https://github.com/marketplace/actions/black-duck-security-scan.

URL: blackduck.skilljar.com/polaris-using-the-black-duck-security-scan-action-for-github

Polaris: Jenkins Integration (Integration)

Summary: Integrate Polaris with Jenkins using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Polaris with Jenkins. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/polaris-jenkins-integration

Polaris: Rapid Bulk SCM Onboarding

Summary: Learn how to onboard hundreds of repositories in minutes with Bulk SCM onboarding in Polaris. Learn how to onboard hundreds of repositories in minutes with Bulk SCM onboarding in Polaris. It is a constant challenge for modern app and DevOps team to onboard and scale AppSec tests in today's highly complex and distributed software environment.

URL: blackduck.skilljar.com/polaris-rapid-bulk-scm-onboarding

Integrating Polaris Findings into Software Risk Manager

Summary: Software Risk Manager (SRM) comes out of the box with a broad set of connectors for popular open source and third party products, including our tools. Integrating Polaris with SRM is simple, but it is almost always easier to see the process in action first. This interactive module walks you through how to integrate and import Polaris findings into SRM.

URL: blackduck.skilljar.com/integrating-polaris-findings-into-software-risk-manager

Polaris: Using the GitHub Action

Summary: This micro-course describes how to use our Security Scan Action for GitHub with Polaris allowing you to easily integrate security testing into your CI pipeline. It will walk you though adding the Security Scan Action to your GitHub workflow.yml file allowing you to automate SAST and SCA scans on every push. You can find more information on our Security Scan Action in the GitHub market place at https://github.com/marketplace/actions/black-duck-security-scan.

URL: blackduck.skilljar.com/polaris-using-the-synopsys-github-action

Polaris: Application Risk Scoring

Summary: This course is an introduction to application risk scoring capabilities in Polaris. Risk Scoring provides each application in Polaris with a risk score which helps differentiate applications on the threat that they represent to an organization. Use this information to identify potential dangers and prioritize how to address them.

URL: blackduck.skilljar.com/polaris-application-risk-scoring

Polaris: Policies

Summary: In this lesson we'll take a look at Polaris's Policies page and learn about its issue and test frequency policies for projects. Polaris offers policy-based escalations for each project in your portfolio. In this lesson we'll take a look at both issue and test frequency policies for projects.

URL: blackduck.skilljar.com/polaris-policies


COVERITY

Learn about Coverity Static Application Security Testing

Address security and quality defects in code as it's being developed.

Baseline ■ □ □ □

- **Basic deployment** Core functionality is installed and minimally configured. Usage may be ad hoc, with little to no automation or integration. Visibility is limited to basic metrics or logs.

Emerging ■ ■ □ □

- **Ramped deployment** Key integrations with CI/CD pipelines are established. Automation begins for routine tasks like scanning or policy enforcement. Teams start aligning product use with development workflows.

Maturing ■ ■ ■ □

- **Advanced deployment** The solution is widely deployed across teams or projects. Automation is policy-driven and consistent. Integration with developer tools and environments is robust. Dashboards and reporting begin to inform decisions.

Optimizing ■ ■ ■ ■

- **Proficient "reference" deployment** Full integration across the SDLC. Analytics dashboards provide actionable insights. Feedback loops drive continuous improvement. Manual intervention is rare. Usage is proactive, with predictive capabilities and strategic alignment.

Coverity: Installing the Analysis Software ■ □ □ □

Summary: This micro course will walk you through how to install the Coverity Analysis Software. It provides step-by-step guidance for the complete process.

URL: blackduck.skilljar.com/coverity-installing-the-analysis-software

Coverity for Developers (End Users) ■ □ □ □

Summary: This learning path covers everything an end user needs to know about using Coverity. This learning path includes the micro courses Introduction to Coverity, Coverity: Examining and Triaging issues, Coverity: Views, Filters and Notifications, Coverity: Concepts for Developers, and Coverity: Desktop Analysis Options. It also includes Coverity: Classic Fast Desktop for your IDE, and Coverity: Classic Fast Desktop CLI as optional lessons.

URL: blackduck.skilljar.com/coverity-for-developers-end-users

Introduction to Coverity ■ □ □ □

Summary: This micro course provides a quick introduction to what Coverity is. This high-level overview of Coverity is also included in some of our role and mission-based courses. If you are not planning to take any other course, or just want to get a quick Coverity overview, then this is the course for you.

URL: blackduck.skilljar.com/introduction-to-coverity

Coverity: License Activation and Software Download ■ □ □ □

Summary: This micro course will show you how to activate your Coverity license and download the software. This course can be a good starting point if your company has just purchased Coverity software.

URL: blackduck.skilljar.com/license-activation-and-software-download

Coverity: Examining and Triaging issues ■ □ □ □

Summary: This micro course will show you how to examine and triage issues using the Coverity web interface. It covers how to navigate different projects, how to look at defect details, and explores some of the available options. It also covers how to classify issues, set severity levels, and define required actions.

URL: blackduck.skilljar.com/coverity-examining-and-triaging-issues

Installing Coverity Platform (Server) on Linux

Summary: Learn to Install Your Coverity Platform (Server) on Linux. This micro course will show you how to install the Coverity Connect Platform server on Linux. It will walk you through the complete installation process so you know exactly what to expect before you start the process yourself.

URL: blackduck.skilljar.com/installing-coverity-platform-server-on-linux

Coverity: Concepts for Developers

Summary: This micro course covers important Coverity terms and concepts for developers. you will learn how projects, streams, and snapshots map to more familiar source control concepts such as branches and releases. You will also learn about issue merging, and how components can be used to logically partition source code.

URL: blackduck.skilljar.com/coverity-concepts-for-developers

Coverity: Installing the Connect Server

Summary: This micro course will show you how to install the Coverity Connect Platform server. This micro course will show you how to install the Coverity Connect Platform server. It will walk you through the complete installation process so you know exactly what to expect before you start the process yourself.

URL: blackduck.skilljar.com/installing-the-connect-server

Coverity: Rollout Stages

Summary: This micro-course provides you with things to consider as you roll out and mature your teams use of Coverity. While the order of the rollout stages presented here no longer exactly matches our latest Production Adoption Maturity Model (PAMM) recommendations the video still provides very useful information on what to consider as you deploy different Coverity features.

URL: blackduck.skilljar.com/coverity-rollout-stages

Point and Scan Quick Start for Coverity Connect users

Summary: This micro course will show you how the Coverity Point and Scan graphical tool can be used to simply capture and analyze code. Point and Scan is intended for users running occasional scans of one or more codebases and is not intended for use in automation but it does provide basic guidance on how a user can set up automation using the Coverity CLI. This means Point and Scan is a great starting point for many users.

URL: blackduck.skilljar.com/point-and-scan-quick-start-for-coverity-connect-users

Coverity: Getting Started Projects and Streams

Summary: This micro course will show you how to get started with understanding and creating Coverity projects and streams. Projects and Streams are used to map your projects and source control branches onto the Coverity server. While this process is fairly straightforward and forgiving it is always better to set things up correctly from the start

URL: blackduck.skilljar.com/coverity-getting-started-projects-and-streams

Analyzing Code Using the Coverity CLI

Summary: This micro course will show you how to use the new simplified Coverity CLI to auto-capture and analyze code. The new Coverity CLI enables teams to easily generate analysis results often without needing to understand or set up a special build environment for each codebase. This course will walk you through using the new Coverity CLI so you know exactly what to expect before you start the process yourself

URL: blackduck.skilljar.com/analyzing-code-using-the-coverity-cli

Coverity: Picking your Code Capture Strategy

Summary: This micro course will discuss the various options for capturing code helping you decide on the best approach. Coverity provides several different methods for capturing the source code that needs to be analyzed. Each method is optimized for different needs. Trying to decide on the best method to use for your codebase can be confusing for new users. This micro course will walk you through your options and help you to make the best choice for your situation and codebase.

URL: blackduck.skilljar.com/coverity-picking-your-code-capture-strategy

Coverity: Downloading the Analysis license and Software

Summary: This micro course will walk you through how to download the Coverity Analysis license and Software. The course will take you step by step from logging into the community to downloading exactly what you need.

URL: blackduck.skilljar.com/coverity-downloading-the-analysis-license-and-software

Coverity: Baselining Analysis Results

Summary: In this micro course, we will cover what to do when bringing an existing codebase with lots of Coverity findings into Coverity for the first time. It is never a good idea to overwhelm developers with a huge number of issues all at one time. Understanding how to properly baseline your code is key to avoiding overwhelming the team and starting on a good path forward.

URL: blackduck.skilljar.com/coverity-baselining-analysis-results

Coverity Reporting Basics

Summary: This micro course will show you how to use the Coverity report tools and how to easily export the data you need to create custom reports.

URL: blackduck.skilljar.com/coverity-reporting-basics

Coverity for Managers

Summary: A Course for Managers covering rollout steps, how to measure ROI, and basic reporting. You want an overview of the common Coverity deployment models, and how they may fit into your SDLC ecosystem and processes. You wish to know the best practices to successfully introduce Coverity into existing teams and projects. You want to understand the Coverity Adoption Maturity path, through the stages of which you can evolve the initial deployment, to maximize your investment. You want to measure and track the integrity of your software. If that is the case, then this course is for you.

URL: blackduck.skilljar.com/coverity-for-managers

Coverity: Views, Filters and Notifications

Summary: This micro course covers the available view types, how to create custom views, and how to create a notification based on a view. Being able to quickly focus on the issues that matter the most to you is very important especially If Coverity finds a large number of issues. This micro course covers when to use the various view types, how to create custom views, and how to create a notification based on a view. This will enable you to easily focus on the issues that are the most critical to you.

URL: blackduck.skilljar.com/coverity-views-filters-and-notifications

Coverity Connect: SAML SSO Authentication

Summary: This micro course covers configuring Coverity Connect with SAML SSO. Coverity Connect supports SAML 2.0 single sign-on (SSO) authentication. This course covers how to configure Connect as a SAML Service Provider (SP) with an SAML Identity Provider (IdP), such as OKTA.

URL: blackduck.skilljar.com/coverity-connect-saml-sso-authentication

Coverity: GitLab Integration **(Integration)**

Summary: Integrate Coverity with GitLab using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Coverity with GitLab. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/coverity-gitlab-integration

Coverity: GitHub Integration (Integration)

Summary: Integrate Coverity with GitHub using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Coverity with GitHub. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/coverity-github-integration

Coverity: Jenkins Integration (Integration)

Summary: Integrate Coverity with Jenkins using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Coverity with Jenkins. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/coverity-jenkins-integration

Coverity: Azure DevOps Integration (Integration)

Summary: Integrate Coverity with Azure DevOps using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Coverity with Azure DevOps. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/coverity-azure-devops-integration

Coverity: Backups and Data purging

Summary: This micro course will show you how to set up automatic Coverity backups and data purging. Backups and managing database size are important aspects of any system that contains a database. This micro course will show you how to set up automatic backups of your Coverity Connect server. The course will also cover how to configure issue detail purging and snapshot summary purging which will greatly assist in keeping the size of the Connect database manageable.

URL: blackduck.skilljar.com/coverity-backups-and-data-purging

Using Sigma Rapid Scan Static in GitHub

Summary: Standalone Rapid Scan Static is a fast and easy to use headless SAST scanner that fits seamlessly into the early stages of the modern development lifecycle and is free for use by Coverity customers. This course will walk you through the exact steps needed to set up a GitHub action including the use of GitHub secrets to protect your security. Both GitHub experts and beginners should find the included example main.yml file helpful in getting started with Rapid Scan Static.

URL: blackduck.skilljar.com/using-sigma-analysis-in-github

Coverity: Users Groups and Roles

Summary: This micro course will show you how to manage Users, Groups and Roles on your Connect server. Managing users, groups, and roles is a critical part of administering a Connect server. This micro course will show you how to add users and groups to your system and also covers how to use roles to correctly assign permissions.

URL: blackduck.skilljar.com/users-groups-and-roles

Coverity: Builtin and Custom Attributes

Summary: This micro course will show you how to create custom attributes in the Coverity issue database. This micro course will show you how to create custom attributes in the Coverity triage store. An attributes is what Coverity calls a field in the Coverity issue database (triage store). This can be very helpful when you need to track additional data about issues that Coverity does not include by default.

URL: blackduck.skilljar.com/coverity-builtin-and-custom-attributes

Getting Started with Sigma Rapid Scan Static Standalone

Summary: Rapid Scan Static using the Sigma engine is a fast and easy to use headless SAST scanner that fits seamlessly into the early stages of the modern development lifecycle that is free for use by Coverity customers. This micro-course will walk you through running a standalone Rapid Scan Static analysis using the CLI and show you how you can use a configuration file to set custom default options. The micro-course will also cover how you can easily use a policy file to break builds when integrating Rapid Scan Static into a pipeline like Jenkins.

URL: blackduck.skilljar.com/getting-started-with-sigma

Coverity: Checking Connect status and diagnostics

Summary: This micro course will show you how to start, and check diagnostics on your Connect server. This micro course will show you how to start, and check diagnostics on your Connect server. It will walk you through the available system diagnostics found under the help menu and demonstrate how to download the available log files. In addition, it also covers the commands needed to manually startup and shutdown the Coverity server.

URL: blackduck.skilljar.com/checking-connect-status-and-diagnostics

Creating a coverity.yaml configuration file.

Summary: This micro course will show you how to create a Coverity Yaml configuration file. Both the Coverity CLI and Point and Scan can run with just the default autogenerated configuration file. To get the best results however it is often helpful and sometimes required that users update their coverity.yaml configuration file. This tutorial will show you how you can use the provided schema to make editing the file easier and give you a basic idea of what you need to do when updating the file.

URL: blackduck.skilljar.com/creating-a-coverityyaml-configuration-file

Code Sight Configuration for Coverity Users

Summary: This course will help you learn to configure Code Sight to work with Coverity so that you can access advanced features and make use of the tool in non-default configurations. It is recommended that one member of each team using Code Sight or someone from DevOps take this course so that they can distribute customized configuration files. In addition, as an optional lesson, this course provides some basic troubleshooting information.

URL: blackduck.skilljar.com/code-sight-configuration-for-coverity-user

Coverity: How to replace your license

Summary: This micro course will show you how to update your Coverity license before or when it expires. The Coverity license consists of two parts; the platform license and the analysis license. They are downloaded and deployed separately. When your Coverity license expires or ideally a short while beforeit expires you will need to update it on your Coverity Connect platform server. You will also need to update your analysis license. This micro course will show you how to update your Coverity licenses.

URL: blackduck.skilljar.com/coverity-how-to-replace-your-license

Coverity: Doing a Basic Upgrade

Summary: This micro course will show you how to do a basic Coverity upgrade.

URL: blackduck.skilljar.com/coverity-doing-a-basic-upgrade

Coverity: Desktop Analysis Options

Summary: This micro course will help you decide if desktop analysis makes sense for you and if so what approach to take Coverity offers two options for running a desktop analysis Code Sight and Classic Fast Desktop. This micro course will help you decide if desktop analysis makes sense for you and if so which approach to take.

URL: blackduck.skilljar.com/coverity-desktop-analysis-options

Coverity: Classic Fast Desktop CLI

Summary: This micro course will help you get started with Coverity Classic Fast Desktop CLI giving you the power of Coverity features on your desktop. It will show you how to configure and use the CLI. It will also show you how you can use it in VI and Emacs.

URL: blackduck.skilljar.com/coverity-classic-fast-desktop-cli

Coverity: Classic Fast Desktop for your IDE

Summary: This micro course will help you get started with Coverity Classic Fast Desktop giving you the power of Coverity features within the comfort and convenience of your IDE. It will show you how to configure and use the plugin/extension in your IDE.

URL: blackduck.skilljar.com/coverity-classic-fast-desktop-for-your-ide

Integrating Coverity Findings into Software Risk Manager

Summary: Software Risk Manager (SRM) comes out of the box with a broad set of connectors for popular open source and third party products, including our tools. Integrating Coverity with SRM is simple, but it is almost always easier to see the process in action first. This interactive module walks you through how to integrate and import Coverity findings into SRM.

URL: blackduck.skilljar.com/integrating-coverity-findings-into-software-risk-manager

Rehosting your License and Upgrading to a new Coverity Server

Summary: This micro course will show you how to update your Coverity license so it will work on a new server. It will then go over the best method to move or upgrade Coverity onto that new server. It is intended for Coverity Admins, Devops and Security administrators who are preparing for moving Coverity to new server hardware.

URL: blackduck.skilljar.com/rehosting-your-license-and-upgrading-to-a-new-coverity-server

Creating Custom Coverity Checkers with CodeXM

Summary: This course takes you through the basics of writing custom Coverity checkers and integrating them into your Coverity analysis. You will also learn how you can use the CodeXM extension for Visual Studio Code to make the process of writing and testing checkers easier.

URL: blackduck.skilljar.com/creating-custom-coverity-checkers-with-codexm

Coverity: Using Models to Improve Analysis

Summary: In this course, you will learn how you can use models to give more information to Coverity and improve your analysis results helping to eliminate false positives and false negatives. It is intended for Coverity Admins, DevOps, and Security personal with enough knowledge of the codebase to be able to provide additional information to the analysis. Models are not normally needed for false positives but can be very helpful if you have a recurring issue with a particular type of issue.

URL: blackduck.skilljar.com/coverity-using-models-to-improve-analysis

BLACK DUCK SCA

Learn about Black Duck SCA Software Composition Analysis

Manage and monitor open source risk.

Baseline

- **Basic deployment** Core functionality is installed and minimally configured. Usage may be ad hoc, with little to no automation or integration. Visibility is limited to basic metrics or logs.

Emerging

- **Ramped deployment** Key integrations with CI/CD pipelines are established. Automation begins for routine tasks like scanning or policy enforcement. Teams start aligning product use with development workflows.

Maturing

- **Advanced deployment** The solution is widely deployed across teams or projects. Automation is policy-driven and consistent. Integration with developer tools and environments is robust. Dashboards and reporting begin to inform decisions.

Optimizing

- **Proficient "reference" deployment** Full integration across the SDLC. Analytics dashboards provide actionable insights. Feedback loops drive continuous improvement. Manual intervention is rare. Usage is proactive, with predictive capabilities and strategic alignment.

Black Duck SCA: Scanning Guide and Tips

Summary: This guide will outline different scanning tools, their advantages and disadvantages, and some considerations for the best use of scanning. This course will show an outline of different scanning tools. The advantages and disadvantages are listed to help users better choose scan methodologies that are tuned to their goals.

URL: blackduck.skilljar.com/black-duck-scanning-guide-and-tips

Black Duck SCA: Hosted System Log-in

Summary: This course is for users who are beginning with their Hosted Black Duck instance. It will walk you through the registration process. At the end, you will complete your first log-in on your Hosted Black Duck instance.

URL: blackduck.skilljar.com/black-duck-hosted-system-log-in

Black Duck SCA: Project Group Basics

Summary: Learn the basics of the Projects Group feature Black Duck provides the ability to logically group all your projects, allowing you to organize which projects belong to which business unit while making it easier for you to view risk across the organization. Project groups can contain both projects and other project groups to provide a multi-level hierarchy. Black Duck's Project Groups feature manages access and roles for business units across your organization.

URL: blackduck.skilljar.com/black-duck-project-group-basics

Black Duck: Cloning Versions & Projects

Summary: This course walks through the steps and settings for cloning your Black Duck projects. Cloning is useful in a variety of contexts. Clones can be used to create new baseline BOMs, or they can serve as templates for testing various component adjustments. This course will show you how to clone versions and projects, and how to map a scan to a clone.

URL: blackduck.skilljar.com/black-duck-cloning-versions-projects

Black Duck: Self Guided Onboarding Part 3 - Scan Results & Reporting

Summary: For Black Duck Administrators, Developers, or Managers - you will be guided through working with scan results & generating reports.

URL: blackduck.skilljar.com/black-duck-self-guided-onboarding-part-3-scan-results-reporting

Black Duck SCA: Installation using Docker Swarm

Summary: This course will show you how to install Black Duck using Docker Swarm. A walkthrough for installing Docker CE is provided, followed by an installation tutorial for Black Duck. The Black Duck installation tutorial includes downloading and running the Black Duck containers, and locating Black Duck's configuration files and scripts.

URL: blackduck.skilljar.com/black-duck-installation-using-docker-swarm

Black Duck: Core Entities Guide

Summary: This article is a guide to some of the basic elements of Black Duck, their functions, and their relations. This course highlights some key aspects of Black Duck by describing some main functionality and how they relate to each other. It is beneficial to understand these relationships when navigating through Black Duck and managing results.

URL: blackduck.skilljar.com/black-duck-core-entities-guide

Introduction to Black Duck Solutions

Summary: Learn the benefits and risks of using Open Source software and how Black Duck solutions can help organizations manage the security, licensing, and operational risk that comes along with using it.

URL: blackduck.skilljar.com/introduction-to-black-duck-solutions

Black Duck SCA: Configure Security Risk Ranking

Summary: Black Duck SCA allows you to adjust the risk ranking for security vulnerabilities. Multiple vulnerability scores for a given vulnerability are displayed in the interface. If your company has a corporate policy that aligns with a security risk framework that differs from the default, you can now set the risk scoring in Black Duck SCA to match the risk profile used by your company.

URL: blackduck.skilljar.com/black-duck-configure-security-risk-ranking

Black Duck SCA: Setting Global Remediation Status

Summary: An introduction to using Global Remediation Status for improved BOM workflow. Specific security vulnerabilities may appear frequently in open source components that you use across projects. This can slow down the component review process if they are being marked for remediation individually. Setting a Global Remediation Status for frequently repeating vulnerabilities is a great way to improve review speed.

URL: blackduck.skilljar.com/black-duck-setting-global-remediation-status

Black Duck: Managing Users and Roles

Summary: Black Duck has well defined user roles and options to configure users' accounts. This course will walk you through the roles and configuration options. You will learn how to assign user roles, create groups, assign users and groups to projects, and assign roles to groups.

URL: blackduck.skilljar.com/black-duck-hub-managing-users-and-roles

Black Duck SCA: Scanning with Detect GUI

Summary: This beginners course will cover the basics of the Detect GUI tool for Black Duck SCA. The Detect CLI is the recommended method of using Detect.

URL: blackduck.skilljar.com/black-duck-sca-scanning-with-detect-gui

Introduction to Scanning Open Source Software with Black Duck

Summary: A Course for Black Duck Users Learn how to scan Open Source Software with Black Duck.

URL: blackduck.skilljar.com/introduction-to-scanning-open-source-software-with-black-duck

Black Duck: Detectors Introduction

Summary: Learn the role of Detector arguments in scan configurations Detectors can be leveraged to enhance Black Duck scans. This course will introduce advanced configurations that are possible with Detect, in order to use detectors to improve efficiency. We walk through two examples using the npm and Maven detectors.

URL: blackduck.skilljar.com/black-duck-detectors-introduction

Black Duck SCA: Watching Projects and Saving Searches

Summary: How to edit your watchlist and use saved searches The Black Duck dashboards can be customized to help you focus on important projects. Users can create project watch lists, and saved searches, in order to group projects and versions. This course will show you how to use the Black Duck dashboards to watch projects and create focused groups of project versions by using saved searches.

URL: blackduck.skilljar.com/black-duck-watching-projects-and-saving-searches

Black Duck SCA: Configuring Policy Management

Summary: This course will show you how to create, enable, and override Policy Rules. Policy rules are an important aspect of the Black Duck workflow. They can greatly improve the component review process. This short course will teach you to create policy rules, take advantage of Black Duck's default policy rules, and override policy violations as needed.

URL: blackduck.skilljar.com/black-duck-configuring-policy-management

Black Duck: Custom System Announcements

Summary: Learn how to create customized messages and announcements displayed to Black Duck users Starting with Black Duck 2020.8, administrators can create system- Duck users. The messages are written in Markdown, and can be displayed in multiple formats. This course describes how to create custom sign-on and post sign-on messages, along with their configuration options.

URL: blackduck.skilljar.com/black-duck-custom-system-announcements

Black Duck SCA: Identifying Unmatched Components

Summary: Learn about working with unmatched components in Black Duck Scan results end up being components in your Bill of Materials. However, sometimes components of scan results may not be identified in Black Duck. This course shows you how to manage these components to build an accurate Bill of Materials.

URL: blackduck.skilljar.com/black-duck-identifying-unmatched-components

Black Duck SCA: Navigating the Interface

Summary: An Introduction to the Black Duck SCA Interface. This course will give you a broad overview of the Black Duck SCA interface. New users who want to become familiar with Black Duck SCA will benefit. We'll cover the major features of the main dashboard, side navigation bar, and project version dashboard.

URL: blackduck.skilljar.com/black-duck-navigating-the-interface

Black Duck: Introduction to Scanning

Summary: Learn how to install Detect GUI and CLI and run your first scans. This course will show you how to use Detect Command Line Interface (CLI) tool and run your first scans. The course covers downloading the scan tool and running it with basic configurations. You will also learn about how Detect scans your code, and get introduced to some advanced scan configurations.

URL: blackduck.skilljar.com/black-duck-installing-synopsys-detect

Black Duck SCA: A Technical Introduction

Summary: This course introduces the components and overall functions of Black Duck SCA. Learn the technical fundamentals of Black Duck SCA from the overall function of the product to the relationship between it and the Black Duck SCA Knowledge Base. You will understand the code printing process and how the code prints are leveraged with the Black Duck SCA Knowledge Base to assess your code's security risk. Interactive tutorials assist in walking through a basic scan, and viewing risk in Black Duck SCA.

URL: blackduck.skilljar.com/black-duck-hub-a-technical-introduction

Black Duck SCA: From Configuration to First Results

Summary: This course is a condensed workflow that shows new users an overview of initial configuration to getting your first scan results. Black Duck is a versatile Software Composition Analysis tool. Users can scan code bases throughout the development process to identify components and vulnerabilities, monitor risk, ensure compliance, and more. This course will give new users a generic introduction of Black Duck by walking through some basic steps to create a user, run a first scan, and view results.

URL: blackduck.skilljar.com/black-duck-from-configuration-to-first-results

Black Duck: Self Guided Onboarding Part 1 - Getting Started & Configuration

Summary: For Black Duck Administrators - you will be guided through the Black Duck GUI configuration and setup. In this course, you will complete the configuration tasks necessary to ensure that the Black Duck GUI is, Security - User Authentication: Integrating with LDAP or SAML, Managing Users & Roles and Creating Projects.

URL: blackduck.skilljar.com/black-duck-self-guided-onboarding-part-1-getting-started-configuration

Black Duck SCA: Working with Scan Results

Summary: Learn how to review and perform actions on your Black Duck results. This course will familiarize you with the Bill of Materials for your Black Duck projects. You'll learn the process of removing, adding, and adjusting discovered components. You will also learn how to track remediation of security vulnerabilities that were discovered during scans.

URL: blackduck.skilljar.com/black-duck-hub-working-with-scan-results

Black Duck SCA: Attributing OSS in your Applications

Summary: Learn how to create Notices reports for Black Duck project versions. This course will outline the typical parameters of an open source license. It will contrast popular license types, and demonstrate how to meet your attribution requirements for any open source you're using. This course covers creating a Notices file for your project in Black Duck.

URL: blackduck.skilljar.com/black-duck-attributing-oss-in-your-applications

Black Duck SCA: Generating Reports

Summary: Learn how to leverage the available reports in Black Duck to provide insight into the open source components you're using and their associated risk. Black Duck provides various types of reports. We'll highlight both the standard vulnerability reports and customized Notices reports that comply with the attribution requirement of virtually all open source licenses that they use.

URL: blackduck.skilljar.com/black-duck-hub-generating-reports

Black Duck SCA SBOM Import

Summary: Learn how to generate a Bill of Materials by importing an SBOM file Black Duck allows users to upload an SBOM file and view the components as a Black Duck Bill of Materials. Users can monitor and query their results as if they were from a scan.

URL: blackduck.skilljar.com/black-duck-sbom-import

Black Duck SCA: Creating Projects

Summary: Learn how to create projects, map scans, and manage project groups & members. This course will show you how to create projects in the Black Duck UI, change project settings, and map a scan to a project. You will also learn how to add subprojects and manage access to projects in Black Duck.

URL: blackduck.skilljar.com/black-duck-creating-projects

Black Duck SCA: Copyright Statements

Summary: This course introduces the Black Duck tools necessary for managing copyright statements in your codebase. Copyright statements often must be checked, referenced, or reported when using Open Source Software. Black Duck can help you manage copyright statements associated with your OSS. You will learn how to view, create, edit, activate, and deactivate copyright statements.

URL: blackduck.skilljar.com/black-duck-copyright-statements

Black Duck SCA: Security Risk Remediation Strategy

Summary: This course will cover the Remediation Strategy recommendations for security risks found by Black Duck. This course will cover the Remediation Strategy recommendations for security risks found by Black Duck. Users will learn about actionable steps and considerations to work with vulnerable components.

URL: blackduck.skilljar.com/black-duck-security-risk-remediation-strategy

Black Duck SCA: SBOM Generation

Summary: Learn how to generate an SBOM in the Black Duck GUI. Black Duck allows for the creation of an SBOM within the user interface. SBOM is a standard format for tracking OSS in your software projects. Black Duck makes it very quick and easy to generate a Bill of Materials in this format.

URL: blackduck.skilljar.com/black-duck-sbom-generation

Black Duck SCA: Scanning Best Practices

Summary: Learn to structure your projects and set up scans using best practices. Black Duck scans must be managed in order to avoid unnecessary accumulation. Scanning best practices will ensure that you keep relevant scans and delete irrelevant ones. This course will teach you a template for how to structure your Black Duck projects, and configure your scans, in order to optimize your scan and review workflow.

URL: blackduck.skilljar.com/black-duck-scanning-best-practices

Black Duck: Self Guided Onboarding Part 2 - Scanning with Detect

Summary: For Black Duck Administrators or Developers - you will be guided through installing Detect & running your first scan. In this course, you will complete the installation and configuration tasks necessary to start scanning, Installing Detect, Scanning your codebase with Detect and Scanning best practices

URL: blackduck.skilljar.com/black-duck-self-guided-onboarding-part-2-scanning-with-detect

Black Duck SCA Admin Options and System Settings

Summary: Black Duck allows admins to adjust settings to fit their organization's requirements. These options can help with server maintenance, calibration of settings, and access management.

URL: blackduck.skilljar.com/black-duck-admin-options-and-system-settings

Black Duck SCA Scanning and Component Management (Learning Path)

Summary: This learning path covers the basics of scanning, managing component results, and common workflows.

URL: blackduck.skilljar.com/path/black-duck-sca-scanning-and-component-management

Black Duck SCA Security Risk Workflow (Learning Path)

Summary: The Black Duck SCA Security Risk Workflow learning path is designed for security professionals looking to understand the basic workflow of security risk. From producing scan results to remediating security risks, this path covers what you will need to know to discover risk and take actionable steps to secure your project.

URL: blackduck.skilljar.com/path/black-duck-security-risk-workflow

Black Duck SCA Vulnerability Management (Learning Path)

Summary: This series of courses cover viewing risk in your results and the suggested process to verify and address them to secure the software supply chain.

URL: blackduck.skilljar.com/path/black-duck-sca-vulnerability-management

Black Duck SCA in a Nutshell

Summary: Learn the benefits and risks of using Open Source software and how Black Duck SCA can help organizations manage the security, licensing, and operational risk that comes along with using it.

URL: blackduck.skilljar.com/introduction-to-black-duck-solutions

Black Duck SCA: Using Custom Scan Signatures

Summary: This course covers how and when to use Custom Scan Signatures to improve workflow. Custom scan signatures can be used to keep track of proprietary components in your bill of materials. They are also a useful tool for including any other components that may be excluded from your scans. This course will cover how to create custom scan signatures and use them to your advantage.

URL: blackduck.skilljar.com/black-duck-using-custom-scan-signatures

Black Duck: Managing Open Source Licenses

Summary: A short introduction to managing open source licenses with Black Duck. This course will show you how to view open source licenses in your projects. You will learn to create and edit custom licenses. Additionally, we'll cover editing and restoring Black Duck Knowledge Base licenses.

URL: blackduck.skilljar.com/black-duck-managing-open-source-licenses

Black Duck SCA: Using MFA

Summary: This course will cover how to setup MFA for their Black Duck server. This course will show users how to enable and setup multi-factor authentication on their Black Duck server. Using MFA is a great way to increase the security of your Black Duck data

URL: blackduck.skilljar.com/black-duck-sca-using-mfa

Black Duck SCA: Advanced License Management

Summary: This course will help you understand custom license families, terms, and license fulfillment in Black Duck. Black Duck has several advanced features involved in License Management. These can help suit business needs beyond simple license viewing and approval, and creating notices files. This course addresses three advanced features. It covers Custom License Families, Custom License Terms, and License Terms Fulfillment.

URL: blackduck.skilljar.com/black-duck-advanced-license-management

Black Duck: Discovering Open Source Snippets

Summary: Learn how to run Snippet Scans and view their results Black Duck is able to scan your code for open source snippets, small pieces of open source code that can easily go undiscovered. This course will describe how open source snippets enter your code. We will also walk through the process of detecting & managing them with Black Duck.

URL: blackduck.skilljar.com/black-duck-discovering-open-source-snippets

Black Duck SCA: Access Token Management for Admins

Summary: Learn how to manage access tokens as an admin User Administrators of the Black Duck system need a mechanism to maintain and control access to Black Duck via access tokens. This course will walk through how to purge tokens from the Access Token management tool.

URL: blackduck.skilljar.com/black-duck-access-token-management-for-admins

Black Duck Administration Competency Series

Summary: Black Duck Administration Competency Series

URL: blackduck.skilljar.com/black-duck-administration-competency-series

Black Duck: Custom Fields

Summary: This course will teach you how Custom Fields can improve your component review process. Your organization may have aspects of a project that are important to track during the component review process, but are not represented in Black Duck. Custom Fields allow you to create your own parameters to track what's important to you. This course will show you how to create and view Custom Fields in Black Duck.

URL: blackduck.skilljar.com/black-duck-custom-fields

Black Duck SCA: Legal OSS Policy Starter Kit

Summary: Learn about leveraging policy for managing License Risk. This article is intended to give clients a basic policy configuration for License Risk when first starting with Black Duck, or if no formal Legal OS Policy has been defined within their organization.

URL: blackduck.skilljar.com/black-duck-legal-oss-policy-starter-kit

Black Duck SCA: SBOM Templates

Summary: This course covers how to create and use Black Duck SCA's SBOM Templates feature. Black Duck SCA's SBOM Template feature makes it easy to create and configure templates for SBOM reports. This course will cover how to create and use templates.

URL: blackduck.skilljar.com/black-duck-sbom-templates

Black Duck SCA: Unmatched Origins Feature and Scan Identification

Summary: Learn about using Black Duck's Unmatched Origins Feature and Package Manager Scan Identification to manage internally developed components. This course describes how to leverage Black Duck's Unmatched Origins component management feature for automatic identification of internally developed components via Package Manager scans.

URL: blackduck.skilljar.com/black-duck-unmatched-origins-feature-and-scan-identification

Black Duck SCA: Jenkins Integration **(Integration)**

Summary: Integrate Black Duck SCA with Jenkins using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Black Duck SCA with Jenkins. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/black-duck-sca-jenkins-integration

Black Duck SCA: GitHub Integration Using Security Scan (Integration)

Summary: Integrating Black Duck SCA with GitHub using Security Scan. The purpose of this guide is to be a one-stop-shop for integrating Black Duck SCA with GitHub using Security Scan.

URL: blackduck.skilljar.com/black-duck-sca-github-integration

Black Duck SCA: Azure DevOps Integration (Integration)

Summary: Integrate Black Duck SCA with Azure DevOps using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Black Duck SCA with Azure DevOps. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/black-duck-sca-azure-devops-integration

Black Duck SCA Notification Settings

Summary: Learn how to use Black Duck's notification settings and available features. Black Duck allows users to control notifications and enables admins to select the types of notifications for the system to produce. Tune these settings to help reduce noise and increase server performance.

URL: blackduck.skilljar.com/black-duck-notification-settings

Black Duck SCA: GitHub Action Basics

Summary: This course will cover how to install, configure, and run the Black Duck GitHub Action for Black Duck SCA. Learn how to integrate Black Duck SCA into your GitHub developer workflow. Scans are launched automatically from your CI workflow, and developer feedback is provided through comments on pull requests - including upgrade guidance for insecure components - and branch protection policies (complimented with generated Fix PRs) prevent security vulnerabilities from being introduced to your main branch.

URL: blackduck.skilljar.com/black-duck-sca-github-action-basics

Black Duck SCA: SBOM Import Custom Component Auto-Creation

Summary: This course covers how to use Black Duck's Custom Component Auto-Creation feature for Unmatched Components when importing an SBOM Black Duck's Custom Component Auto-Creation feature automates the creation and mapping of custom components for unmatched components when importing an SBOM.

URL: blackduck.skilljar.com/black-duck-sbom-import-custom-component-auto-creation

Black Duck: Snippet Scanning and New Triage Workflow

Summary: A Course for Black Duck Code Scanners. Black Duck offers the ability to scan your codebase to identify code snippets that match portions of code from components in the Knowledge Base. Reviewing discovered snippets is a different process than the typical BOM component review. This course will cover viewing your snippet results and how to triage them individually, as well as in bulk.

URL: blackduck.skilljar.com/black-duck-snippet-scanning-and-new-triage-workflow

Black Duck SCA SAML Integration

Summary: A short introduction to SAML on Black Duck SCA. This tutorial will show you how to configure single sign-on (SSO) via SAML for Black Duck. A brief walkthrough of a basic Okta setup is provided, followed by a tutorial that covers the steps to connect Black Duck to Okta. The SAML configuration is Black Duck is general, so the Black Duck steps can be used for your SSO service of choice.

URL: blackduck.skilljar.com/black-duck-saml-integration

Black Duck SCA: Bridge CLI Basics

Summary: This course will cover basic usage of the Bridge tool to run a scan. This course will cover the basics of running a scan using the Bridge tool via CLI. The basic calls and setup are covered here to get you started.

URL: blackduck.skilljar.com/black-duck-synopsys-bridge-cli-basics

Black Duck SCA: Configuring LDAP Integration

Summary: How to configure the LDAP options in Black Duck. This course will show you how to facilitate LDAP-based authentication in Black Duck. You will learn the prerequisites and configuration steps necessary to integrate your Black Duck server with your LDAP environment. LDAP user and group management configuration in Black Duck are covered as well.

URL: blackduck.skilljar.com/black-duck-hub-configuring-ldap-integration

Black Duck: Scanning Docker Images using Docker Inspector

Summary: This course introduces the settings and techniques used for scanning Docker Images using Docker Inspector. Docker Inspector can be used to scan Docker images, so the results can be reviewed in Black Duck. This course will show you how to run a basic Docker image scan. It will also cover various Detect properties that can be used to scan only certain layers of the Docker image. This tool can be used for customers without access to Secure Container Scanning.

URL: blackduck.skilljar.com/black-duck-scanning-docker-images

Black Duck SCA: CSV Scan Archive

Summary: This tutorial will cover creating and downloading a CSV scan file that lists all files that were scanned. Black Duck SCA customers can create a CSV file of all files that were scanned. This file may be used for keeping track of all files scanned or audit purposes.

URL: blackduck.skilljar.com/black-duck-sca-csv-scan-archive

Black Duck SCA: Scanning with Jenkins

Summary: How to configure Black Duck scans in Jenkins. In this course, you will learn how to add scanning to your Jenkins projects. The interactive tutorial will walk through downloading and setting up the Detect integration for Jenkins. We will conclude with with passing scan properties to Detect through Jenkins.

URL: blackduck.skilljar.com/black-duck-jenkins-integration

Black Duck SCA: Fix PR Overview Using Black Duck Security Scan

Summary: This course will be a brief overview of the Fix PR feature for integrations using the Security Scan Action in GitHub as an example. This introductory overview will walk through the steps of a basic workflow for a user to generate a Fix PR. The example will use GitHub but the process will be similar for other CI tools.

URL: blackduck.skilljar.com/black-duck-sca-fix-pr-overview-using-black-duck-security-scan

Black Duck: Secure Container Scanning Basics

Summary: This course will cover running a basic Secure Container scan, its requirements, and its benefits. This course will help you getting started with Secure Container scanning and viewing the results in a Container BOM. This method of scanning produces an accurate Bill of Materials organized by image layer to easily identify and locate risk.

URL: blackduck.skilljar.com/black-duck-secure-container-scanning-basics

Black Duck SCA: GitLab Integration (Integration)

Summary: Integrate Black Duck SCA with GitLab using Black Duck Security Scan or the Bridge CLI. The purpose of this guide is to be a one-stop-shop for integrating Black Duck SCA with GitLab. It covers both the recommend approach using the Black Duck Security scan and the alternative option of using the Bridge CLI.

URL: blackduck.skilljar.com/black-duck-sca-gitlab-integration

Black Duck SCA License and Compliance Workflow (Learning Path)

Summary: This learning path includes courses to show users how to use Black Duck SCA for legal and industry compliance, as well as license management.

URL: blackduck.skilljar.com/path/black-duck-sca-license-and-compliance-workflow

Black Duck SCA Lightweight Scanning (Learning Path)

Summary: The Black Duck SCA Lightweight Scanning learning path is designed for security professionals looking to leverage lightweight scan tools. These tools add risk detection earlier in the build process, whether that be by automated scan or performed manually by a developer looking to quickly check a dependency.

URL: blackduck.skilljar.com/path/black-duck-lightweight-scanning

Black Duck SCA SBOM Reporting (Learning Path)

Summary: The courses in this learning path cover features for SBOM report generation, tuning, and importing.

URL: blackduck.skilljar.com/path/black-duck-sca-sbom-reporting

Scanning for C and C++ Projects using Black Duck

Summary: This course will walk you through using the Black Duck Coverity Build Capture tool. Creating an accurate Bill of Materials for C and C++ projects can be challenging. The Black Duck C/C++ tool does not require a Coverity license, and it can be used to scan your C/C++ projects to create a Bill of Materials in Black Duck.

URL: blackduck.skilljar.com/scanning-for-c-and-c-projects-using-black-duck

Introduction to Code Sight with Black Duck SCA

Summary: This tutorial will help you understand how using Code Sight can help developers when working with Black Duck SCA. This tutorial will help you understand how using Code Sight can help developers when working with Black Duck SCA.

URL: blackduck.skilljar.com/introduction-to-code-sight-with-black-duck-sca

Black Duck: Infrastructure-As-Code Scanning

Summary: Learn how to scan for IaC security issues and view results using Black Duck. The Black Duck IaC (Infrastructure as Code) scan mode is a simple way to detect infrastructure and deployment method issues in your configuration files. This course will walk through how to run IaC scans and view the results in Black Duck.

URL: blackduck.skilljar.com/black-duck-infrastructure-as-code-scanning

Black Duck Alert: Managing Notifications

Summary: Learn how to setup streamlined notifications with Black Duck Alert. Black Duck Alert allows for the sharing of Hub notifications, like vulnerability status changes and policy violations, through a number of distribution channels. This course will cover the process of connecting to your Black Duck server, and setting up a distribution channel for your notifications. We will also cover some details about Alert user management.

URL: blackduck.skilljar.com/black-duck-alert-managing-notifications

Black Duck: Configurable Individual File Matching

Summary: Learn how to configure and run Individual File Matching during your scans Prior to Black Duck 2020.2, a small set of file extensions were matched individually by default during scans. This is no longer the default behavior, however users do have the option to enable it. This course will explain Individual File Matching in more detail and walk you through the steps to enable it in your scans.

URL: blackduck.skilljar.com/black-duck-configurable-individual-file-matching

Black Duck SCA: Rapid Scan

Summary: An Introduction to Black Duck rapid scanning. This course describes how to setup and run Black Duck rapid Scans with Detect. It describes the function and use case for Rapid Scanning on Black Duck. An interactive tutorial will walk you through your first rapid scan.

URL: blackduck.skilljar.com/black-duck-rapid-scan

Black Duck SCA: Managing Deep License Data

Summary: This short course will show you how to use Black Duck's deep license data features. Deep license data, also known as embedded licenses, can be present in your OSS components.This course will show you how to enable deep license data tracking in your BOM. You will learn to scan for embedded licenses using Detect and view the data in your BOM.

URL: blackduck.skilljar.com/black-duck-managing-deep-license-data

Black Duck SCA SCM Integration

Summary: Learn how to setup and use Black Duck's SCM Integration feature. Black Duck's SCM Integration feature allows for the direct communication with SCM Providers to onboard repositories individually or in bulk. Mapping repos from supported SCM Providers to Black Duck Projects and Versions will give quick and easy visibility to the repos' composition and risk.

URL: blackduck.skilljar.com/black-duck-scm-integration

Installing an On-premise Black Duck KnowledgeBase

Summary: Install your on-prem KnowledgeBase and connect to your Black Duck instance. This course will show you how to download Black Duck KnowledgeBase OnPrem artifacts, set up your KnowledgeBase Server, and set up a Black Duck instance connected to the KB OnPrem.

URL: blackduck.skilljar.com/installing-an-on-premise-black-duck-knowledgebase

Black Duck: Connecting to the Report Database

Summary: This course walks through the steps for connecting to the Black Duck Report Database. The Black Duck Report Database can be used to generate customized reports. This course will show you how to connect to the Report Database. Once connected, you will be able to leverage it to extract the data you want and determine your own display tools.

URL: blackduck.skilljar.com/black-duck-report-database

Black Duck: Vulnerability Impact Analysis

Summary: How to scan and view reachable vulnerabilities in Black Duck. Vulnerability Impact Analysis can disclose reachable vulnerabilities in your code base for supported languages. This course will describe how to scan for vulnerability impact using Detect CLI and Detect Desktop. You will also learn how to view and reachable vulnerabilities in Black Duck.

URL: blackduck.skilljar.com/black-duck-vulnerability-impact-analysis

Black Duck SCA Heatmaps

Summary: Learn how to use Black Duck's Heatmap feature Black Duck's Heatmap feature allows users to view their scan activity. The heatmap offers a high level overview of scan activity on the server for performance optimization strategies.

URL: blackduck.skilljar.com/black-duck-heatmaps

BLACK DUCK BINARY ANALYSIS

BLACK DUCK BINARY ANALYSIS

Learn about Black Duck Binary Analysis

Identify open source supply chain risks even when you don't have access to the code.

Baseline

- **Basic deployment** Core functionality is installed and minimally configured. Usage may be ad hoc, with little to no automation or integration. Visibility is limited to basic metrics or logs.

Emerging

- **Ramped deployment** Key integrations with CI/CD pipelines are established. Automation begins for routine tasks like scanning or policy enforcement. Teams start aligning product use with development workflows.

Maturing

- **Advanced deployment** The solution is widely deployed across teams or projects. Automation is policy-driven and consistent. Integration with developer tools and environments is robust. Dashboards and reporting begin to inform decisions.

Optimizing

- **Proficient "reference" deployment** Full integration across the SDLC. Analytics dashboards provide actionable insights. Feedback loops drive continuous improvement. Manual intervention is rare. Usage is proactive, with predictive capabilities and strategic alignment.

Introduction to Black Duck Binary Analysis BDBA Standalone

Summary: Black Duck Binary Analysis (BDBA) is an automated software composition analysis tool that enables organizations to audit open source software compliance, vulnerabilities in third-party code, and achieve governance over open source. In this video, we will talk about the features and capabilities of the product, and why you should be using binary analysis to detect vulnerabilities and components from applications. This Introduction is for those users using BDBA standalone not Integrated with Black Duck.

URL: blackduck.skilljar.com/introduction-to-protecode-sc

Black Duck Binary Analysis: Introduction to Cyber Supply Chain

Summary: This course is a quick walkthrough on how the cyber supply chain works Black Duck Binary Analysis is a great tool for discovering known vulnerabilities from the software packages you use when building your software. This micro-course introduces the Cyber Supply Chain and walks you through the challenges you may face.

URL: blackduck.skilljar.com/black-duck-binary-analysis-introduction-to-cyber-supply-chain

Black Duck Binary Analysis: Vulnerabilities and Code Decay

Summary: Learn about vulnerabilities and code decay by walking through this course Vulnerabilities do not appear from thin air, but they are introduced unknowingly when the software is being built. Code decays over time, and new vulnerabilities are discovered all the time. This micro-course talks about code decay and what it means regarding vulnerabilities.

URL: blackduck.skilljar.com/black-duck-binary-analysis-vulnerabilities-and-code-decay

Black Duck Binary Analysis: Key Features

Summary: This course is a quick walkthrough on BDBA key features. Black Duck Binary Analysis is a software composition analysis platform that addresses the challenges of an increasingly complex and fragmented cyber supply chain. This micro-course walks through the key features of BDBA and explains how the tool can help both builders and buyers within the cyber supply chain.

URL: blackduck.skilljar.com/black-duck-binary-analysis-key-features

Black Duck Binary Analysis: A Walkthrough

Summary: This course is a quick walkthrough of the BDBA user interface. Using Black Duck Binary Analysis is quite simple and intuitive. Uploading software packages is easy, and you get to see the results very quickly. This micro-course is a walkthrough of the basic functions and the web UI.

URL: blackduck.skilljar.com/black-duck-binary-analysis-a-walkthrough

Black Duck Binary Analysis: Uploading and Analysis Overview

Summary: This course is a quick walkthrough on how to upload binary files in BDBA Uploading binary files in BDBA is where your analysis starts. This micro-course walks you through different options of doing the upload, looking at the analysis overview, and how you should interpret all the available analysis details once the scan has finished.

URL: blackduck.skilljar.com/black-duck-binary-analysis-uploading-and-analysis-overview

Black Duck Binary Analysis: User Profile and Settings

Summary: This course is a quick walkthrough of the user profile and the individual user settings. Before you start uploading binary packages, you may want to check your user profile and the settings for your user. Your profile is also a great place to see all the software packages you have uploaded yourself, and you can modify your authentication settings from the same place as well.

URL: blackduck.skilljar.com/black-duck-binary-analysis-user-profile-and-settings

Black Duck Binary Analysis: Groups

Summary: This course is a walkthrough of group management in Black Duck Binary Analysis. Managing individual users in any platform can be a pain. In Black Duck Binary Analysis, you can create groups and subgroups for different products, different development versions, and so on. Managing users in groups enables your users to be more productive, since they won't be seeing analysis results from binaries that are not their responsibility. This interactive course walks you through how to manage groups in BDBA.

URL: blackduck.skilljar.com/black-duck-binary-analysis-groups

Black Duck Binary Analysis: Scan List Operations

Summary: This course is a quick walkthrough of the scan list in BDBA. All your ongoing and completed scans are in a scan list on the main page of your group. The list contains scans from all the group members, and it shows if the binary file contains vulnerabilities, shows how many components there are, and so on. This micro-course is a walkthrough of the scan list and what operations you can do with it.

URL: blackduck.skilljar.com/black-duck-binary-analysis-scan-list-operations

Black Duck Binary Analysis: Vulnerability Triage

Summary: This course is a quick walkthrough on how to triage vulnerabilities in BDBA. When your binary analysis reveals vulnerabilities from the used components, you should always do a risk assessment. Not all vulnerabilities are equal, and some may not even affect you. This micro-course is a walkthrough of how you can triage vulnerabilities in BDBA, and which details you should factor in with your decisions.

URL: blackduck.skilljar.com/black-duck-binary-analysis-vulnerability-triage

Black Duck Binary Analysis: Information Leakage

Summary: This course is a quick walkthrough on Information Leakage in BDBA. Information Leakage is a feature in BDBA that detects unintentionally leaked data from the scanned binaries. This sensitive data may contain access tokens, email addresses, or encryption keys. This micro-course walks you through how information leakage feature works in BDBA.

URL: blackduck.skilljar.com/black-duck-binary-analysis-information-leakage

Black Duck Binary Analysis: Reporting

Summary: This course is a quick walkthrough on various reporting options in BDBA. Once you have done the binary analysis and finished with the triage phase, you should forward the analysis results to the appropriate teams and people. This micro-course is a walkthrough of different reporting options available in BDBA.

URL: blackduck.skilljar.com/black-duck-binary-analysis-reporting

Black Duck Binary Analysis: Support for Black Duck Security Advisories

Summary: This course is a quick walkthrough of the new Black Duck Security Advisory support in Black Duck Binary Analysis. Running a binary analysis with BDBA now shows you Black Duck Security Advisories details when available. Black Duck Security Advisories provide more accurate information on vulnerable software version ranges to help users get more out of NVD data.

URL: blackduck.skilljar.com/black-duck-binary-analysis-support-for-black-duck-security-advisories

Black Duck Binary Analysis: Account Settings and Options

Summary: This course is a walkthrough of the account settings and options in Black Duck Binary Analysis. When you start using Black Duck Binary Analysis in your organization for the first time, it is recommended to go through your account settings to make sure everything is set according to your requirements and processes. Account settings allow you to change vulnerability matching options, default roles and permissions, API key details, and much more.

URL: blackduck.skilljar.com/black-duck-binary-analysis-account-settings-and-options

Black Duck Binary Analysis Essentials (Learning Path)

Summary: The Black Duck Binary Analysis Essentials learning path is designed for new users who are getting to know BDBA and the world of known vulnerabilities. This path if focused to new users who want to learn about cyber supply chain and vulnerabilities in general in addition to BDBA capabilities and features. You will learn how to upload binary files, interpret the analysis results, triage vulnerabilities, produce reports, use custom data templates, and utilize the information leakage feature. This learning path contains the BDBA Lab course as well.

URL: blackduck.skilljar.com/path/black-duck-binary-analysis-essentials

Black Duck Binary Analysis Integrated: Scan with Detect GUI

Summary: This course walks you through how to use BDBA Integrated with Detect GUI. This course walks you through how to use BDBA Integrated with Detect GUI.

URL: blackduck.skilljar.com/black-duck-binary-analysis-integrated-scan-with-synopsys-detect-gui

Black Duck Binary Analysis Integrated: Scan with Detect Command Line

Summary: This course walks you through how to use BDBA Integrated with Detect via Command Line. This course walks you through how to use BDBA Integrated with Detect via Command Line.

URL: blackduck.skilljar.com/black-duck-binary-analysis-integrated-scan-with-synopsys-detect-command-line

Black Duck Binary Analysis Integrated: Examining the Results

Summary: This course walks you through how to inspect and adjust the binary analysis results in Black Duck Hub. This course walks you through how to inspect and adjust the binary analysis results in Black Duck Hub.

URL: blackduck.skilljar.com/black-duck-binary-analysis-integrated-examining-the-results

Black Duck Binary Analysis Essentials

Summary: BDBA Essentials covers the basic concepts of binary analysis, and walks through the everyday usage of Black Duck Binary Analysis. This course offers a holistic overview of core product features, functionality and common use cases when used as a standalone installation either as an in-house appliance or hosted service. You will first learn the product conceptual framework followed by a functional walk-through. BDBA Essentials consists of theory in text format and interactive tutorials that will take you through the product.

URL: blackduck.skilljar.com/protecode-sc-essentials

Black Duck Binary Analysis: User Management and Permissions

Summary: This course is a walkthrough of user management in BDBA.This course is a walkthrough of user management, user permissions, and other administrative functions regarding new and existing users in Black Duck Binary Analysis. An interactive tutorial walks you through how the user roles work, how you can invite new users, place them in groups, and organize your userbase with the built-in options and settings.

URL: blackduck.skilljar.com/black-duck-binary-analysis-user-management-and-permissions

Black Duck Binary Analysis: User Management and Default Roles

Summary: This course walks through the new and improved user management options when creating new users in Black Duck Binary Analysis. Defining roles for a new user in Black Duck Binary Analysis is now easier due to new default role options in the User Management section. This course walks you through how the new options work, and how you can modify the user after creating them.

URL: blackduck.skilljar.com/black-duck-binary-analysis-user-management-and-default-roles

Black Duck Binary Analysis: Detected Components

Summary: This course is a quick walkthrough of the detected components in BDBA. Once you have uploaded a binary file in BDBA, you get the analysis overview. All the vulnerabilities reside in the components, so that's where we are focusing on with this micro-course. You'll learn whichdetails are relevant for you, how to look at the discovered components, and understand the upgrade guidance.

URL: blackduck.skilljar.com/black-duck-binary-analysis-detected-components

Black Duck Binary Analysis: API Basics

Summary: This course is a quick walkthrough of API basic usage in Black Duck Binary Analysis. Using Black Duck Binary Analysis is quite straightforward via the Web UI, but it is not a good way to automate your regular scans. Using the API enables you to automate nightly uploads and scans, saving you time and trouble with such repetitive tasks. This course walks you through how the API works, and shows you a few examples on how to start using the BDBA API.

URL: blackduck.skilljar.com/black-duck-binary-analysis-api-basics

Black Duck Binary Analysis: Custom Data and Custom Data Templates

Summary: This course is a quick walkthrough on the Custom Data feature in BDBA. Custom Data is a method of categorizing and grouping your scanned binaries. You can apply the feature before you even upload any binary files and assign custom data to certain binary files. This micro-course walks you through how custom data and custom data templates are used in BDBA.

URL: blackduck.skilljar.com/black-duck-binary-analysis-custom-data-and-custom-data-templates

Black Duck Binary Analysis: How to Enable API Key Authentication

Summary: Basic authentication is no longer supported with BDBA API in hosted platform. This course walks you through how to enable API key authentication. Black Duck Binary Analysis deprecated the basic authentication option for API access in 2020.09 release in the hosted platform. This course covers the API key authentication process that replaces the less secure basic authentication option when using BDBA API.

URL: blackduck.skilljar.com/black-duck-binary-analysis-how-to-enable-api-key-authentication

Black Duck Binary Analysis: Rapid Scan Static Support

Summary: This course is a quick walkthrough on how the Rapid Scan Static works in Black Duck Binary Analysis. With this new addition of Rapid Scan Static support, you are able to utilize the power of a lightweight SAST scanner for finding vulnerabilities in source code. If the analyzed binary has web applications, this new feature is able to find vulnerabilities from the source code and show them as meaningful results with remediation suggestions.

URL: blackduck.skilljar.com/black-duck-binary-analysis-rapid-scan-static-support

Black Duck Binary Analysis: Linux Kernel Module Support

Summary: This course is a quick walkthrough on how BDBA detects individual Linux kernel modules. When scanning binaries with BDBA, you get a list of components and their vulnerabilities and licenses. With this new support for Linux kernel modules in 2021.12, you can see individual kernel modules listed in the scan results. You also get additional vulnerability details related to missing modules and vulnerabilities associated with them.

URL: blackduck.skilljar.com/black-duck-binary-analysis-linux-kernel-module-support

Black Duck Binary Analysis: Docker Container Scanning

Summary: This course is a walkthrough on how to upload, scan, and inspect Docker Registry containers in Black Duck Binary Analysis web interface. In addition to regular executables and disk images, Black Duck Binary Analysis supports Docker container scanning as well. You can fetch the container via the Web UI, upload it manually from your local disk, or use the API for fetching and scanning the container.

URL: blackduck.skilljar.com/black-duck-binary-analysis-docker-container-scanning

Black Duck Binary Analysis: API Fetch for Docker Registry and Custom Data

Summary: BDBA supports API fetch for Docker Registry, and this course walks through the steps and different options available. With the correct syntax, you are able to define the used BDBA instance, your group, username, and the image from Docker Registry without opening your browser. By default, the Docker Registry API Fetch downloads the latest release, but you can use Docker tags to define other versions as well. It is easy to automate containerscanning by using the API.

URL: blackduck.skilljar.com/black-duck-binary-analysis-api-fetch-for-docker-registry-and-custom-data

Black Duck Binary Analysis: SBOM Annotations

Summary: This course is a quick walkthrough on how the SBOM annotations work in BDBA. When you scan a binary package with BDBA, you get extensive analysis results where you can look at all the components, their details, and vulnerabilities. BDBA has introduced SBOM annotations as a new feature for making your reports more detailed. This course walks through the usage of SBOM annotations in BDBA.

URL: blackduck.skilljar.com/black-duck-binary-analysis-sbom-annotations

Black Duck Binary Analysis: How to create a Vendor Vulnerability

Summary: BDBA offers the ability to add custom vulnerabilities to both proprietary and OSS components, and this course shows how to create them. Black Duck Binary Analysis offers the ability to add vulnerabilities to either your own proprietary components or existing OSS components by using CPE. You can add multiple different vulnerabilities to the database, and give unique vulnerability IDs for each vulnerability. You can also determine a CVSSv2/v3 equivalent score to your own vulnerability.

URL: blackduck.skilljar.com/black-duck-binary-analysis-how-to-create-a-vendor-vulnerability

Black Duck Binary Analysis: How to create a Vendor Component

Summary: Black Duck Binary Analysis offers the ability to add fingerprints for your own components, and make them detectable in your binary scans. This course will show you how to upload a vendor component, and demonstrate how the process of modifying the component properties works. It will also show you an example of how the vendor component is detected during an analysis.

URL: blackduck.skilljar.com/black-duck-binary-analysis-how-to-create-a-vendor-component

Black Duck Binary Analysis: From Install to First Results

Summary: This course is a walkthrough for new BDBA Appliance users on how to set up the system and get first results. Black Duck Binary Analysis Appliance is a standalone version of BDBA. The VM image is downloaded locally, and configured to operate either on a local computer, or serving a larger user base in an internal network. This course is a walkthrough of the main steps on how to get your BDBA appliance running and how to get your first results.

URL: blackduck.skilljar.com/black-duck-binary-analysis-from-install-to-first-results

Black Duck Binary Analysis Advanced (Learning Path)

Summary: The Black Duck Binary Analysis Advanced learning path is designed for more seasoned users of BDBA. This learning path doesn't walk through any of the basics or theory of binary analysis but is focused on the more advanced topics and account management. With the help of this learning path, you'll learn about BDBA API usage, supported components, account settings, group management, and docker container scanning. This learning path contains the BDBA Lab course as well.

URL: blackduck.skilljar.com/path/black-duck-binary-analysis-advanced

Black Duck Binary Analysis Appliance (Learning Path)

Summary: The Black Duck Binary Analysis Appliance learning path is designed for BDBA virtual appliance users. This learning path focuses only on the appliance-related topics for BDBA and introduces a few key features you should know about when working with the appliance. You will learn about Kubernetes deployment, initial setup options, server monitoring, virtual appliance migration, and how to optimize and troubleshoot your BDBA appliance. This learning path contains the BDBA Lab course as well.

URL: blackduck.skilljar.com/path/black-duck-binary-analysis-appliance

Black Duck Binary Analysis: Lab Course

Summary: This is a course for Black Duck Binary Analysis lab exercises. This course provides you different level lab works you can practice in a cloud-based VM environment. In addition to the step-by-step labs, you can play around with the BDBA appliance freely and experiment with various BDBA features. While the course provides you the needed details for executing the labs, you need have knowledge on BDBA in order to get the most of this labs course. It is highly recommended you have finished a considerable amount of BDBA courses before doing the labs.

URL: blackduck.skilljar.com/black-duck-binary-analysis-lab-course

Black Duck Binary Analysis: Initial Setup Options for Appliance

Summary: This course is a walkthrough of BDBA appliance initial setup options. When you use the hosted version of BDBA, many of the setup options are readily automated for you. With the on-premise appliance, you have much more options available to customize your BDBA experience. This interactive course walks you through the initial setup options for the BDBA appliance.

URL: blackduck.skilljar.com/black-duck-binary-analysis-initial-setup-options-for-appliance

Black Duck Binary Analysis: Analysis Configuration File Usage

Summary: This course is a quick walkthrough on how to utilize the .bdba.yaml file in your BDBA scans. When uploading and scanning binaries in BDBA, in normal situations you must do all the version changes and vulnerability triaging manually. BDBA currently supports an extra file for Analysis Configuration which you can use to automatically determine component versions and triage vulnerabilities.

URL: blackduck.skilljar.com/black-duck-binary-analysis-analysis-configuration-file-usage

Black Duck Binary Analysis: Virtual Appliance Migration

Summary: This course is a quick walkthrough on how to migrate your old Debian 9 BDBA Virtual Appliance to new Debian 11. BDBA is dropping support for Debian 9 later in 2022. It is highly recommended to migrate your virtual appliance to Debian 11 before the support for Debian 9 ends. This micro course shows you how to do the migration in browser, and it gives you documentation links on how to do it via the API.

URL: blackduck.skilljar.com/black-duck-binary-analysis-virtual-appliance-migration

Black Duck Binary Analysis: How to set up server monitoring

Summary: This course walks you through how to set up server monitoring for your on-premise BDBA appliance. When running the BDBA appliance in your organization, it can be helpful to establish a monitoring environment to see how the appliance is doing. The monitoring tools enable you to see a lot of details about the state of the appliance.

URL: blackduck.skilljar.com/black-duck-binary-analysis-how-to-set-up-server-monitoring

Black Duck Binary Analysis: Troubleshooting and Optimizing the Appliance

Summary: This course walks you through various troubleshooting and optimization options that are available when using BDBA appliance. As the appliance administrator, you can download log files for inspecting them yourself, or sending them to the BDBA experts at our support. There are a lot of different settings for optimizing the appliance, and this interactive course walks you through those options in BDBA.

URL: blackduck.skilljar.com/black-duck-binary-analysis-troubleshooting-and-optimizing

DEFENSICS

Learn about Defensics Fuzz Testing

Identify defects and zero-day vulnerabilities in services and protocols.

Baseline ■ □ □ □

- **Basic deployment** Core functionality is installed and minimally configured. Usage may be ad hoc, with little to no automation or integration. Visibility is limited to basic metrics or logs.

Emerging ■ ■ □ □

- **Ramped deployment** Key integrations with CI/CD pipelines are established. Automation begins for routine tasks like scanning or policy enforcement. Teams start aligning product use with development workflows.

Maturing ■ ■ ■ □

- **Advanced deployment** The solution is widely deployed across teams or projects. Automation is policy-driven and consistent. Integration with developer tools and environments is robust. Dashboards and reporting begin to inform decisions.

Optimizing ■ ■ ■ ■

- **Proficient "reference" deployment** Full integration across the SDLC. Analytics dashboards provide actionable insights. Feedback loops drive continuous improvement. Manual intervention is rare. Usage is proactive, with predictive capabilities and strategic alignment.

Introduction to Defensics ■ □ □ □

Summary: In this video, you will learn what Defensics fuzzing is all about. Fuzzing is a method of software testing that uncovers failure modes and unknown vulnerabilities by deliberately sending malformed inputs to a target. Because itâ€™s a common technique utilized by hackers, our Fuzz Testing employs dynamic, black box testing, meaning it requires no source code, to simulate real-life scenarios. We will talk about the features and capabilities of the product, and why you should be using fuzz testing to eliminate bugs and vulnerabilities in your products.

URL: blackduck.skilljar.com/introduction-to-defensics

Defensics: Get Started with Defensics Testing ■ □ □ □

Summary: This course goes through a basic checklist when starting Defensics testing. You'll find important tips on how to get your tests going. Starting Defensics testing can be a very easy task, or a bit more challenging one. It all depends on the environment, test target, and the protocol at hand. This course addresses several important details on how to get your testing going smoothly with Defensics.

URL: blackduck.skilljar.com/defensics-get-started-with-defensics-testing

Defensics: Fuzzing Guidelines ■ □ □ □

Summary: This course walks through important guidelines for fuzz testing. Fuzz testing is usually interpreted as intrusive from the target point of view. There are some important guidelines you should follow when doing fuzz testing. This course walks through some scenarios and guidelines that you should keep in mind when doing fuzz testing with Defensics.

URL: blackduck.skilljar.com/defensics-fuzzing-guidelines

Defensics: How to Access Arena and Download Defensics ■ □ □ □

Summary: This course walks you through how to download Defensics from the Download Arena. One way to download Defensics is to access the Download Arena. In addition to Defensics installer, test suites and other downloadable items are available in the Download Arena. This course uses an interactive tutorial to walk through the steps of downloading Defensics.

URL: blackduck.skilljar.com/defensics-how-to-access-arena-and-download-defensics

Defensics: How to Download a License from Community ■ □ □ □

Summary: This course walks you through how to download a Defensics license from the Community. This course describes what steps you have to take when downloading a Defensics license from the Community. In addition to just downloading a license, you may have the ability to adjust the amount of seats per license, re-host a license, and create multiple licenses.

URL: blackduck.skilljar.com/defensics-how-to-download-a-license-from-community

Defensics: How to Download Defensics from our Community

Summary: This course walks you through how to download Defensics from our Community. Defensics needs to be installed locally prior to using it, and it can be downloaded from our Community. In addition to Defensics installer, you are able to download test suite install files from the Community as well. This course walks you through the process with the help of an interactive tutorial.

URL: blackduck.skilljar.com/defensics-how-to-download-defensics-from-synopsys-community

Defensics: How to Get Your Flex Server Running

Summary: This course walks you through how to get your Flex license server running and connected to Defensics. Flex Server is the license server for Defensics. When installing Defensics, the license server binaries are also copied in to the system. These binaries are required along with the license file to get your license server running. This course walks through the process of setting it up with an interactive tutorial.

URL: blackduck.skilljar.com/defensics-how-to-get-your-flex-server-running

Defensics Monitor: Installing the GUI

Summary: This course walks you through how to install Defensics Monitor GUI to your local machine in Windows. This installation walkthrough applies to Linux as well. Once you have downloaded Defensics Monitor, you need to install it to your local machine with appropriate administrative privileges. The installation procedure is quite straightforward, and the following interactive tutorial will show you how to make it happen in Windows. The process is very similar in Linux environment.

URL: blackduck.skilljar.com/defensics-installing-the-gui

Defensics: Test Suite Browser and Test Suite installation

Summary: Learn how to install test suites, how the suite browser operates, and how to launch test suites in Defensics. Installing Test Suites is the starting point of Defensics fuzz testing. You are able to download and install any test suite you have a license for. These test suites can be installed to multiple computers running Defensics in your organization. Downloading the Test Suites is quick and easy, and this course walks you through how to do it.

URL: blackduck.skilljar.com/defensics-test-suite-browser-and-test-suite-installation

Black Duck Defensics: Basic Settings and Interoperability

Summary: Learn the concept of basic settings in Black Duck Defensics and what you need to focus on. We will also walk through the interoperability run. The fundamental requirement for Black Duck Defensics testing is being able to establish a connection with the test target. Once a connection and the proper protocol communication works, you can start running the actual fuzz tests. This course walks through the basic settings and shows how the interoperability test works.

URL: blackduck.skilljar.com/black-duck-defensics-basic-settings-and-interoperability

Defensics: Instrumentation Overview

Summary: This course is a quick walkthrough of different instrumentation methods in Defensics. Defensics determines the pass/fail verdict for each test case based on instrumentation results.Instrumentation essentially means checking the health of the tested system. This course is an overview of different instrumentation methods in Defensics.

URL: blackduck.skilljar.com/defensics-instrumentation-overview

Defensics: Test Cases

Summary: Learn how to adjust and configure Test Cases and the test run in Black Duck Defensics. Black Duck Defensics testing includes a lot of test cases, so it is useful to know how you can tweak the test case selection to optimize your test run. This course walks through different options for test cases in Black Duck Defensics.

URL: blackduck.skilljar.com/black-duck-defensics-test-cases

Defensics: Test Run

Summary: This course is a quick walkthrough on how the Defensics Test Run operates and what you need to consider to prepare for it. Once you have configured your test target to allow incoming connections, and you have configured Defensics with the right settings, it is time to start the actual test run. This course walks you through what the test run looks like, and what options you have during the test run. We will also have a short walkthrough of the steps prior to starting the test run.

URL: blackduck.skilljar.com/defensics-test-run

Defensics: Interpreting Results

Summary: Learn about test run results and what they mean in Defensics test runs. When running tests with Defensics it is important to understand what the results mean. The results tell you if you have configured the test environment properly, and if the tested system fails due to fuzz testing. This course walks through results interpretation in Defensics.

URL: blackduck.skilljar.com/defensics-interpreting-results

Defensics: Advanced Settings

Summary: Learn how the Advanced Settings can help your testing in Defensics. Most of the important settings are located in the Basic Settings section in Defensics, but there is an additional selection of options available should you need to tweak your test setup. Advanced Settings help you to optimize and debug your test run.

URL: blackduck.skilljar.com/defensics-advanced-settings

Defensics: Remediation Package

Summary: Learn about creating and using Remediation packages in Defensics. Reproducing and fixing the found vulnerabilities is the main goal of Defensics testing. With the help of Remediation packages, developers can easily reproduce the found issues on their own computer, and mak sure the issues are properly fixed.

URL: blackduck.skilljar.com/defensics-remediation-package

Defensics: Reporting

Summary: This course is a quick walkthrough on how to create a report from your test run results in Defensics. While Defensics results and logs are an excellent source of test run details, it is good to know how to generate a report that doesnâ€™t require looking at the log files in the application itself. This course walks you through how you can generate and view an HTML-based report from Defensics test run results.

URL: blackduck.skilljar.com/defensics-reporting

Defensics: How to Get Help

Summary: Learn how to create a Support Package, and how to submit a Support Case to get help for Defensics. Sometimes you may encounter situations where you need the help of our Support Team to get help with Defensics. Our Community provides you an easy way to contact our Support Team and get assistance. We'll also learn how to create a Support Package to gather important details from Defensics.

URL: blackduck.skilljar.com/defensics-how-to-get-help

Black Duck Defensics: Installation

Summary: This mini-course is a walkthrough of how to install the new Black Duck Defensics in Windows. The installation flow is very similar in Linux systems. This mini-course is a walkthrough of how to install the new Black Duck Defensics in Windows. The installation flow is very similar in Linux systems. We are going to install Black Duck Defensics, configure lisensing, and connect you to the Download Portal where you can download and install test suites for Black Duck Defensics.

URL: blackduck.skilljar.com/black-duck-defensics-installation

Black Duck Defensics: New Project and a Test Run

Summary: This mini-course is a walkthrough of how create a new Project in Black Duck Defensics. We are going to create a new configuration as well, and do a test run.This mini-course is a walkthrough of how create a new Project in Black Duck Defensics. We are going to create a new configuration as well, and do a test run. The UI in the new Black Duck Defensics differs from the classic UI a bit, and the flow is more streamlined to make using Defensics more intuitive.

URL: blackduck.skilljar.com/black-duck-defensics-new-project-and-a-test-run

Defensics: Basic Settings and Interoperability

Summary: Learn what the basic settings are all about in Defensics and what you need to focus on. We will also walk through the interoperability run. The fundamental requirement for Defensics testing is being able to establish a connection with the test target. Once a connection and the proper protocol communication works, you can start running the actual fuzz tests. This course walks through the basic settings and shows how the interoperability test works.

URL: blackduck.skilljar.com/defensics-basic-settings-and-interoperability

Black Duck Defensics: When to use Valid Case Instrumentation

Summary: Learn about Valid Case Instrumentation in Black Duck Defensics with this course. When running server-side testing, valid case instrumentation is usually quick and easy to set up. Valid case instrumentation gives you quick results, but it is recommended to use more in-depth instrumentation methods for more detailed results.

URL: blackduck.skilljar.com/black-duck-defensics-when-to-use-valid-case-instrumentation

Black Duck Defensics: Test Run

Summary: This course is a quick walkthrough on how the Black Duck Defensics Test Run operates and what you need to consider to prepare for it. Once you have configured your test target to allow incoming connections, and you have configured Black Duck Defensics with the right settings, it is time to start the actual test run. This course walks you through what the test run looks like, and what options you have during the test run. We will also have a short walkthrough of the steps prior to starting the test run.

URL: blackduck.skilljar.com/black-duck-defensics-test-run

Black Duck Defensics: Reporting

Summary: Learn how to create test run reports in Black Duck Defensics with the help of this course. While forwarding log files and other details to developers is essential for fixing the found vulnerabilities, reporting to other people and having an overview of the issues is important as well. This course walks through how to create reports in Black Duck Defensics.

URL: blackduck.skilljar.com/black-duck-defensics-reporting

Black Duck Defensics: How to Get Help

Summary: Learn how to create a Support Package, and how to submit a Support Case to get help for Black Duck Defensics. Sometimes you may encounter situations where you need the help of our Support Team to get help with Defensics. Our Community provides you an easy way to contact our Support Team and get assistance. We'll also learn how to create a Support Package to gather important details from Defensics.

URL: blackduck.skilljar.com/black-duck-defensics-how-to-get-help

Defensics FuzzBox: How to Use a WLAN Test Suite

Summary: A course for developers, testers and administrators for starting to use and setting up Defensics FuzzBox for the first time. Defensics FuzzBox OS is an operating system with customized libraries and configurations to enable negative testing for IEEE 802.11 protocol layers. Testing with FuzzBox 802.11 requires FuzzBox OS installed to the computer (x86 64-bit hardware) with injector hardware (WLAN adapter) and another computer (real or virtualized) running Defensics Monitor.

URL: blackduck.skilljar.com/defensics-fuzzbox-how-to-use-a-wlan-test-suite

Defensics FuzzBox: How to Create a Fuzzbox Installation USB Key

Summary: A course for developers, testers and administrators for starting to use and setting up Defensics FuzzBox for the first time. Defensics FuzzBox OS is an operating system with customized libraries and configurations to enable negative testing for IEEE 802.11 protocol layers. Testing with FuzzBox 802.11 requires FuzzBox OS installed to the computer (x86 64-bit hardware) with injector hardware (WLAN adapter) and another computer (real or virtualized) running Defensics Monitor. This course is the first of four lessons: How to Create a Fuzzbox Installation USB Key.

URL: blackduck.skilljar.com/defensics-fuzzbox-getting-started

Defensics FuzzBox: Installing the FuzzBox OS

Summary: A course for developers, testers and administrators for starting to use and setting up Defensics FuzzBox for the first time. Defensics FuzzBox OS is an operating system with customized libraries and configurations to enable negative testing for IEEE 802.11 protocol layers. Testing with FuzzBox 802.11 requires FuzzBox OS installed to the computer (x86 64-bit hardware) with injector hardware (WLAN adapter) and another computer (real or virtualized) running Defensics Monitor. This course is the second of four lessons: Installing the FuzzBox OS.

URL: blackduck.skilljar.com/defensics-fuzzbox-installing-the-fuzzbox-os

Defensics FuzzBox: Authorize a New Monitor

Summary: Defensics FuzzBox OS is an operating system with customized libraries and configurations to enable negative testing for IEEE 802.11 protocol layers. Testing with FuzzBox 802.11 requires FuzzBox OS installed to the computer (x86 64-bit hardware) with injector hardware (WLAN adapter) and another computer (real or virtualized) running Defensics Monitor. This course is the third of four lessons: Authorize a New Monitor. After finishing these lessons, you are able to install and use the Defensics FuzzBox solution in your own production environment.

URL: blackduck.skilljar.com/defensics-fuzzbox-authorize-a-new-monitor

Defensics FuzzBox (Learning Path)

Summary: The Defensics FuzzBox learning path is designed for any user who starts using Defensics FuzzBox. This path is focused on the first steps of FuzzBox usage. The path covers creating a USB installation key, installing the FuzzBox OS, authorizing a new monitor, and how to use a WLAN test suite.

URL: blackduck.skilljar.com/path/defensics-fuzzbox

Defensics: When to use Valid Case Instrumentation

Summary: Learn about Valid Case Instrumentation in Defensics with this course. When running server-side testing, valid case instrumentation is usually quick and easy to set up. Valid case instrumentation gives you quick results, but it is recommended to use more in-depth instrumentation methods for more detailed results.

URL: blackduck.skilljar.com/defensics-when-to-use-valid-case-instrumentation

Defensics: How to Debug Interoperability

Summary: Learn how to debug interoperability issues when running tests in Defensics. Before you start running tests with Defensics, you have to make sure the protocol test suite and the test target are able to communicate with each other. You may have basic network connectivity, but configuring protocol message exchange usually requires a bit more work. This course walks through the most common issues you may encounter when running the interoperability test.

URL: blackduck.skilljar.com/defensics-how-to-debug-interoperability

Defensics: Testplans

Summary: Learn how to use testplans with Defensics UI and utilize them with command line automation. When you run the same test run against the same test target multiple times with Defensics, using testplans is an excellent way to automate it, and lessen your workload on configuring the test suite every time.

URL: blackduck.skilljar.com/defensics-testplans

Defensics: Re-run Test Cases

Summary: Learn how to eliminate false positives by re-running test cases in Defensics with the help of this course. When doing fuzz testing with Defensics, it is essential to weed out the actual failures by re-running test cases. This course walks you through how to re-run test cases based on a previous test run.

URL: blackduck.skilljar.com/defensics-re-run-test-cases

Defensics Monitor: Running HTTP API v2 Server

Summary: This tutorial covers some of the basics with the HTTP API v2 usage: how to configure and start the server. You can control test case execution via API by using the new and improved HTTP API v2 Server in Defensics.This course walks you through how to start the server, introduces some authentication options, and gives you a good starting point on the HTTP API usage.

URL: blackduck.skilljar.com/defensics-running-http-api-v2-server

Defensics Monitor: Command Line Execution

Summary: This course walks through the command line execution for Defensics that applies to both Windows and Linux due to identical syntax. Using command line execution is the best way of automating your fuzz testing. This course walks through the command line execution for Defensics that applies to both Windows and Linux due to identical syntax.

URL: blackduck.skilljar.com/defensics-command-line-execution

Defensics: From Install to First Results

Summary: This course is a walkthrough for new Defensics users on how to do a quick setup and see your first results. Defensics is a comprehensive, versatile, automated black box fuzzer that enables organizations to efficiently and effectively discover and remediate security weaknesses in software. This course is a walkthrough of the main steps on how to get your Defensics environment set up and how to get your first results

URL: blackduck.skilljar.com/defensics-from-install-to-first-results

Black Duck Defensics: How to Debug Interoperability

Summary: Learn how to debug interoperability issues when running tests in Black Duck Defensics. Before you start running tests with Black Duck Defensics, you have to make sure the protocol test suite and the test target are able to communicate with each other. You may have basic network connectivity, but configuring protocol message exchange usually requires a bit more work. This course walks through the most common issues you may encounter when running the interoperability test.

URL: blackduck.skilljar.com/black-duck-defensics-how-to-debug-interoperability

Black Duck Defensics: Test Cases

Summary: Learn how to adjust and configure Test Cases and the test run in Black Duck Defensics. Black Duck Defensics testing includes a lot of test cases, so it is useful to know how you can tweak the test case selection to optimize your test run. This course walks through different options for test cases in Black Duck Defensics.

URL: blackduck.skilljar.com/black-duck-defensics-test-cases

Black Duck Defensics: Re-run Test Cases

Summary: Learn how to eliminate false positives by re-running test cases in Black Duck Defensics with the help of this course. When doing fuzz testing with Black Duck Defensics, it is essential to weed out the actual failures by re-running test cases. This course walks you through how to re-run test cases based on a previous test run.

URL: blackduck.skilljar.com/black-duck-defensics-re-run-test-cases

Black Duck Defensics: Interpreting Results

Summary: This course is a quick walkthrough on how to inspect and interpret test run results in Black Duck Defensics. When running tests with Black Duck Defensics it is important to understand what the results mean. The results tell you if you have configured the test environment properly, and if the tested system fails due to fuzz testing. This course walks through results interpretation in Black Duck Defensics.

URL: blackduck.skilljar.com/black-duck-defensics-interpreting-results

Defensics SDK: Introduction

Summary: This course is an introduction to Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course is an introduction to Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-introduction

Defensics: External Instrumentation

Summary: This course is a quick walkthrough on how to use External Instrumentation in Defensics GUI. Instrumentation is the fundamental method of determining if something unwanted occurred in your test target. Defensics has a wide variety of these health checks, but one of the most versatile one is the External Instrumentation. This course walks through the basics of External Instrumentation, and shows an example how to use a script to check the health of the test target.

URL: blackduck.skilljar.com/defensics-external-instrumentation

Defensics: Sequence Editing

Summary: This course is a quick walkthrough on how sequence editing works in Defensics. When running tests with Defensics, you are usually good with simply modifying the settings in the test suite. However, depending on the protocol, your test target may require some special adjustments to the messages sent by Defensics. Sequence Editor is an excellent tool to help you customize your Defensics testing.

URL: blackduck.skilljar.com/defensics-sequence-editing

Defensics: Setting up Agent Instrumentation

Summary: This course walks you through how to set up Agent Instrumentation in Defensics for detecting additional issues in tested systems. Agent Instrumentation is an effective way of detecting more issues from your tested system. This course walks you through how to configure both Defensics and your SUT for Agent Instrumentation.

URL: blackduck.skilljar.com/defensics-setting-up-agent-instrumentation

Defensics: gRPC Test Suite

Summary: This course is a walkthrough of the gRPC Test Suite and the gRPC Wizard. The gRPC Test Suite has a tool for creating test sequences called gRPC Wizard. The gRPC Wizard is a tool for converting Protocol buffers' definitions into a format which is understood by Defensics. This tutorial will walk you trough the basic usage of the wizard, so that you are able to create your own test sequences from your own Protocol buffers definitions.

URL: blackduck.skilljar.com/defensics-grpc-test-suite

Defensics Essentials

Summary: Defensics Essentials offers an in-depth walkthrough of fuzz testing with Defensics, and covers the essential features and capabilities of the product. Everything you need to know about Defensics, including vulnerabilities, fuzzing techniques, core product features, functionality and common use cases. To allow hands-on experience, topical lectures are augmented by lab exercises to be performed on a cloud-based virtual machine. NOTE: This course is not kept up-to-date. You should check out Knowledge Paths for Defensics for the most recent role-based course selections.

URL: blackduck.skilljar.com/defensics-essentials

Defensics: Lab Course

Summary: This course provides you different level lab works you can practice in a cloud-based VM environment. In addition to the step-by-step labs, there are other protocols enabled in the VM environment you can play with. While the course provides you the needed details for executing the labs, you need have knowledge on both Defensics and Linux in order to get the most of this labs course. It is highly recommended you have finished a considerable amount of Defensics courses before doing the labs.

URL: blackduck.skilljar.com/defensics-labs-and-playground

Defensics SDK: Environment Setup

Summary: This course walks you through how to set up the Defensics SDK environment and the fuzzing framework. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for uncommon, custom or proprietary protocols and file format parsers. This course walks through setting up the Defensics SDK environment.

URL: blackduck.skilljar.com/defensics-sdk-environment-setup

Defensics SDK: Plugin for IntelliJ IDEA

Summary: This course is a quick walkthrough of the features of the Defensics SDK IntelliJ IDEA plugin and on how to install it. Defensics SDK plugin for IntelliJ IDEA makes your development tasks easier and more streamlined. The plugin features help you on your daily coding tasks with syntax highlighting, model validation, brace matching, and with many other features. This course is a walkthrough of the plugin and its capabilities

URL: blackduck.skilljar.com/defensics-sdk-plugin-for-intellij-idea

Defensics SDK: Modeling

Summary: This course covers the modeling part of Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through modeling in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-modeling

Defensics SDK: Dynamic Functionality

Summary: This course walks through dynamic functionality in Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through dynamic functionality in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-dynamic-functionality

Defensics SDK: Accessing and Modifying Elements

Summary: This course teaches how to access and modify elements in Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through how to access and modify elements in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-accessing-and-modifying-elements

Defensics SDK: Input and Output

Summary: This course walks through input and output in Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through input and output in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-input-and-output

Defensics SDK: Settings

Summary: This course covers the settings part of Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through settings in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-settings

Defensics SDK: Custom Anomalies

Summary: This course walks through custom anomalies in Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through custom anomalies in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-custom-anomalies

Defensics SDK: Probes and Instrumentation

Summary: This course walks through probes and instrumentation in Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through probes and instrumentation in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-probes-and-instrumentation

Defensics SDK: Packing and Running the Suite

Summary: This course walks through how to pack and run the suite in Defensics SDK. The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through packing and running the suite in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-packing-and-running-the-suite

Defensics SDK: Test Suite Development Workflow

Summary: The Fuzz Testing SDK (Defensics SDK) is a fuzzing framework that enables organizations to develop their own test suites for testing uncommon, custom or proprietary protocols and file format parsers. The Defensics SDK draws on the capabilities of the powerful Defensics fuzz testing engine, by defining a framework used for creating custom test suites. This course walks through the test suite development workflow in Defensics SDK.

URL: blackduck.skilljar.com/defensics-sdk-test-suite-development-workflow

Defensics SDK (Learning Path)

Summary: The Defensics SDK learning path is designed for all the users who are starting to use Defensics SDK for building their custom test suites. This path covers all the steps in a self-paced format, starting with an introduction to Defensics SDK, setting up your environment, and continuing with all the important topics when working with Defensics SDK. Several courses in this learning path include exercises that you can work on in your own environment, learning the topics with hands-on practice.

URL: blackduck.skilljar.com/path/defensics-sdk

CODE SIGHT

Learn about Code Sight

Address security and quality defects in code as it's being developed.

Baseline

- **Basic deployment** Core functionality is installed and minimally configured. Usage may be ad hoc, with little to no automation or integration. Visibility is limited to basic metrics or logs.

Emerging

- **Ramped deployment** Key integrations with CI/CD pipelines are established. Automation begins for routine tasks like scanning or policy enforcement. Teams start aligning product use with development workflows.

Maturing

- **Advanced deployment** The solution is widely deployed across teams or projects. Automation is policy-driven and consistent. Integration with developer tools and environments is robust. Dashboards and reporting begin to inform decisions.

Optimizing

- **Proficient "reference" deployment** Full integration across the SDLC. Analytics dashboards provide actionable insights. Feedback loops drive continuous improvement. Manual intervention is rare. Usage is proactive, with predictive capabilities and strategic alignment.

Introduction to Code Sight

Summary: This course will help Polaris, Black Duck, Coverity, and Standard Edition users understand and get started using Code Sight. This course will help Black Duck, Coverity, Polaris and Standard Edition users understand and get started using the Code Sight IDE plug-in/extension. The Code Sight Plug-in/extension provides developers with an interface to our portfolio of tools right in their IDE. After taking this micro-course you will know how Code Sight can help you and the basics of how it works.

URL: blackduck.skilljar.com/introduction-to-code-sight

Code Sight Standard Edition Getting Started

Summary: This course will help developers understand and get started using Code Sight Standard Edition. This micro-course does not cover the additional features available to Coverity or Black Duck users looking to use Code Sight as it only covers how to use the features found in Code Sight Standard Edition. After taking this micro-course you will understand how Code Sight Standard Edition can help you and be able to use it to find defects in your projects.

URL: blackduck.skilljar.com/code-sight-standard-edition-getting-started

Code Sight: Team View

Summary: This course shows you how Code Sight can be used to view issues from other tools such as Polaris, Software Risk Manager (formerly known as Code Dx), Coverity and Coverity on Polaris. We'll review how to look at issues from the server in your local IDE Code Sight is a convenient plugin that is now able to connect with other tools like Polaris, Software Risk Manager, Coverity and Coverity on Polaris. Code Sight can fetch the issues from a specific project to be shown in the Team View tab.

URL: blackduck.skilljar.com/code-sight-team-view-1

Code Sight Installation

Summary: A course for Developers who want to download and install the Code Sight plug-in/extension so that they can find Black Duck or Coverity results on their desktops. This course will walk you through how to download and install the Code Sight plug-in/extension into your IDE so that you can find Black Duck or Coverity results on your desktops. A Black Duck license is required to get Black Duck results. A Coverity or Polaris license is required for Coverity results.

URL: blackduck.skilljar.com/code-sight-installation

Micro-course Index Page

Polaris

Polaris: Getting started with fAST SCA . . . 6
Polaris: Insights and Reports . . . 6
Polaris: Creating an Access Token . . . 6
Polaris: Ways to Triage Issues . . . 6
Polaris: Using the Bridge CLI . . . 6
Polaris: A Video Introduction . . . 7
Polaris: Getting started with fAST Dynamic . . . 7
Polaris: Getting started with fAST STATIC . . . 7
Polaris: Reviewing Scan Results . . . 7
Polaris: Create Application . . . 7
Polaris: My Organization Settings, Groups and Roles . . . 8
Polaris: Create and Manage Labels . . . 8
Polaris: GitLab Integration **(Integration)** . . . 8
Polaris Jira Integration . . . 8
Polaris Single Sign-on (SSO) Configuration with SAML 2.0 . . . 8
Polaris: Running a Signature Analysis . . . 9
Polaris: Azure DevOps Bug Tracking Integration . . . 9
Polaris: Creating an SBOM Report . . . 9
Polaris: Azure DevOps Integration **(Integration)** . . . 9
Polaris: Using the Black Duck Security Scan Action for GitHub **(Integration)** . . . 9
Polaris: Jenkins Integration **(Integration)** . . . 10
Polaris: Rapid Bulk SCM Onboarding . . . 10
Integrating Polaris Findings into Software Risk Manager . . . 10
Polaris: Using the GitHub Action . . . 10
Polaris: Application Risk Scoring . . . 10
Polaris: Policies . . . 11

Coverity

Coverity: Installing the Analysis Software . . . 13
Coverity for Developers (End Users) . . . 13
Introduction to Coverity . . . 13
Coverity: License Activation and Software Download . . . 13
Coverity: Examining and Triaging issues . . . 13
Installing Coverity Platform (Server) on Linux . . . 14
Coverity: Concepts for Developers . . . 14
Coverity: Installing the Connect Server . . . 14

Coverity: Rollout Stages . . . 14
Point and Scan Quick Start for Coverity Connect users . . . 14
Coverity: Getting Started Projects and Streams . . . 15
Analyzing Code Using the Coverity CLI . . . 15
Coverity: Picking your Code Capture Strategy . . . 15
Coverity: Downloading the Analysis license and Software . . . 15
Coverity: Baselining Analysis Results . . . 15
Coverity Reporting Basics . . . 16
Coverity for Managers . . . 16
Coverity: Views, Filters and Notifications . . . 16
Coverity Connect: SAML SSO Authentication . . . 16
Coverity: GitLab Integration **(Integration)** . . . 16
Coverity: GitHub Integration **(Integration)** . . . 17
Coverity: Jenkins Integration **(Integration)** . . . 17
Coverity: Azure DevOps Integration **(Integration)** . . . 17
Coverity: Backups and Data purging . . . 17
Using Sigma Rapid Scan Static in GitHub . . . 17
Coverity: Users Groups and Roles . . . 18
Coverity: Builtin and Custom Attributes . . . 18
Getting Started with Sigma Rapid Scan Static Standalone . . . 18
Coverity: Checking Connect status and diagnostics . . . 18
Creating a coverity.yaml configuration file . . . 18
Code Sight Configuration for Coverity Users . . . 19
Coverity: How to replace your license . . . 19
Coverity: Doing a Basic Upgrade . . . 19
Coverity: Desktop Analysis Options . . . 19
Coverity: Classic Fast Desktop CLI . . . 19
Coverity: Classic Fast Desktop for your IDE . . . 20
Integrating Coverity Findings into Software Risk Manager . . . 20
Rehosting your License and Upgrading to a new Coverity Server . . . 20
Creating Custom Coverity Checkers with CodeXM . . . 20
Coverity: Using Models to Improve Analysis . . . 20

Black Duck SCA

Black Duck SCA: Scanning Guide and Tips . . . 22
Black Duck SCA: Hosted System Log-in . . . 22
Black Duck SCA: Project Group Basics . . . 22
Black Duck: Cloning Versions & Projects . . . 22

Black Duck: Self Guided Onboarding Part 3 - Scan Results & Reporting . . . 22
Black Duck SCA: Installation using Docker Swarm . . . 23
Black Duck: Core Entities Guide . . . 23
Introduction to Black Duck Solutions . . . 23
Black Duck SCA: Configure Security Risk Ranking . . . 23
Black Duck SCA: Setting Global Remediation Status . . . 23
Black Duck: Managing Users and Roles . . . 24
Black Duck SCA: Scanning with Detect GUI . . . 24
Introduction to Scanning Open Source Software with Black Duck . . . 24
Black Duck: Detectors Introduction . . . 24
Black Duck SCA: Watching Projects and Saving Searches . . . 24
Black Duck SCA: Configuring Policy Management . . . 25
Black Duck: Custom System Announcements . . . 25
Black Duck SCA: Identifying Unmatched Components . . . 25
Black Duck SCA: Navigating the Interface . . . 25
Black Duck: Introduction to Scanning . . . 25
Black Duck SCA: A Technical Introduction . . . 26
Black Duck SCA: From Configuration to First Results . . . 26
Black Duck: Self Guided Onboarding Part 1 - Getting Started & Configuration . . . 26
Black Duck SCA: Working with Scan Results . . . 26
Black Duck SCA: Attributing OSS in your Applications . . . 26
Black Duck SCA: Generating Reports . . . 27
Black Duck SCA SBOM Import . . . 27
Black Duck SCA: Creating Projects . . . 27
Black Duck SCA: Copyright Statements . . . 27
Black Duck SCA: Security Risk Remediation Strategy . . . 27
Black Duck SCA: SBOM Generation . . . 28
Black Duck SCA: Scanning Best Practices . . . 28
Black Duck: Self Guided Onboarding Part 2 - Scanning with Detect . . . 28
Black Duck SCA Admin Options and System Settings . . . 28
Black Duck SCA Scanning and Component Management (Learning Path) . . . 28
Black Duck SCA Security Risk Workflow (Learning Path) . . . 29
Black Duck SCA Vulnerability Management (Learning Path) . . . 29
Black Duck SCA in a Nutshell . . . 29
Black Duck SCA: Using Custom Scan Signatures . . . 29
Black Duck: Managing Open Source Licenses . . . 29
Black Duck SCA: Using MFA . . . 30
Black Duck SCA: Advanced License Management . . . 30

Black Duck: Discovering Open Source Snippets . . . 30
Black Duck SCA: Access Token Management for Admins . . . 30
Black Duck Administration Competency Series . . . 30
Black Duck: Custom Fields . . . 31
Black Duck SCA: Legal OSS Policy Starter Kit . . . 31
Black Duck SCA: SBOM Templates . . . 31
Black Duck SCA: Unmatched Origins Feature and Scan Identification . . . 31
Black Duck SCA: Jenkins Integration **(Integration)** . . . 31
Black Duck SCA: GitHub Integration Using Security Scan **(Integration)** . . . 32
Black Duck SCA: Azure DevOps Integration **(Integration)** . . . 32
Black Duck SCA Notification Settings . . . 32
Black Duck SCA: GitHub Action Basics . . . 32
Black Duck SCA: SBOM Import Custom Component Auto-Creation . . . 32
Black Duck: Snippet Scanning and New Triage Workflow . . . 33
Black Duck SCA SAML Integration . . . 33
Black Duck SCA: Bridge CLI Basics . . . 33
Black Duck SCA: Configuring LDAP Integration . . . 33
Black Duck: Scanning Docker Images using Docker Inspector . . . 33
Black Duck SCA: CSV Scan Archive . . . 34
Black Duck SCA: Scanning with Jenkins . . . 34
Black Duck SCA: Fix PR Overview Using Black Duck Security Scan . . . 34
Black Duck: Secure Container Scanning Basics . . . 34
Black Duck SCA: GitLab Integration **(Integration)** . . . 34
Black Duck SCA License and Compliance Workflow (Learning Path) . . . 35
Black Duck SCA Lightweight Scanning (Learning Path) . . . 35
Black Duck SCA SBOM Reporting (Learning Path) . . . 35
Scanning for C and C++ Projects using Black Duck . . . 35
Introduction to Code Sight with Black Duck SCA . . . 35
Black Duck: Infrastructure-As-Code Scanning . . . 36
Black Duck Alert: Managing Notifications . . . 36
Black Duck: Configurable Individual File Matching . . . 36
Black Duck SCA: Rapid Scan . . . 36
Black Duck SCA: Managing Deep License Data . . . 36
Black Duck SCA SCM Integration . . . 37
Installing an On-premise Black Duck KnowledgeBase . . . 37
Black Duck: Connecting to the Report Database . . . 37
Black Duck: Vulnerability Impact Analysis . . . 37
Black Duck SCA Heatmaps . . . 37

Black Duck Binary Analysis

Introduction to Black Duck Binary Analysis BDBA Standalone . . . 39
Black Duck Binary Analysis: Introduction to Cyber Supply Chain . . . 39
Black Duck Binary Analysis: Vulnerabilities and Code Decay . . . 39
Black Duck Binary Analysis: Key Features . . . 39
Black Duck Binary Analysis: A Walkthrough . . . 39
Black Duck Binary Analysis: Uploading and Analysis Overview . . . 40
Black Duck Binary Analysis: User Profile and Settings . . . 40
Black Duck Binary Analysis: Groups . . . 40
Black Duck Binary Analysis: Scan List Operations . . . 40
Black Duck Binary Analysis: Vulnerability Triage . . . 40
Black Duck Binary Analysis: Information Leakage . . . 41
Black Duck Binary Analysis: Reporting . . . 41
Black Duck Binary Analysis: Support for Black Duck Security Advisories . . . 41
Black Duck Binary Analysis: Account Settings and Options . . . 41
Black Duck Binary Analysis Essentials (Learning Path) . . . 41
Black Duck Binary Analysis Integrated: Scan with Detect GUI . . . 42
Black Duck Binary Analysis Integrated: Scan with Detect Command Line . . . 42
Black Duck Binary Analysis Integrated: Examining the Results . . . 42
Black Duck Binary Analysis Essentials . . . 42
Black Duck Binary Analysis: User Management and Permissions . . . 42
Black Duck Binary Analysis: User Management and Default Roles . . . 43
Black Duck Binary Analysis: Detected Components . . . 43
Black Duck Binary Analysis: API Basics . . . 43
Black Duck Binary Analysis: Custom Data and Custom Data Templates . . . 43
Black Duck Binary Analysis: How to Enable API Key Authentication . . . 43
Black Duck Binary Analysis: Rapid Scan Static Support . . . 44
Black Duck Binary Analysis: Linux Kernel Module Support . . . 44
Black Duck Binary Analysis: Docker Container Scanning . . . 44
Black Duck Binary Analysis: API Fetch for Docker Registry and Custom Data . . . 44
Black Duck Binary Analysis: SBOM Annotations . . . 44
Black Duck Binary Analysis: How to create a Vendor Vulnerability . . . 45
Black Duck Binary Analysis: How to create a Vendor Component . . . 45
Black Duck Binary Analysis: From Install to First Results . . . 45
Black Duck Binary Analysis Advanced (Learning Path) . . . 45
Black Duck Binary Analysis Appliance (Learning Path) . . . 45
Black Duck Binary Analysis: Lab Course . . . 46
Black Duck Binary Analysis: Initial Setup Options for Appliance . . . 46

Black Duck Binary Analysis: Analysis Configuration File Usage . . . 46
Black Duck Binary Analysis: Virtual Appliance Migration . . . 46
Black Duck Binary Analysis: How to set up server monitoring . . . 46
Black Duck Binary Analysis: Troubleshooting and Optimizing the Appliance . . . 47

Defensics

Introduction to Defensics . . . 49
Defensics: Get Started with Defensics Testing . . . 49
Defensics: Fuzzing Guidelines . . . 49
Defensics: How to Access Arena and Download Defensics . . . 49
Defensics: How to Download a License from Community . . . 49
Defensics: How to Download Defensics from our Community . . . 50
Defensics: How to Get Your Flex Server Running . . . 50
Defensics Monitor: Installing the GUI . . . 50
Defensics: Test Suite Browser and Test Suite installation . . . 50
Black Duck Defensics: Basic Settings and Interoperability . . . 50
Defensics: Instrumentation Overview . . . 51
Defensics: Test Cases . . . 51
Defensics: Test Run . . . 51
Defensics: Interpreting Results . . . 51
Defensics: Advanced Settings . . . 51
Defensics: Remediation Package . . . 52
Defensics: Reporting . . . 52
Defensics: How to Get Help . . . 52
Black Duck Defensics: Installation . . . 52
Black Duck Defensics: New Project and a Test Run . . . 52
Defensics: Basic Settings and Interoperability . . . 53
Black Duck Defensics: When to use Valid Case Instrumentation . . . 53
Black Duck Defensics: Test Run . . . 53
Black Duck Defensics: Reporting . . . 53
Black Duck Defensics: How to Get Help . . . 53
Defensics FuzzBox: How to Use a WLAN Test Suite . . . 54
Defensics FuzzBox: How to Create a Fuzzbox Installation USB Key . . . 54
Defensics FuzzBox: Installing the FuzzBox OS . . . 54
Defensics FuzzBox: Authorize a New Monitor . . . 54
Defensics FuzzBox (Learning Path) . . . 54
Defensics: When to use Valid Case Instrumentation . . . 55
Defensics: How to Debug Interoperability . . . 55

Defensics: Testplans . . . 55
Defensics: Re-run Test Cases . . . 55
Defensics Monitor: Running HTTP API v2 Server . . . 55
Defensics Monitor: Command Line Execution . . . 56
Defensics: From Install to First Results . . . 56
Black Duck Defensics: How to Debug Interoperability . . . 56
Black Duck Defensics: Test Cases . . . 56
Black Duck Defensics: Re-run Test Cases . . . 56
Black Duck Defensics: Interpreting Results . . . 57
Defensics SDK: Introduction . . . 57
Defensics: External Instrumentation . . . 57
Defensics: Sequence Editing . . . 57
Defensics: Setting up Agent Instrumentation . . . 57
Defensics: gRPC Test Suite . . . 58
Defensics Essentials . . . 58
Defensics: Lab Course . . . 58
Defensics SDK: Environment Setup . . . 58
Defensics SDK: Plugin for IntelliJ IDEA . . . 58
Defensics SDK: Modeling . . . 59
Defensics SDK: Dynamic Functionality . . . 59
Defensics SDK: Accessing and Modifying Elements . . . 59
Defensics SDK: Input and Output . . . 59
Defensics SDK: Settings . . . 59
Defensics SDK: Custom Anomalies . . . 60
Defensics SDK: Probes and Instrumentation . . . 60
Defensics SDK: Packing and Running the Suite . . . 60
Defensics SDK: Test Suite Development Workflow . . . 60
Defensics SDK (Learning Path) . . . 60

Code Sight

Introduction to Code Sight . . . 62
Code Sight Standard Edition Getting Started . . . 62
Code Sight: Team View . . . 62
Code Sight Installation . . . 62