

Black Duck® SCA – Implementation Packages

The services described in this Black Duck SCA Implementation Package (the "**Services**") are provided by Black Duck® and/or its Affiliates (collectively, "**BD**") to Customer in accordance with the terms of this Black Duck SCA Implementation Package (this "**Services Package**") and are subject to the terms and conditions of the Purchasing Agreement and the End User License and Maintenance Agreement pursuant to which this these Services have been purchased by Customer, or where no such agreement governing the Services to be provided is referenced therein, the most recent version of the End User License Agreement posted at <https://www.blackduck.com/company/legal/end-user-licenses.html> (collectively, the "**Agreement**"), and such terms and conditions are incorporated herein by reference. All capitalized terms that are not defined in this Black Duck SCA Implementation Package will have the meaning set forth in the Agreement.

1 Overview

The Implementation Packages help customers become acquainted with Black Duck SCA. These packages provide a structured and guided approach to help implement and adopt Black Duck SCA.

The Black Duck SCA packages are offered in QuickStart Plus, Pro, and Premier tiers and include the following:

Description	QuickStart Plus	Pro	Premier
Black Duck SCA server deployment	Hosted Only	✓	✓
Codebase onboarding	One (1)	One (1)	Up to two (2)
Scan automation through continuous integration/continuous development ("CI/CD") integration	One (1) CI/CD tool	One (1) CI/CD tool	Up to two (2) CI/CD tools
Bug tracking integration		✓	✓
IDE Integration		✓	✓
Advanced scanning workflow enablement with Rapid, container scanning and, if licensed, ReversingLabs scanning.		✓	✓
Snippet scanning			✓
Integration with one (1) supported binary artifact repository.			✓
Instructor-led training for end-users and Black Duck SCA administrators		✓	✓
Onboarding Runbook			✓

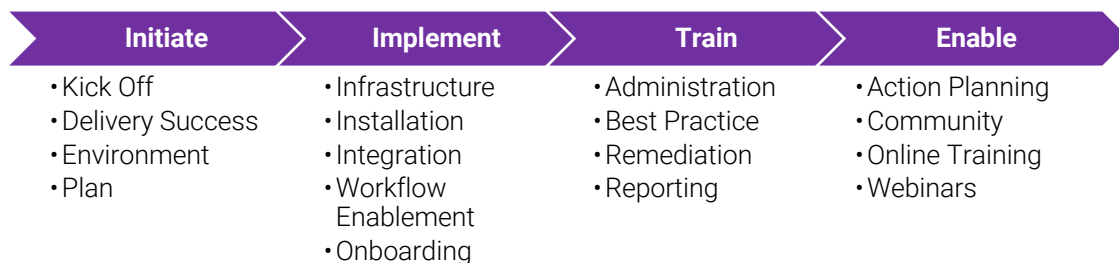
1.1 Package Delivery Success Criteria

Item	Criteria
1	Black Duck SCA instance is “Production Ready” • Black Duck SCA has been installed and configured for use in Customer’s environment. • End-user access provisioned and successfully tested. • Guidance on maintenance, upgrades, and disaster recovery options provided and discussed with the Customer.
2	Designated codebase(s) and respective project team(s) have been onboarded as per section 2.2.
3	Black Duck SCA best practice guidance has been provided to the in-scope codebase(s) project team(s) and designated product champion(s).
4	In-scope product features have been enabled and demonstrated to the relevant project team(s).
5	Customer administrator(s) have been identified and trained in Black Duck SCA administrative functions.
6	The in-scope integrations designated in Section 2.2 are enabled and tested; members of the in-scope project team(s) are trained on their usage.
7	Developer workflows reviewed, enabled, and tested for alignment with Black Duck SCA best practices and fulfillment of Customer’s usage requirements.
8	Customer has been given post-implementation support, including self-paced online training, Community Portal, and Technical Support access.
9	An Action Plan to identify the completed tasks and recommended next steps have been reviewed and discussed with the Customer.

2 Implementation Approach

BD will assist Customer with onboarding groups of users onto Black Duck SCA and will facilitate adoption. The overall process consists of the following phases, as described below.

Figure 1: Phases



2.1 Initiate

The Initiate Phase will be conducted by BD and Customer in one or more meetings with the following objectives:

- **Kick-Off** – Review Customer’s goals and organizational outcomes. Identification of Customer stakeholders for the following functions:
 - Project management,
 - Infrastructure network, database (“DB”), and security,
 - Project team leader(s) – owner of teams pioneering adoption,
 - Integrated application managers – owners of tools/systems with which Black Duck SCA will integrate, and
 - Customer evangelists – members of the Customer’s teams identified as the critical leaders for adoption and success.
- **Requirements** – Customer confirmation of what elements of the Services are applicable.
- **Success Criteria** – Confirm the success criteria as they relate to the scope:
 - Production-ready – Black Duck SCA is operational,
 - 3rd party integrations – continuous integration/deployment, notifications, bug tracking systems,
 - Development team – trained in scanning best practices, tool usage, and remediation, and
 - Administrators – trained in configuration, tool usage, and reporting.
- **Delivery Process** – Review the Black Duck SCA Implementation process:
 - Target goals: short-term, near-term, and long-term,
 - A sample project plan for the initial 90 days, and
 - Establish Customer champion and implementation point of contact.
- **Environment** – Establish the initial environmental needs.
 - Black Duck SCA environment,
 - Black Duck Alert Server deployment method, and
 - Black Duck SCA Reporting.
- **Plan** – Identify a plan of action designed to ensure Services are completed in a timely manner.

2.2 Implement

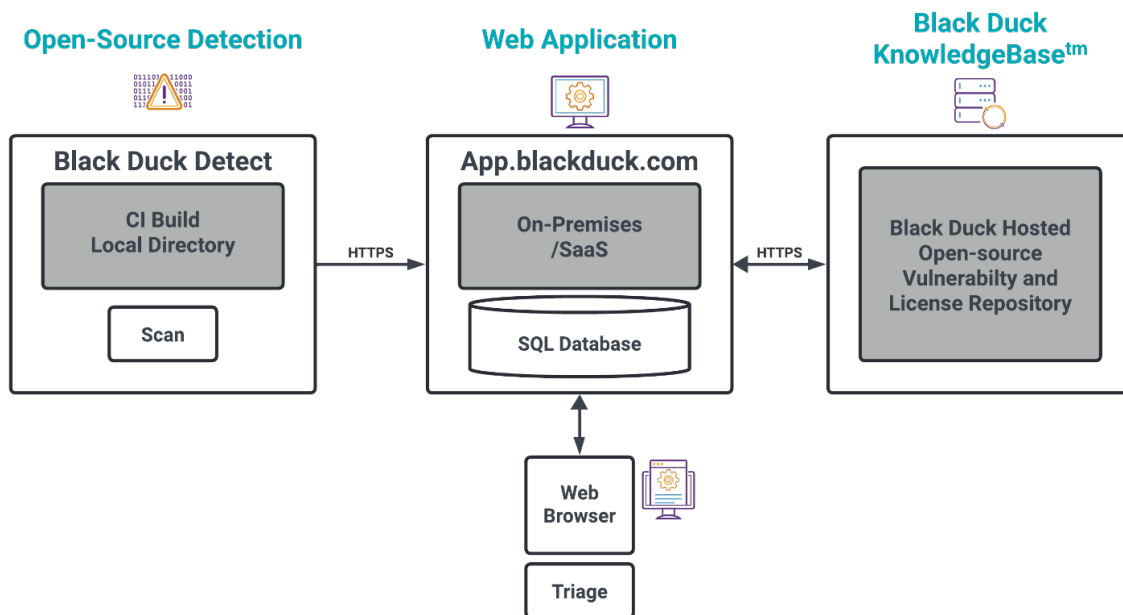
2.2.1 Infrastructure Deployment

BD will assist the Customer with the installation and configuration of Black Duck SCA per Customer selected Implementation package:

Description	QuickStart Plus	Pro	Premier
Setup and configuration of one (1) Black Duck SCA instance • Setup of the Black Duck Alert server • Connectivity with Black Duck SCA Reporting DB • User authentication - Integration via Lightweight Directory Access Protocol("LDAP")/ Security Assertion Markup Language("SAML") • Notifications – Email, MS Team, or Slack	Hosted Only	✓	✓
High availability review and disaster recovery planning		✓	✓
Setup of an on-premises Black Duck Knowledge Base (restricted to select customers)			✓

The following diagram is an approximate representation of a typical system architecture in which Black Duck SCA may be installed.

Figure 2: System Architecture



Open-Source Detection — Black Duck Detect scan client is deployed on build servers or developer desktops alongside the codebase’s native build process. Detect analyzes the codebase after build time and communicates results to the Black Duck SCA web application or directly to the scanning user.

Black Duck SCA Web Application — Web application and database installed in customers’ environment or available as software as a service (“SaaS”) using BD’s Google Cloud platform. The server provides visual tools for working with open-source components and a set of administration user interfaces (“UIs”) and Representational State Transfer (“REST”) application program interfaces (“APIs”) for configuring and managing SCA.

Black Duck KnowledgeBase™ — The KnowledgeBase is located in BD data centers. The web application stays in touch with it to keep the data up-to-date on components, vulnerabilities, and open-source licenses. The knowledge base is looked after by a team of open-source and security experts who improve the vulnerability data regularly. They provide the latest information on vulnerabilities, including their nature, available exploits, potential workarounds, and guidance on how to fix them.

2.2.2 Codebase Onboarding

BD will assist with the onboarding of the in-scope codebase(s) onto Black Duck SCA to meet the described in the selected service package:

Description	QuickStart Plus	Pro	Premier
Scanning with Signature and Detector analysis	1 Codebase	1 Codebase	Up to 2 Codebases
SCM Integration with a supported SCM Repository	1	1	1
Advanced scanning workflow enablement with Rapid , container scanning and ReversingLabs* Scanning *Only available on Black Duck Supply Chain Edition as an add-on*		✓	✓
Snippet scanning			✓
Scanning best practices	✓	✓	✓
Configuration of policy management		✓	✓
Vulnerability and license remediation		✓	✓
Advanced license workflow			✓

A codebase consists of source code with the following attributes:

- Checked out from the same source code management (SCM) repository,
- Uses the same compiler for a given supported programming language,
- Utilizes the same build infrastructure and scripts,
- If multiple checkouts are required (each building a particular component or microservice), then each checkout:
 - comprises a part of a cohesive system and
 - consistently communicates with other components (e.g., direct function call, library, or REST API) to provide the required functionality.

Project Baselineing / Scan Tuning and Configuration — BD will work with Customer representatives to install and configure Black Duck Detect, complete a scan, and review the scan results. BD will provide customers with Pro and Premier packages guidance on how to baseline their projects in Black Duck SCA.

- Install and configure Black Duck Detect.
- Complete an initial scan of the codebase per the customer's service package and conduct a scan review session with Customer representatives.
- Conduct a scanning best practice session.

- With the Pro and Premier packages:
 - Enable advanced scanning of Containers,
 - Setup Rapid scanning workflow for developers and CI/CD,
 - Review baselining best practices, and
 - If licensed, ReversingLabs scan (malware scan) workflow and training to identify the presence of threats such as malware, maldocs, suspicious files, potentially unwanted applications (PUAs), protestware, and suspicious file structure malformations to help avoid dangerous software supply chain attacks.
- With the Premier package:
 - Snippet scanning workflow and training. Snippet matching is beneficial to managing legal risk and detecting possible license infringement. A snippet match occurs when a portion of code in your file matches code in one or more KnowledgeBase files.
 - Advanced license workflow training on the more complex license features of the tool:
 - Deep license data
 - Copyright statements
 - Custom components and licenses
 - License conflicts
 - License fulfillment

Vulnerability and License Remediation – As part of the Pro and Premier packages, BD will work with the Customer to provide guidance on best practices to report and remediate security vulnerability and license risk findings.

- Review initial security and license compliance strategy.
- Review of SCA's reporting capabilities.

2.2.3 Workflow Integration

BD will assist with integrating Black Duck SCA with Customer tools and development processes. The following tasks will be completed for each in-scope application:

Description	QuickStart Plus	Pro	Premier
CI/CD integration (e.g., Azure, Bamboo, and Jenkins)	✓	✓	✓
IDE Plugin Installation and Configuration		✓	✓
One (1) 3rd party workflow system integration (e.g., Azure and Jira)		✓	✓
Alert policy configuration		✓	✓
Integration with a universal artifact repository management system			✓
Reporting database configuration			✓
Advanced policy workshop			✓

Advanced CI/CD workflows			✓
--------------------------	--	--	---

CI/CD Integration – This automates Black Duck Detect scanning seamlessly into your existing CI/CD environment. One (1) CI/CD integration per onboarded codebase will be integrated.

Alert Notification System – Alert supports commonly used distribution channels (e.g., email, Slack, MS Teams, Azure Boards, and Jira). Alert streamlines the process of getting timely, valuable Black Duck SCA related notifications to key stakeholders.

As part of the Pro and Premier packages, BD will:

- Integrate Black Duck SCA with one (1) supported workflow system integration (e.g., Azure/Jira).
- Provide training on setting up e-mail, Slack, and MS Teams notifications.
- Assist the customer confirmation of the policies to trigger the alerts.

Artifact Repository Integration – BD maintains a Black Duck SCA plugin for Artifactory and Nexus 3. With the Premier Package, BD will assist in integrating Black Duck SCA with one (1) Artifactory or Nexus 3 environment.

Reporting Database – After completing the Reporting training below, BD will assist Premier Package customers with a working session to create one desired report in Power BI / Tableau / etc.

After completion of Codebase Onboarding and Training, BD will assist Premier Package customers with two additional advanced sessions:

- **Advanced Policy Workshop** – BD will work with the Customer to:
 - Revisit and review initial policies that were created,
 - Provide Policy starter guidance and suggestions for the customer's goals, and
 - Link policies into Alert workflow and create distribution jobs
- **Advanced CI/CD Workflows** – BD will review the CI/CD environment and provide guidance on implementing more advanced functionality:
 - Build breaking options, and
 - Incremental scans on pull requests or non-persistent branches.

2.3 Train

Description	QuickStart Plus	Pro	Premier
Self-paced online training	✓	✓	✓
End-user training sessions (Up to 16 participants)		✓	✓

Topics covered include:

- **Administration** – Configuration of Black Duck SCA, including project and user roles, and creating and managing projects.
- **Basic Tool Usage** – Review basic tool functionality, completion of initial scans, and working with scan results.
- **Best Practices** – Training on how Black Duck SCA should scan codebases and integrate them into the Customer's software development lifecycle ("SDLC").

- **Remediation** – Remediation practices dependent on Customer needs, including policy management, security, and license compliance (if applicable).
- **Reporting** – Review Black Duck SCA standard reports, Reporting DB, and REST APIs.

Documentation – BD will make available to Customer a report that will help guide Customer's use and maintenance of Black Duck SCA, which will include:

- A report on how Black Duck SCA is deployed.
- A review of the steps carried out during the implementation.

2.4 Enable

Product	QuickStart Plus	Pro	Premier
Product Adoption Maturity Model (PAMM) assessment	✓	✓	✓
Action Plan	✓	✓	✓
Runbooks			✓

This phase ensures Customer is set up for success and is ready to begin using Black Duck SCA.

PAMM – At the start of this phase, BD will work with Customer to complete a PAMM assessment to measure product adoption. The benefits of the PAMM and obtaining a maturity score is that it provides:

- A well-defined roadmap of activities that can be performed to maximize investment in BD's tools.
- Quantitatively measure the product adoption of AppSec tools, which correlates to the security of the applications they are developing.
- A way to compare their maturity with other organizations in their industry.

Action Plan - Using the results from the PAMM assessment, BD will create an Action Plan outlining the recommended activities for Customer's continued adoption of SCA. The **Action plan** provides Customer with:

- A summary of the steps completed during the execution of the service package;
- The results of Customer's maturity as it relates to BD's product adoption maturity model;
- Recommended next steps to mature Customer's implementation,
- Instructions to access:
 - The Community,
 - Online product training and
 - Webinars.

BD will review the Action Plan with the Customer for final sign-off and transition the Customer to the BD Customer Success team.

Runbooks – For Premier package customers, BD will create a customized Runbook to guide to administer Black Duck SCA and onboard additional codebases. The Runbook will provide Customer with step-by-step instructions on:

- Setting up the project in SCA,

- Detect scanning configuration,
- Integrating with CI/CD automation,
- Enabling policies, and
- IDE Integration.

The Runbook will be customized for Customer's project language(s), CI/CD infrastructure, and SDLC workflow.

3 Scope of Services

Licensed Products covered by the Services Packages:

Product	QuickStart Plus	Pro	Premier
Black Duck SCA installed on-premise or hosted by BD	Hosted	On-premise or hosted	On-premise or hosted
Black Duck SCA Knowledgebase (On-premise installation is restricted to select customers)	Hosted	Hosted	On-premise or hosted
Black Duck Detect	✓	✓	✓
Black Duck Alert	✓	✓	✓

Out of Scope — The following items are considered out of the scope of this Services Package:

- The installation and configuration of the standalone Black Duck Binary Analysis ("BDBA"), the Cryptography Module, and OpsSight; and
- The ongoing updates, maintenance, and support of the on-premise Black Duck SCA server or the Black Duck SCA Knowledgebase.

4 Prerequisites and Dependencies

Entry Criteria — The following is a list of requirements and dependencies that the Customer must meet to enable BD to perform the Services:

1. Provide a primary point of contact with a deep understanding of the requirements.
2. If applicable, download the installation files from GitHub (<https://github.com/blackducksoftware/hub>).
3. Review the Documentation and secure hardware that meets the minimum requirements for Black Duck SCA.
4. Verify that a valid license file for Black Duck SCA has been received.
5. Identify the codebase(s) Black Duck SCA will scan.
6. Ensure successful regular builds (i.e., not using SCA) of the codebase are completed on the build server(s).

7. Provide access to system administration assistance for any hardware or networking issues.
8. Provide office space for the BD while onsite (if applicable).
9. Remote access to Black Duck SCA and build servers.
10. For onsite delivery, provide a workstation for BD with connectivity to:
 - The build server,
 - The Black Duck SCA host, and
 - Access could be through remote desktop or virtual network computing ("VNC"), or direct physical access to those hosts.

If the Customer does not meet the prerequisites and dependencies described above, and to the extent that BD is unable to perform the Services due to the Customer's failure to meet these prerequisites and dependencies, BD will not be obligated to perform the affected Services.

5 Location of Performance of Services

Services will be delivered remotely.

Onsite delivery is available at an additional cost and requires a signed agreement. Travel and expenses for the onsite delivery will be billed separately based on actual costs.

6 Purchasing Agreement

The parties shall mutually agree to the schedule for the performance of the Services, subject to the terms of the Agreement and this Service Package. All Services described within this Services Package must be used within one year of the Start Date set forth in the Purchasing Agreement pursuant to which this Services were purchased. Unused services are non-refundable and non-transferable pursuant to the terms and conditions of the Purchasing Agreement. Performance of Services is subject to scheduling and Customer availability.

End of Services Package