

Black Duck® Coverity® Static Analysis – Implementation Packages

The services described in this Coverity Implementation Package (the "Services") are provided by Black Duck® and/or its Affiliates (collectively, "BD") to Customer in accordance with the terms of this Coverity 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 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 Coverity Implementation Package will have the meaning set forth in the Agreement.

1 Overview

Black Duck's Coverity Implementation packages aid customers who are getting acquainted with Coverity. These packages provide a structured and guided approach to help implement and adopt Coverity.

The Coverity Implementation packages are offered by BD in QuickStart Plus, Pro, and Premier tiers and include:

Description	QuickStart Plus	Pro	Premier
Coverity server deployment	✓	✓	✓
Coverity analysis installation and configuration	1 Codebase 1 Compiler	1 Codebase 1 Compiler	2 Codebase 2 Compilers
Workflow integration		✓	✓
Bug tracking Integration		JIRA/BugZilla	✓
Custom bug tracking Integration			✓
IDE Integration		✓	✓
Instructor-led training for end-users (developers) and Coverity administrators		✓	✓
Onboarding Runbook			✓

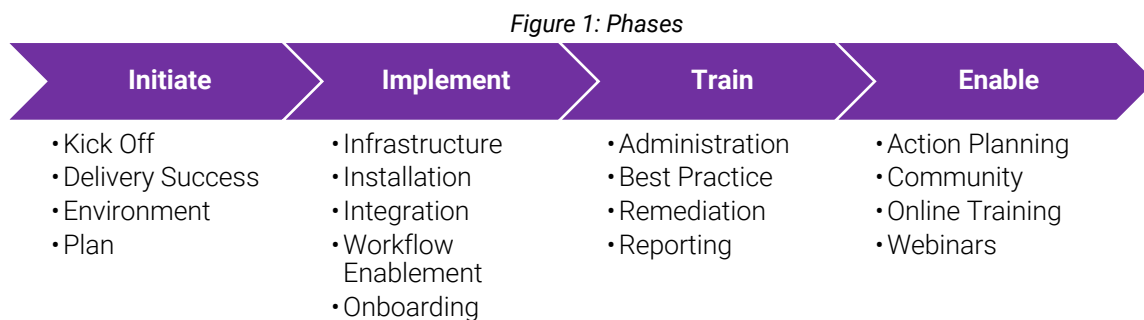
1.1 Package Delivery Success Criteria

Item	Criteria
1	Coverity instance is "Production Ready." • Coverity has been installed and tested in the Customer's environment. • End-user access provisioned and successfully tested. • Maintenance and upgrading procedures have been reviewed and discussed.

Item	Criteria
2	Designated codebase(s) and respective project team(s) have been onboarded per Section 2.2.
3	Coverity best practice guidance 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 Coverity 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 BD best practices and fulfillment of Customer's usage requirements.
8	Customer has been guided on 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 developers onto Coverity and will facilitate developer adoption. The overall process consists of four phases, as described below.



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, and security,
- Project team leader(s) – owner of teams pioneering adoption,
- Integrated application managers – owners of tools/systems with which Coverity 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 – Coverity 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 Coverity implementation process:

- Target goals: short-term, near-term, long-term,
- A sample project plan for the first 90 days, and
- Establish Customer champion and implementation point of contact.

Environment – Establish the initial environmental needs.

- Coverity Server and Analysis deployment method.

Plan – Identify a plan of action designed to ensure Services are completed in a timely manner.

2.2 Implement

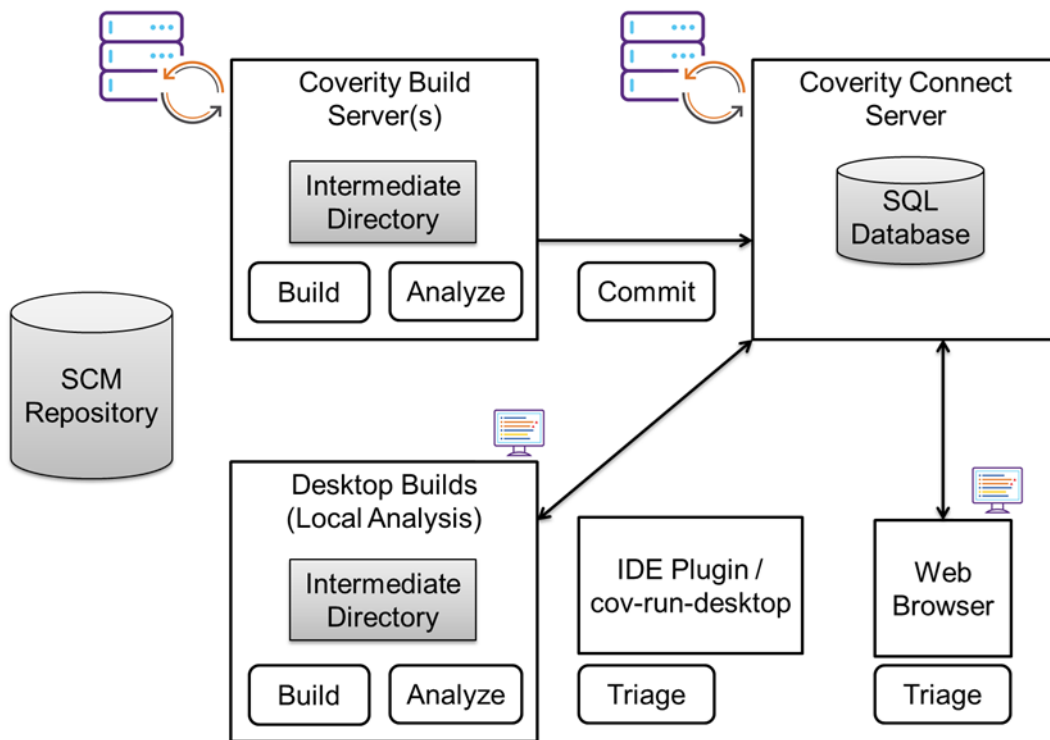
2.2.1 Infrastructure Deployment

BD will assist with the installation and configuration of Coverity per Customer's selected implementation package:

Description	QuickStart Plus	Pro	Premier
Coverity Connect Server installed on one (1) host server	✓	✓	✓
Coverity Analysis installed on build server(s)	1 Build Server	1 Build Server	2 Build Servers
User authentication integration with Lightweight Directory Access Protocol("LDAP")/Security Assertion Markup Language("SAML")	✓	✓	✓
Automatic backup configuration	✓	✓	✓
Triage store configuration		✓	✓
Desktop Analysis (integrated development environment ("IDE") plugin) installation			✓
Role-based access control ("RBAC") configuration			✓
Codebase(s) onboarded	1 Codebase 1 Compiler	1 Codebase 1 Compiler	2 Codebases 2 Compilers

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

Figure 2: System Architecture



Coverity Connect Server — Web application and database installed on a dedicated machine that receives, merges, and stores the detected issues reported by Coverity Analysis. The server provides visual tools for exploring the detected issues and a set of administration user interfaces (“UIs”) and Representational State Transfer (“REST”) application program interfaces (“APIs”) for configuring and managing Coverity.

Coverity Build Server(s) / Desktop Builds — Coverity Analysis is deployed on build server(s) or developer desktops alongside the codebase's native build process. Coverity Analysis builds and analyzes the codebase at compile-time and communicates with the Coverity Connect Server to commit detected issues and other analytics.

IDE Plugin / cov-run-desktop — Coverity Desktop Analysis tools can be used from the command line, an IDE, or various text editors. Desktop Analysis allows quick source code analysis for a subset of files, checking for issues as it is written by Customer.

2.2.2 Codebase Onboarding

BD will assist with the onboarding of the in-scope codebase(s) onto Coverity to meet the usage plans described in this Services Package:

Description	QuickStart Plus	Pro	Premier
Configuration of Coverity Analysis on build server(s)	1 Build Server	1 Build Server	1 Build Server
Analysis will be configured for in-scope codebase(s)	1 Codebase 1 Compiler	1 Codebase 1 Compiler	2 Codebases 2 Compilers
Project(s) and stream(s) created and configured for in-scope application(s)	✓	✓	✓
Checker tuning and configuration		✓	✓

Description	QuickStart Plus	Pro	Premier
Issue baselining		✓	✓
Issue remediation and initial triage		✓	✓

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, and
- 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.

Issue Baselining / Checker Tuning and Configuration – As part of the Pro and Premier packages, BD will work with Customer's representative developers to inspect the first set of issues and establish a baseline for the in-scope codebase(s). Through discussions and review of issue reports, BD will assist the Customer in identifying critical issues and prioritizing issues for remediation.

- BD and the Customer will gain an understanding of the types of issues considered critical/must fix.
- BD will recommend a set of checkers and analysis options to the Customer for focused remediation efforts.
- BD will select critical issues to review with Customer stakeholders.

Analysis options will be adjusted, and a baseline analysis will be generated for tracking issue detection and removal trends.

Issue Remediation and Initial Triage – As part of the Pro and Premier packages, BD will work with the Customer to categorize and triage issues based on Customer's knowledge of their codebase and the agreed-upon criticality level of errors detected. As part of this process, "must-fix" and "high" impact issues will be identified.

BD will help establish a plan to eliminate critical issues from the codebase and facilitate adoption. Customer will be advised on how to establish their success criteria and metrics for issue elimination.

2.2.3 Workflow Integration

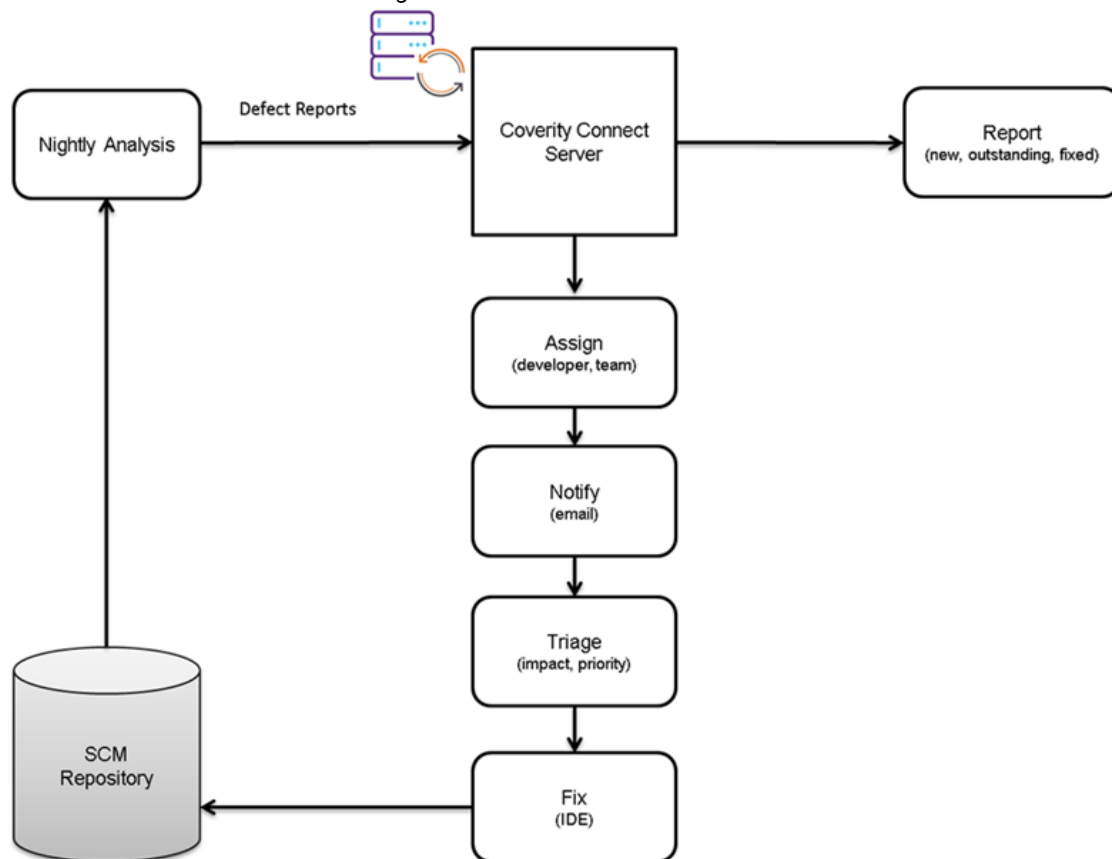
BD assists with the integration of Coverity with Customer tools and development processes. The following tasks will be completed for each in-scope application:

Description	QuickStart Plus	Pro	Premier
Configure Component Maps	✓	✓	✓
Email notification setup and configuration	✓	✓	✓
Automate Coverity Analysis process with build automation or continuous integration/continuous development ("CI/CD")		✓	✓
Enable SCM integration and issue automatic ownership assignment		✓	✓

Description	QuickStart Plus	Pro	Premier
Desktop Analysis (IDE plugin) configuration		✓	✓
Bug tracking system integration with JIRA		✓	✓
Break-the-build Workflow			✓
Custom bug tracking system integration			✓

Issue Resolution Workflow – A best practice is implementing an issue resolution workflow, a standardized process whereby developers are assigned and notified of issues that must be addressed. BD will enable the remediation of the workflow based on the scope of the selected service package.

Figure 3: Issue Resolution Workflow



Developer workflows usually include integration with SCM and issue-tracking systems.

SCM Integration – This automates issue ownership by identifying the last developer to change the source file in which an issue is found. As part of the Pro and Premier packages, one (1) supported SCM system will be integrated.

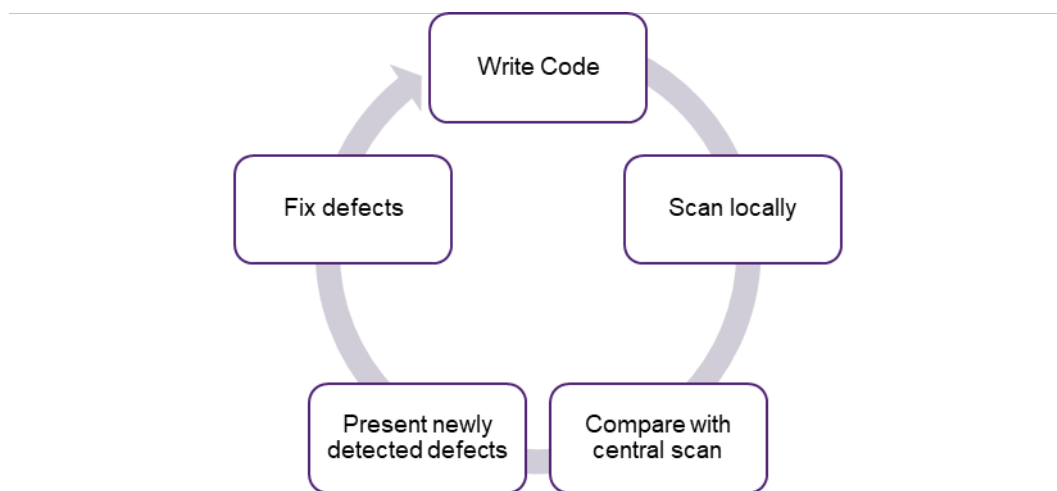
Automated Email Notification – A script will be provided to trigger emails to interested parties of new or outstanding issues. Alerts will be sent to developers assigned a new issue in the past 24 hours, while managers will receive the complete list of new issues.

Issue Tracking System Integration – Users can explicitly promote an individual issue from the Coverity database by clicking the “Export” button available from the Coverity Connect graphical user interface (“GUI”). Based on the package tier, one (1) supported issue tracking system will be integrated and configured for one (1) Coverity Connect server. Premier package Customers who use a custom issue tracking system will be provided a script for integration.

Break-the-build Workflow – With the Premier package, BD will assist Customer in developing an advanced workflow where Coverity Analysis results can be leveraged to break builds, e.g., in a CI/CD pipeline or a Pull/Merge Request build. A plugin or custom script will be provided for this integration.

IDE-Based Analysis – With the Pro and Premier package, BD will assist in deploying IDE-based analysis to two (2) developer workstations. Developers will be able to scan code on their desktops and compare their results against a centralized scan, presenting them with their unique issues. IDE integration will scan code using BD’s desktop IDE plugins or a custom command-line script.

Figure 4: IDE-Based Integration



Alternatively, a centralized “clean before check-in” workflow may be implemented to report new issues in the files modified as part of a developer’s changeset. To implement such a workflow, the Customer must provide a mechanism to identify developer changesets and require the nightly analysis workflow to be in place.

2.3 Train

Description	QuickStart Plus	Pro	Premier
Self-paced online training	✓	✓	✓
End-user training session (Up to 16 participants)		1	2

Training - Topics include:

- **Administration** – Configuration of users, groups, projects, and streams.
- **Basic Tool Usage & Best Practices** – Review tool functionality, triaging, and results review.
- **Reporting** – Review of Coverity reports and REST APIs.

2.4 Enable

Description	Quickstart Plus	Pro	Premier
Product Adoption Maturity Model (PAMM) assessment	✓	✓	✓
Action Plan	✓	✓	✓
Runbook			✓

This phase ensures Customer is set up for success and is ready to begin using Coverity.

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 are 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, and
- 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 Coverity. The Action plan provides Customer with:

- A summary of the steps completed during the execution of the service package;
- An assessment of Customer's maturity as it relates to BD's product maturity model;
- Recommended next steps to mature Customer's implementation and
- 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.

Runbook – For Premier package customers, BD will create Runbooks to help guide Customer on deploying Coverity and self-onboard additional codebases. The Administrator Runbook will provide Customer with step-by-step instructions on:

- Installing the Coverity Connect Server,
- Configuring Users, Groups, and RBAC,
- Integrations (SMTP, SAML/LDAP), and
- Automated backups and maintenance.

The Onboarding Runbook will provide Customer with step-by-step instructions on:

- Installing Coverity Analysis
- Capturing source code and analyzing it
- Integrating with CI/CD automation

- Reviewing results and triaging
- Reporting and IDE plugin

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

3 Scope of Services

The scope of Services is limited as follows:

Package	Codebase
QuickStart	One (1) codebase, < 1 million LoC and one (1) compiler
Pro	One (1) codebase, < 2 million LoC and one (1) compiler
Premier	Two (2) codebases, < 4 million LoC, and up to two (2) compilers

Licensed Product covered by this Services Package:

Product	Version
Coverity	Currently Supported Versions

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. Download all installer packages of Coverity:
 - Coverity Analysis installer
 - Coverity Platform installer
3. Review the Documentation and secure hardware that meets the minimum requirements for:
 - One (1) Coverity Connect host server
 - One (1) build server for each in-scope codebase
4. Verify receipt of a valid license file for Coverity.
5. Identify the codebases that Coverity will analyze.
6. Ensure a successful regular build (i.e., not using Licensed Product) of each codebase has been completed on the build server.
7. Provide access to system administration assistance for any hardware or networking issues.
8. Provide office space for BD while onsite (if applicable).
9. Remote access to the Connect and build servers.
10. Provide a workstation for BD with connectivity to:
 - The build server;
 - The Coverity Connect host; and
 - Access could be through remote desktop or virtual network computing ("VNC"), or direct physical access to those hosts.

Issue Tracking System Integration Requirements – Issue tracking system (“ITS”) integration requires a command line or web services API for creating and updating issues. The following configuration information must be prepared:

- Command-line API syntax or Uniform Resource Locator (“URL”) to web services API;
- ITS project to be used for exporting issues detected by Licensed Product;
- Username and password for an account with sufficient privileges to create and update issues for the project above; and
- Identify all mandatory fields that must be filled in to create an issue. For any fields with a finite list of possible values, specify the appropriate values to be selected.

The following dependencies are required:

- The Perl or Python programming language is available on the Coverity Connect server;
- The Coverity Connect server can communicate with the ITS server across the network without traffic being blocked or filtered by any intermediary firewall or perimeter device; and
- Provide a test ITS instance and/or test ITS project so that any created issues during testing will not impact production.

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 those prerequisites and dependencies, BD will not be obligated to deliver 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