

Black Duck® Seeker® Interactive Analysis - Implementation Packages

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

1 Overview

BD's Seeker Implementation Packages guide customers who are getting acquainted with our application security tools. These packages provide a structured and guided approach to help with implementation, deployment, and adoption of Seeker.

The Seeker Implementation Packages are offered in Quickstart Plus, Pro, and Premier tiers and include:

Description	Quickstart Plus	Pro	Premier
Seeker server deployment	✓	✓	✓
Seeker server external database and high availability (HA) deployment			✓
Seeker agent deployment	1 Agent	3 Agents	6 Agents
Project settings configuration and automation of application(s)	1 Application	1 Application	2 Applications
Workflow integration		✓	✓
Bug Tracking System integration with JIRA		✓	✓
Custom Bug Tracking System integration			✓
Instructor Led training for End-users and administrators		✓	✓
Runbooks			✓

1.1 Package Delivery Success Criteria

The following table outlines BD's criteria for successfully completing the Seeker Implementation Package.

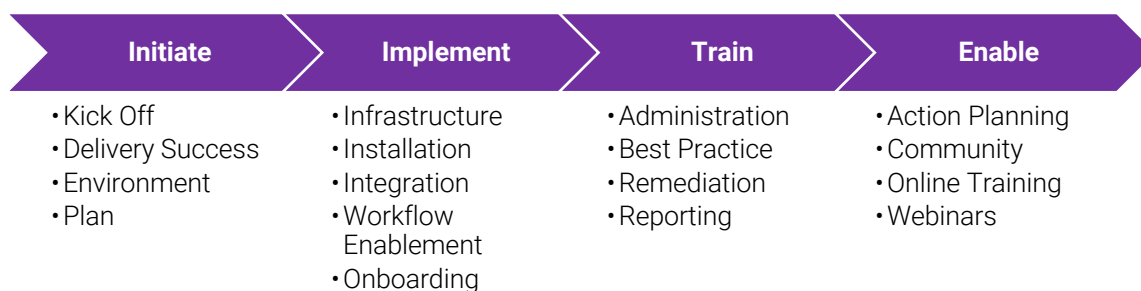
Item	Criteria
1	Seeker installation and configuration: • Seeker Enterprise Server installed on a dedicated machine. • Seeker Enterprise Server is configured (including users, systems, projects, backups, etc.); and • End-user access provisioned and successfully tested
2	Designated application(s) and respective project team(s) have been onboarded as per section 2.2.2 below.
3	Seeker best practice guidance provided to the in-scope codebase(s) project team(s) and designated product champions.
4	In-scope product features have been enabled and demonstrated to the relevant project team(s).
5	Customer administrators have been identified and trained in Seeker administrative functions.
6	The integrations designated in section 2.2.3 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, 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 Approach

BD assists Customer with the deployment of Seeker, the onboarding of the in-scope codebase(s), and facilitate developer adoption.

The process which BD follows consists of the following phases:

Figure 1: Phases



2.1 Initiate

The Initiate Phase will be conducted 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) – the owner of teams pioneering adoption,
 - Integrated Application Managers – owners of tools/systems which Seeker will integrate,
 - Customer Evangelists – members of the Customer's teams identified as the critical leaders for adoption and success,
- **Requirements** – Customer confirmation of elements to be completed for the delivery.
- **Success Criteria** - Confirm the success criteria as they relate to the scope:
 - Production-Ready – Seeker is operational,
 - 3rd Party Integrations – continuous integration/deployment, notifications, bug tracking system,
 - Development Team – trained in scanning best practices, tool usage, and remediation, and
 - Administrators – trained in configuration, tool usage, and reporting.
- **Delivery Process** – Review the Seeker Implementation process:
 - Target goals: short term, near-term, long-term,
 - A sample project plan for the initial 90 days,
 - Establish Customer Champion and Implementation point of contact.
- **Environment** – Establish the initial environmental needs.
 - Seeker Server and Seeker Agent 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

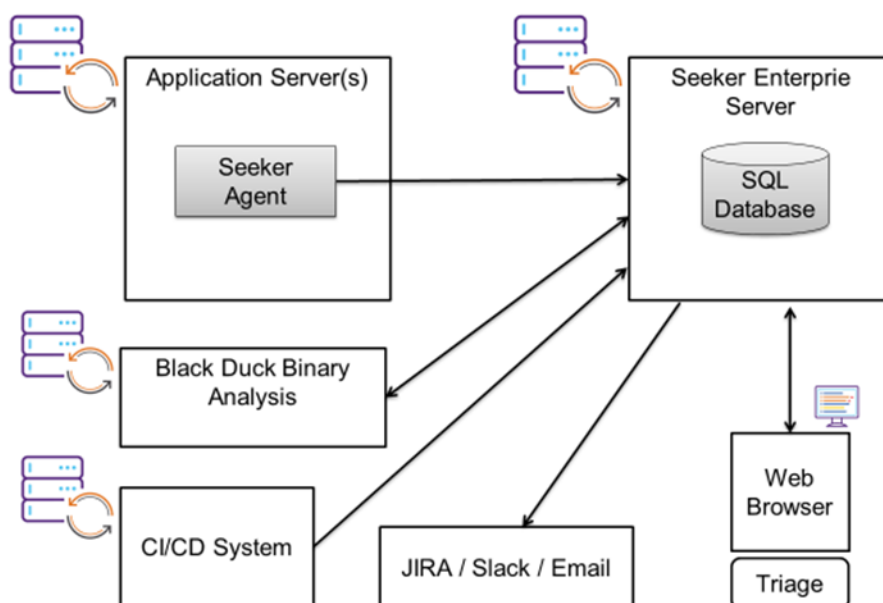
BD will assist with the installation and configuration of Seeker as per the Customer's selected Implementation Package:

Description	Quickstart Plus	Pro	Premier
Installation of the one (1) Seeker Enterprise Server instance	✓	✓	✓
Setup of a highly available Seeker instance and external database			✓
User authentication integration with LDAP/SAML	✓	✓	✓
RBAC configuration			✓
Automatic Backup configuration	✓	✓	✓

Description	Quickstart Plus	Pro	Premier
Black Duck® Binary Analysis installed and configured	✓	✓	✓
Installation of Seeker Agent(s)	1 Agent	Up to 3 Agents	Up to 6 Agents
Application(s) onboarded	1 Application	1 Application	2 Applications

The following diagram approximates a typical system architecture in which the Seeker may be deployed.

Figure 2: System Architecture



Seeker Enterprise Server – The Seeker Web application and database receives, aggregates, and stores the detected vulnerabilities reported by the Agent(s). The server provides visual tools for exploring the detected vulnerabilities and a set of administration UIs and REST APIs for configuring and managing Seeker.

Application Server(s) – Seeker Agent(s) are deployed on the application server(s) alongside the application(s) to be tested. The Agent(s) analyze the application(s) at runtime and communicate with the Seeker Enterprise Server to report detected vulnerabilities and other analytics.

Black Duck Binary Analysis – A virtual appliance image that is hosted on-premise for Software Composition Analysis. Seeker is integrated with Black Duck Binary Analysis to detect known security vulnerabilities in third-party components included in the application(s).

CI/CD System – The installation and deployment of Agent(s) can be automated with Customer's existing CI/CD workflow.

2.2.2 Application Onboarding

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

Description	Quickstart Plus	Pro	Premier
Seeker Agents deployed as part of this service package	1 Agent	Up to 3 Agents	Up to 6 Agents
Number of in-scope applications onboarded with this service package	1 Application	1 Application	2 Applications
Project(s) created and configured for in-scope application(s)	✓	✓	✓
Automatic project version detection and tagging		✓	✓
Checker tuning and configuration		✓	✓
Project Template configuration		✓	✓
Vulnerability baselining		✓	✓
Vulnerability remediation		✓	✓

Agent Configuration – BD works with a representative development team member of Customer to set up the in-scope application as a project in Seeker. The Seeker agents are deployed and configured without impacting other Application Performance Management (APM) tools, and code exclusions are configured to reduce the impact on application performance.

Version Detection – With Pro and Premier packages, BD configures the Seeker Agents to detect the application version automatically and report it back to the Seeker Enterprise server.

Vulnerability Baseline – As part of the Pro and Premier packages, BD will work with representatives from Customer's security team to inspect the initial set of vulnerabilities. Then, through discussion and review of vulnerability reports, BD assists Customers with identifying critical issues and prioritizing vulnerabilities for remediation. Through this process, BD will:

- Educate Customer on the critical/must fix vulnerabilities found on the in-scope application(s);
- Recommend a set of checkers and configurations for focused remediation efforts; and
- Select critical vulnerabilities for review with Customer stakeholders.

Seeker's configuration is tuned to minimize false positives reported by:

- Adjustments to sensitive data identification to identify application-specific sensitive parameters; and
- The addition and configuration of custom sanitizer methods used in the application.

Vulnerability Remediation Plan – As part of the Pro and Premier packages, BD will work with Customer to categorize vulnerabilities using custom tags based on Customer's knowledge of the in-scope application and agreed upon criticality level of vulnerabilities. The result is the identification of the "must-fix" or "critical" vulnerabilities.

BD then collaborates with Customer to determine a plan to remediate critical vulnerabilities from the application and facilitate adoption. In addition, BD advises Customers on how to devise its success criteria and metrics for vulnerability remediation.

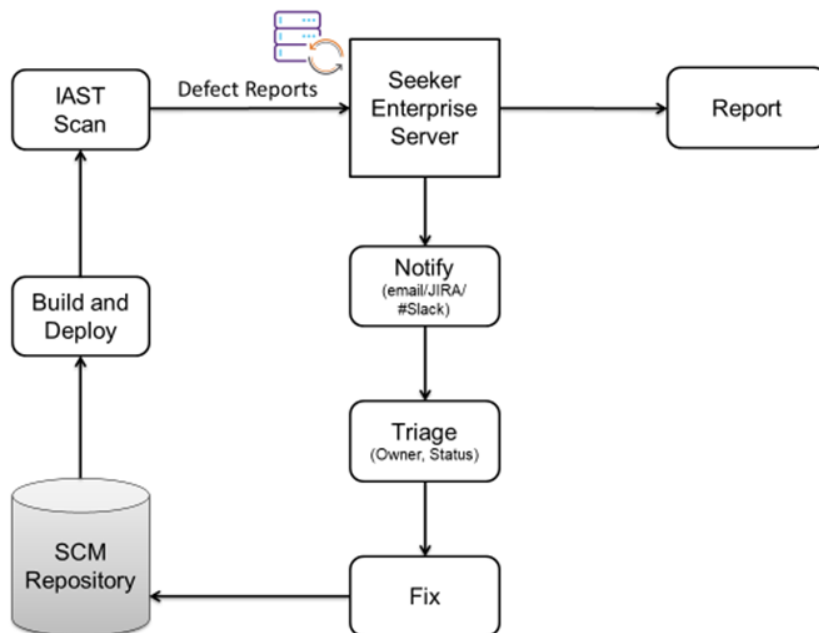
2.2.3 Workflow Integration

BD assists with the integration of Seeker with Customer's tools and development processes. BD will complete the tasks listed in the table below for each in-scope application.

Description	Quickstart Plus	Pro	Premier
Deploy Agent(s) on CI/CD		✓	✓
Notification setup and configuration	✓	✓	✓
Bug Tracking System integration with JIRA		✓	✓
Custom Bug Tracking System integration			✓
Reporting configuration		✓	✓
Policy creation			✓

Vulnerability Resolution Workflow – A best practice is implementing a vulnerability resolution workflow, a standardized process where developers are assigned and notified of vulnerabilities to be addressed. During the completion of the Pro and Premier packages, BD will deliver automation scripts to support such a workflow.

Figure 3: Vulnerabilities Resolution Workflow



Issue Tracking System Integration – Users can set rules or explicitly promote vulnerabilities from the Seeker database from the Seeker Enterprise Server UI. With the Pro service package, integration with one (1) supported bug tracking system (i.e., Jira) is configured, and automatic notifications are enabled.

If the Premier service package is selected, BD will provide a script to integrate Seeker with a custom bug tracking system.

Compliance Policies – Users can set security standards for their software projects in Seeker. If the Premier service package is selected, BD will work with Customer to create these policies based on Customer's requirements.

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 of tool functionality, triaging, and results review.
- **Reporting** – Review of Seeker reports and REST APIs.

2.4 Enable

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

The Enable phase ensures Customer is set up for success and is ready to begin using Seeker.

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 Seeker. 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 Seeker and self-onboard additional codebases. The Administrator Runbook will provide Customer with step-by-step instructions on:

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

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

- Attaching agents to applications
- Integrating with CI/CD automation
- Reviewing results and triaging
- Reporting

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

3 Scope of Services

Licensed Product covered by this Services Package:

Product	Version
Seeker	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. Verify that a valid license file for the Licensed Product has been received.
3. Review the Documentation and secure hardware that meets the minimum requirements for Seeker.
4. Identify the Project Team(s) the BD consultant will work with for the service delivery.
5. Provide access to Infrastructure, Security, Database, and Network teams to assist with any hardware or networking issues.
6. Remote access for Hands-On activities by BD staff is available.
7. Provide office space for the BD consultant if onsite.

If Customer does not meet the prerequisites and dependencies described above, and to the extent that BD is unable to perform the Services because of Customer's failure to meet those prerequisites and dependencies, BD will not be obligated to complete 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