SYNOPSYS®

Coverity and Black Duck Binary Analysis Integration

Identify known vulnerabilities in third-party packages, and triage them in Coverity Connect

Overview

Most software developed today uses third-party or open source components, which often contain vulnerabilities susceptible to cyber attack. Applications in critical areas such as finance, healthcare, and national defense are an especially appealing target for hackers and cyber criminals. In addition, development organizations rarely identify or review third-party licenses, leaving their code susceptible to copyright issues. Our solution integrates Black Duck Binary Analysis results into the standard Coverity defect triage workflow to diagnose potentially expensive vulnerabilities and license issues associated with third-party components.

Black Duck Binary Analysis

Black Duck Binary Analysis is a binary and runtime code analysis platform that addresses the challenges of an increasingly complex and fragmented software supply chain. Black Duck Binary Analysis can scan practically any software or system, including desktop and mobile applications, embedded system firmware, and more. It quickly identifies third-party and open source components, known vulnerabilities, license types, and other potential risk issues.

Coverity Connect

Coverity Connect is a comprehensive, collaborative issue management interface that lets you see code status and health and evaluate and triage findings in a project. Metrics such as the number of new, fixed, and outstanding vulnerabilities provide defect trend data over time.

How the integration works

The integration works with either a Black Duck Binary Analysis cloud instance or an on-premises installation. A new Coverity Connect instance is provisioned (or an existing one reused), and the scripted solution is installed in the customer environment. It automates the process of uploading an application, monitoring the scan, extracting vulnerability and third-party licensing information, and importing the vulnerability information into Coverity Connect. The solution can be configured to scan each new version of an application automatically to reveal new vulnerabilities and whether old ones have been fixed.

Essentials

Black Duck Binary Analysis identifies critical vulnerabilities and license information in third-party components in an application.

Scripted solution

- Imports Black Duck Binary Analysis vulnerabilities into Coverity Connect
- Calculates the CVSS score and severity for each vulnerability
- Shows new and fixed vulnerabilities between versions

Detailed findings

- Link to Black Duck Binary Analysis project with bill of materials
- Link to National Vulnerability Database
- Copyright information
- Automatic merging of similar vulnerabilities into one defect

Contact Synopsys sales for more information.

Presentation of findings

The integration provides a developer-friendly presentation of findings in Coverity Connect for evaluation and triage. Scan results include technical descriptions of vulnerabilities, Common Vulnerability Scoring System (CVSS) scores, and CVSS severity ratings. For each vulnerability identified by Black Duck Binary Analysis, Coverity Connect contains links to additional data where needed, such as the comprehensive bill of materials. Management and security teams can review the trend reports to keep track of the risk profile of each application.

Key benefits

The Black Duck Binary Analysis and Coverity integration provides superior results:

- **Efficient.** Quickly scan virtually any software or firmware for known vulnerabilities.
- **Comprehensive.** Identify both software quality and security issues in code (Coverity) and vulnerabilities in software components (Black Duck Binary Analysis).
- **Convenient.** See all vulnerability results in one familiar interface—Coverity Connect—with helpful links to appropriate data.
- **Revealing.** Perform supply chain management with the help of the powerful Coverity Connect user interface for managing vulnerabilities.
- **Actionable.** Proactively combat code decay. Get alerts for newly discovered vulnerabilities that affect previously scanned software, and see which vulnerabilities have been fixed in newer versions of software.

Summary

The Black Duck Binary Analysis and Coverity integration provides critical visibility into security vulnerabilities in third-party code. With Coverity Connect, both engineering and IT security teams can pinpoint the vulnerabilities affecting their applications and establish an action plan for a targeted review of third-party vulnerabilities and licensing information. In the long term, your organization can establish a companywide policy to manage third-party code, building on the Black Duck Binary Analysis and Coverity integration.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

01/30/19.ds-coverity-blackduck-binary.