SYNOPSYS®

Synopsys Software Composition Analysis (Protecode) and Static Analysis (Coverity) Integration

Identifies known vulnerabilities in third-party packages and provides the ability to triage them within Coverity Connect

What problems does this integration solve?

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, medicine, and national defense are an especially appealing target of hackers and cyber criminals. In addition, third-party licenses are rarely identified or reviewed in full and are thus susceptible to copyright issues. Our solution uses Synopsys Software Composition Analysis (Protecode) and the standard Synopsys Static Analysis (Coverity) defect triage workflow to diagnose potentially expensive vulnerabilities associated with third-party components.

What is Synopsys Software Composition Analysis (SCA)?

Synopsys SCA is a binary and run-time code analysis platform that addresses the challenges of an increasingly complex and fragmented software supply chain. Synopsys SCA quickly identifies third-party and open source components, known vulnerabilities, license types, and other potential risk issues. Because Synopsys SCA analyzes binary code, as opposed to source code, it can scan practically any software or system, including desktop and mobile applications, embedded system firmware, and more.

What is 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 outstanding, new, and fixed vulnerabilities provide defect trend data over time.

The Synopsys SCA and Static Analysis Integration

The integration works with either a Synopsys SCA cloud instance or an on-premises installation and consists of the following steps:

1. A Coverity Connect instance is provisioned, or a pre-existing one is reused.
2. The scripted solution is installed within 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.
3. Developers and security teams review the scan results (technical description, Common Vulnerability Scoring System [CVSS] score, and CVSS severity rating) to triage each vulnerability.

4. Automation can be enabled to scan newer versions of the same application to reveal which vulnerabilities are fixed, which ones still exist, and any new ones that are introduced.

Presentation of findings

The integration provides a developer friendly presentation of findings within Coverity Connect for evaluation and triage. Management and security teams can review the trend reports to keep track of the risk profile of each application.

Benefits

The Synopsys SCA and Static Analysis Integration provides superior results with its customer-focused qualities:

- **Convenient:** See all vulnerability results in one familiar place—Coverity Connect.
- **Revealing:** Perform supply chain management with the help of the powerful Coverity Connect user interface for managing vulnerabilities.
- **Efficient:** Scan virtually any software or firmware quickly for known vulnerabilities.
- **Informative:** See how each vulnerability shown in Coverity Connect links to the appropriate data in Synopsys SCA, such as the comprehensive Bill of Materials.
- **Comprehensive:** Use Synopsys Static Analysis to identify software quality and security issues and SCA to see vulnerabilities in software components, all in a single interface.
- **Actionable:** Proactively combat code decay by receiving alerts for newly discovered vulnerabilities that affect previously scanned software. See which vulnerabilities have been fixed in newer versions of software.

ESSENTIALS

Synopsys SCA identifies critical vulnerabilities and license information in third-party components within an application.

Scripted solution

- Imports Synopsys SCA vulnerabilities into Coverity Connect
- Calculates the CVSS score and severity for each vulnerability
- Shows new and fixed vulnerabilities between versions

Detailed findings

- Link to Synopsys SCA Project with Bill of Materials
- Link to National Vulnerability Database
- Copyright information
- Automatic merging of similar vulnerabilities into one defect

Contact Synopsys sales for additional information.

Summary

The Synopsys SCA and Static Analysis Integration provides critical visibility into security vulnerabilities in third-party code. With Coverity Connect, both engineering and IT security teams can pinpoint the specific 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 Synopsys SCA and Static Analysis Integration.

The Synopsys difference

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We've united leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. We don't stop when the test is over. As a recognized leader in application security testing, we offer onboarding and deployment assistance, remediation guidance, and training solutions that empower you to optimize your investment.

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™