Kiuwan Insights

This section guides you through the functions of Kiuwan Insights.

Contents:

- Introduction to Kiuwan Insights
- Components Inventory
  - Supported languages and resources
  - Database vulnerabilities
- Security, Obsolescence, and Licensing

Kiuwan Insights Dashboard:

- Insights Components
- Insights Obsolescence
- Insights Licenses
- Insights Security

Introduction to Kiuwan Insights

Many applications incorporate external **open source and third-party components** that enable developers to build new functionality quickly and efficiently. But while the use of open source components has many benefits, it also introduces risk. Kiuwan Insights helps you manage this risk by providing answers to the key questions described below.

Common questions with 3rd party components

- **Do you have a complete inventory of the 3rd party components being used by your software?**

  If you are a developer you most probably know the answer to this question. But if you are in a position closer to management, likely, you don't know the answer. Modern applications, in most cases, are using open source components and yours will not be an exception. And, although the benefits are clear, you might be thinking of some inherent risks.

- **Do you know the degree of security breaches introduced by those 3rd party components?**
  You most probably are dedicating a lot of effort to remediate security vulnerabilities in your software, but those efforts are useless if 3rd components are vulnerable. As you know, any security vulnerability makes the whole application vulnerable.

- **Do you know if those components are obsolete?**
  You might be using "outdated" components or, even worse, "dead" components. Old versions might be introducing security breaches or bugs that are solved in newer versions. Or even worse, what would happen if those buggy components are *dead*, i. e. are not being updated?

- **Are you aware of legal licensing implications of using those 3rd party components?**

  Many 3rd party components are *Copyleft* licensed. In a broad sense, these kind of licenses mean that, although you are allowed to use that software in your application, once you have included them in your application, the whole application becomes *Cop yleft* licensed, i.e. you are implicitly giving every person who receives a copy of your software permissions to reproduce, adapt, or distribute it. Is this your intention? If not, you should identify all the Copyleft components you are using in your application and act accordingly.

Kiuwan Insights comes to answer all these questions by providing:

1. a complete **components inventory** of 3rd party software used by your applications, and
2. detailed information on **security**, **obsolescence** and **licensing risks** of those components

Components Inventory

Kiuwan Insight analyzes your application software, discovering all external dependencies, and builds a **components inventory** that lets you track any external piece of code that could be part of your application.

Go to **Insights** > **Components** to access the components inventory.

Supported languages and resources

Kiuwan Insights uses the following resources to extract information on 3rd party dependencies.

Supported languages	Supported repositories	Supported build systems	Repositories Used	Database Vulnerabilities Used	Licenses extract from
Go	• GitHub	• go.mod • Gopkg.lock	GitHub: https://github.com/	• NVD: https://nvd.nist.gov/	• GitHub
Java	• Maven • Gradle	• Ant (*.xml files) • Maven (pom.xml files) • Gradle (*.gradle files) • *.jar, *.war, *.ear files	Maven (central or others configured in settings.xml or pom.xml files): https://repo.maven.apache.org/maven2/	• NVD: https://nvd.nist.gov/	• pom.xml • License file into jar file.
Javascript	• Npm • Bower	• Npm (package.json files) • Bower (bower.json files) • Yarn (package.json files)	Npm: https://www.npmjs.com/	• NVD: https://nvd.nist.gov/	• NPM Rest services.
Kotlin	• Maven • Gradle • Ant	• Ant (*.xml files) • Maven (pom.xml files) • Gradle (*.gradle and *.gradle.kts files)	Maven (central or others configured in settings.xml or pom.xml files): https://repo.maven.apache.org/maven2/	• NVD: https://nvd.nist.gov/	• Maven services
.Net	• Nuget	• Nuget (*.csproj, project.json, global.json, *.vbproj files)	Nuget: https://www.nuget.org/	• NVD: https://nvd.nist.gov/	• Nuget Rest services.
Php	• Packagist	• Composer (composer.json, composer.lock files)	Packagist: https://packagist.org/	• NVD: https://nvd.nist.gov/	• NVD: https://nvd.nist.gov/

Python	• PyPI • GitHub	• PyPI (setup.py files) • Requirements (txt file with declared dependencies)	PyPI: https://pypi.org/	• NVD: https://nvd.nist.gov/	• PyPI Rest services
Ruby	• RubyGems	• Gemfile, Gemfile.lock and *.gemspec files	RubyGems: https://rubygems.org/	• NVD: https://nvd.nist.gov/ • Bundler audit database	• License and obsolescence pending
Scala	• Maven	• SBT (build.sbt)	Maven (central or others configured in settings.xml or pom.xml files): https://repo.maven.apache.org/maven2/	• NVD: https://nvd.nist.gov/	• pom.xml.
Swift	• Cocoapods • GitHub	• Podspec (*.podspec, Podfile.lock files) • Package (Package.swift files)	Repository Podspec in Github: https://github.com/CocoaPods/Specs	• NVD: https://nvd.nist.gov/	• podspec.json of the component.

Database vulnerabilities

NVD: https://nvd.nist.gov/

From these sources, Kiuwan Insight builds the Components Inventory of your application.

You can add your specific private (local or remote) and/or public repositories by properly configuring Kiuwan Local Analyzer.

Please visit Insights - Additional Maven repositories for further information.

Security, Obsolescence, and Licensing

At a glance, Kiuwan Insights provides detailed information and visual indicators that quickly let you know the different levels of risk associated with every external component.

Every component is assigned a level (High, Medium, Low or None) on three different risk metrics:

- **Security Risk** (due to vulnerabilities introduced by components)
- **Obsolescence Risk** (due to using obsolete components)
- **License Risk** (due to legal implications of used components' licenses)

Security information is available at **Insights > Security**

Obsolescence information is available at **Insights > Obsolescence**

Licensing information is available at **Insights > Licenses**