Software Security Course

The CodeWeTrust's source code scanner

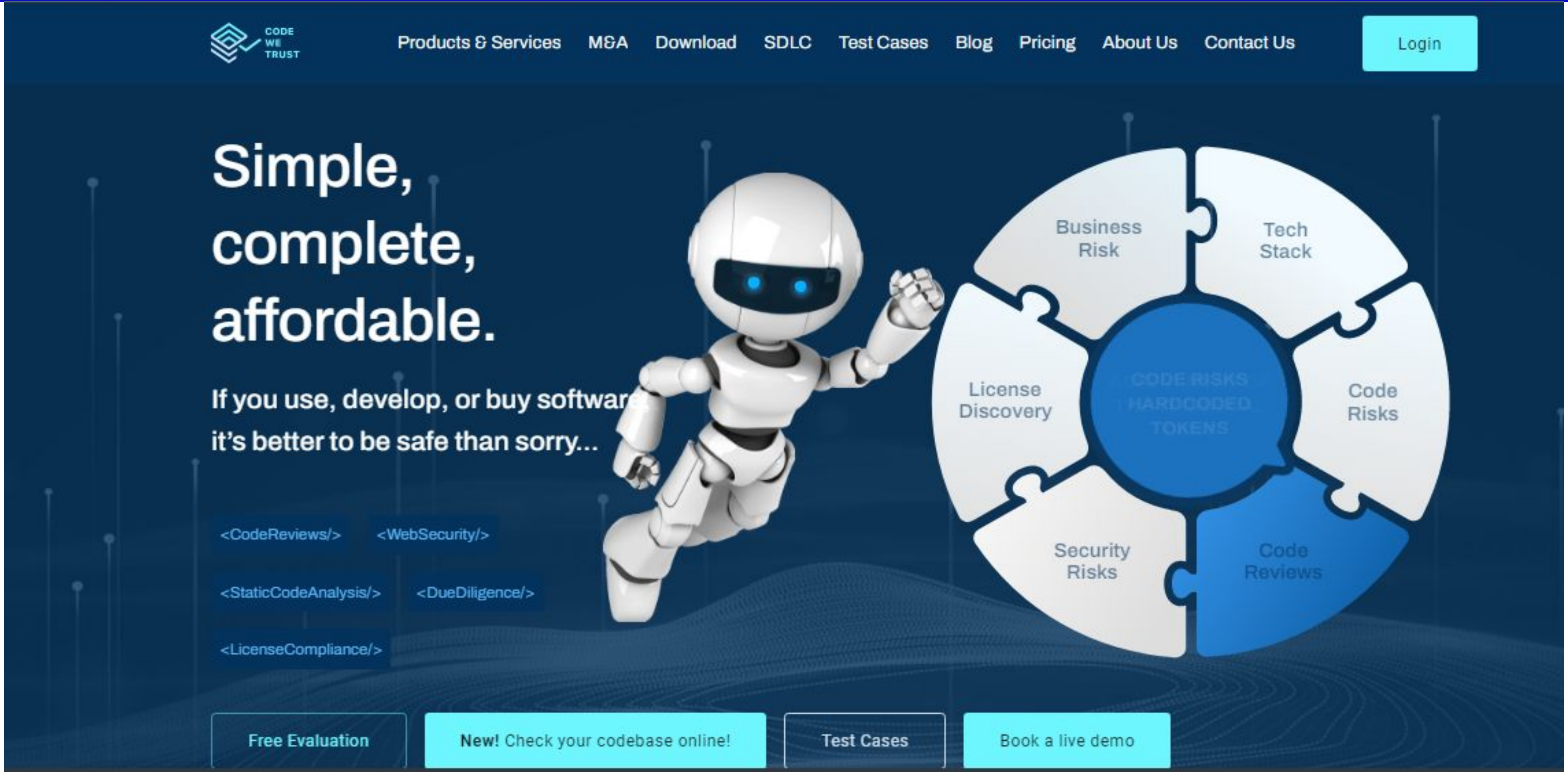
C. Voliotis

Trustillio- CodeWetrust
Department of Informatics
University of Piraeus

Overview of CodeWeTrust's c2m

Part 1

Introduction (website)



Simple, complete, affordable.

If you use, develop, or buy softwar it's better to be safe than sorry...

source code scanning key advantages

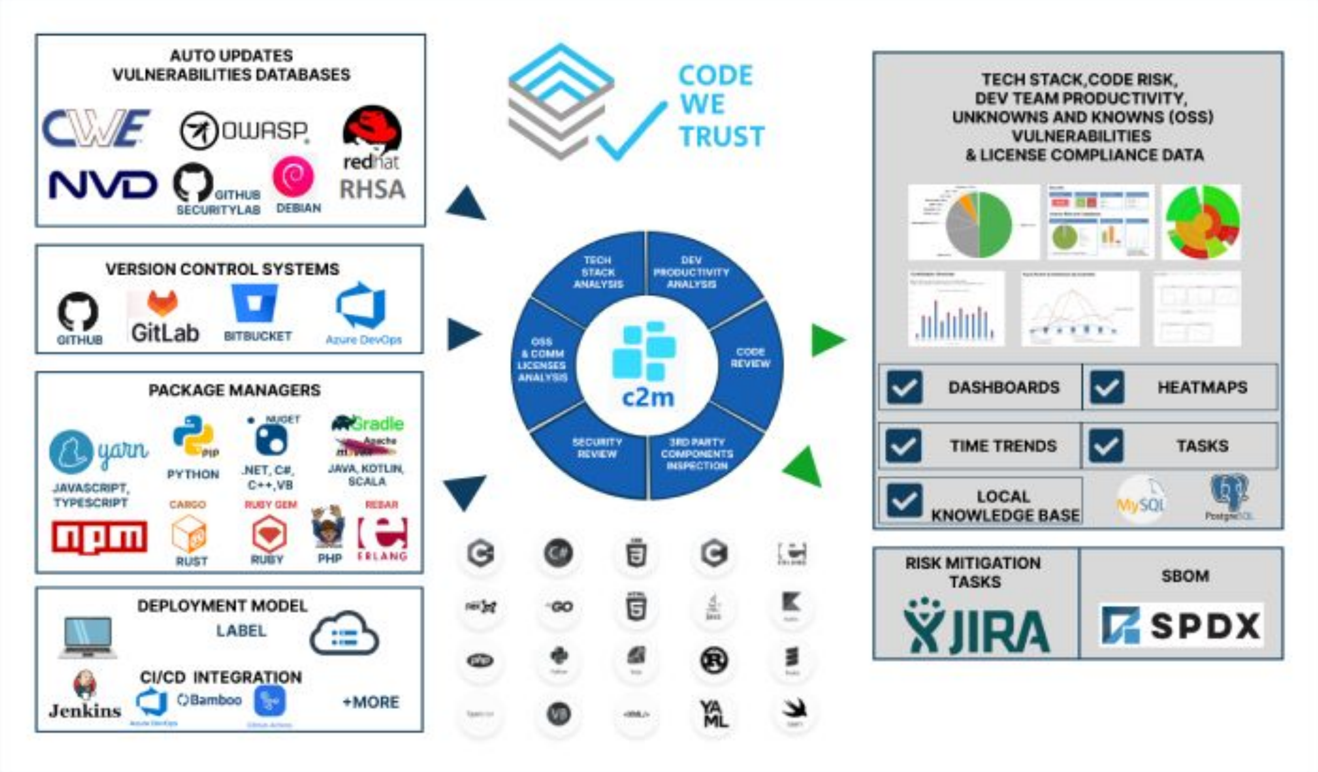
"BLIND" AUDIT
SOURCE CODE ASSESSMENT
WITHOUT CODE SHARING

EVALUATION OF
PROPRIETARY AND 3RD PARTY CODE
SOURCE CODE ANALYSIS + SOFTWARE COMPOSITION ANALYSIS+ SECURITY PRODUCTIVITY

AUTOMATED SELF-SERVED
CONSISTENT AUTO-GENERATED REPORTS SLIDES, DASH BOARDS, JIRA

LOW ADOPTION COST
ON-PREM OR HOSTED,GET CODE FROM GITHUB, GITLAB, BITBUCKET, AZURE, LOCAL DISK
SUPPORTS 99% OF THE USED TECH STACKS

WHITE-LABEL VERSION
AVAILABLE ON ANNUAL ENTERPRISE PLANS ONLY



AUTO UPDATES
VULNERABILITIES DATABASES

VERSION CONTROL SYSTEMS

PACKAGE MANAGERS

DEPLOYMENT MODEL
LABEL
CI/CD INTEGRATION

+MORE

CODE WE TRUST

TECH STACK ANALYSIS
DEV PRODUCTIVITY ANALYSIS
CODE REVIEW
3RD PARTY COMPONENTS INSPECTION
SECURITY REVIEW
OSS & COMM LICENSES ANALYSIS
c2m
GO
YAML

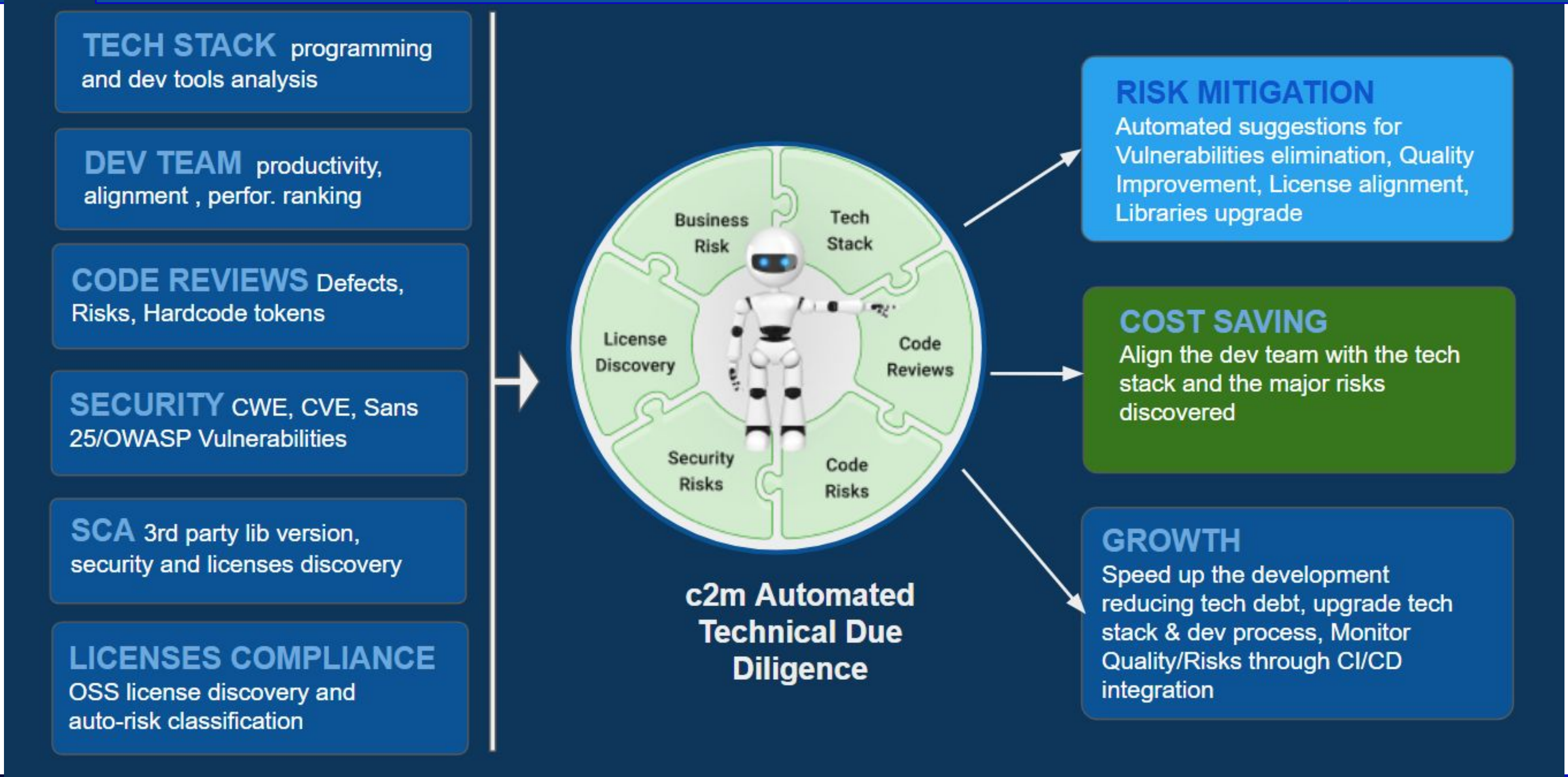
TECH STACK,CODE RISK,
DEV TEAM PRODUCTIVITY,
UNKNOWNS AND KNOWNS (OSS)
VULNERABILITIES
& LICENSE COMPLIANCE DATA

☑ DASHBOARDS
☑ HEATMAPS
☑ TIME TRENDS
☑ TASKS
☑ LOCAL KNOWLEDGE BASE

RISK MITIGATION TASKS

SBOM

C2m at a glance!



TECH STACK programming and dev tools analysis

DEV TEAM productivity, alignment , perfor. ranking

CODE REVIEWS Defects, Risks, Hardcode tokens

SECURITY CWE, CVE, Sans 25/OWASP Vulnerabilities

SCA 3rd party lib version, security and licenses discovery

LICENSES COMPLIANCE OSS license discovery and auto-risk classification

c2m Automated Technical Due Diligence

RISK MITIGATION
Automated suggestions for Vulnerabilities elimination, Quality Improvement, License alignment, Libraries upgrade

COST SAVING
Align the dev team with the tech stack and the major risks discovered

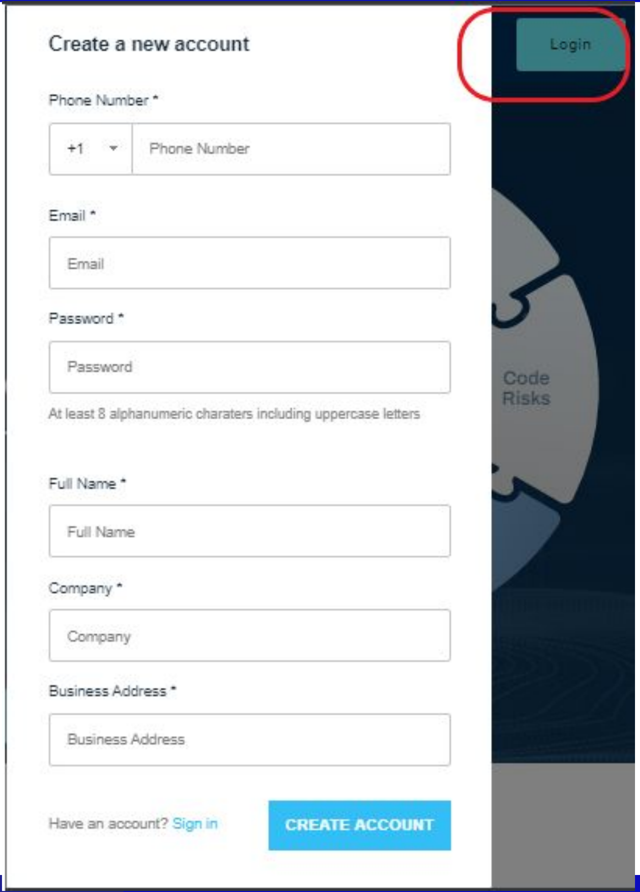
GROWTH
Speed up the development reducing tech debt, upgrade tech stack & dev process, Monitor Quality/Risks through CI/CD integration

Onboarding on CodeWeTrust's c2m

Part 2

Onboarding steps

1. Join the CodeWeTrust’s portal using your corporate email account. Personal email accounts (gmail.com, hotmail.co etc will be rejected(
2. CodeWetrust will upgrade your account license to “FULL ACCESS” upon notification.
3. You could use the University Staging or you could download and install the app at your workstation (laptop, PC). Download Page+Specs : Download c2m 'Light' | Code We Trust
4. Installation guide: C2M- Quick User Guide - codewetrust
5. Online manual: https://c2m-codewetrust.gitbook.io/codewetrust/c2m-user-guide/user-guide-ver-6.0.0



Create a new account

Phone Number *

+1 ▾ Phone Number

Email *

Email

Password *

Password

At least 8 alphanumeric charaters including uppercase letters

Full Name *

Full Name

Company *

Company

Business Address *

Business Address

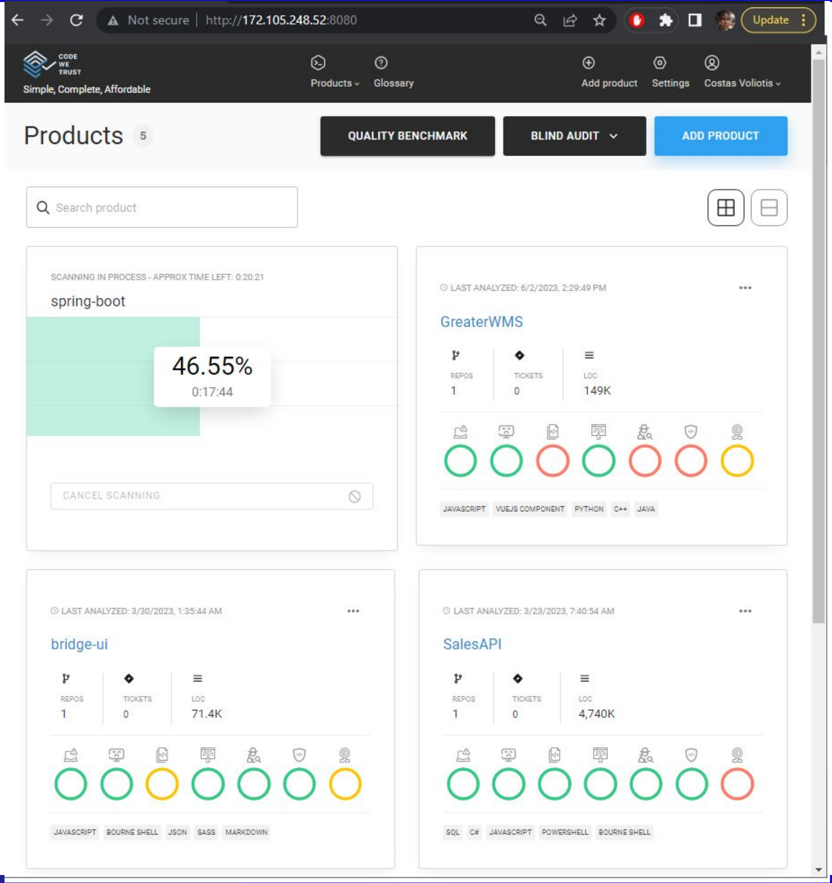
Have an account? Sign in

Prerequisites for local installation

1. Docker engine (Install Docker Engine) with 10+ GB RAM and 20+ GB disk space for containers, x64 CPU.
2. Deactivate the sleep mode. This very important because when thepc/laptop enters on sleep mode the process is interrupt sharply.
3. The c2m application should be with Administrator privileges so to have access c:\users\appData, where the temporary results re stored.
4. Although the c2m application is carefully tested on Windows, Linux and MacOS, we suggest the installation on Linux systems.

Getting started with c2m scanner

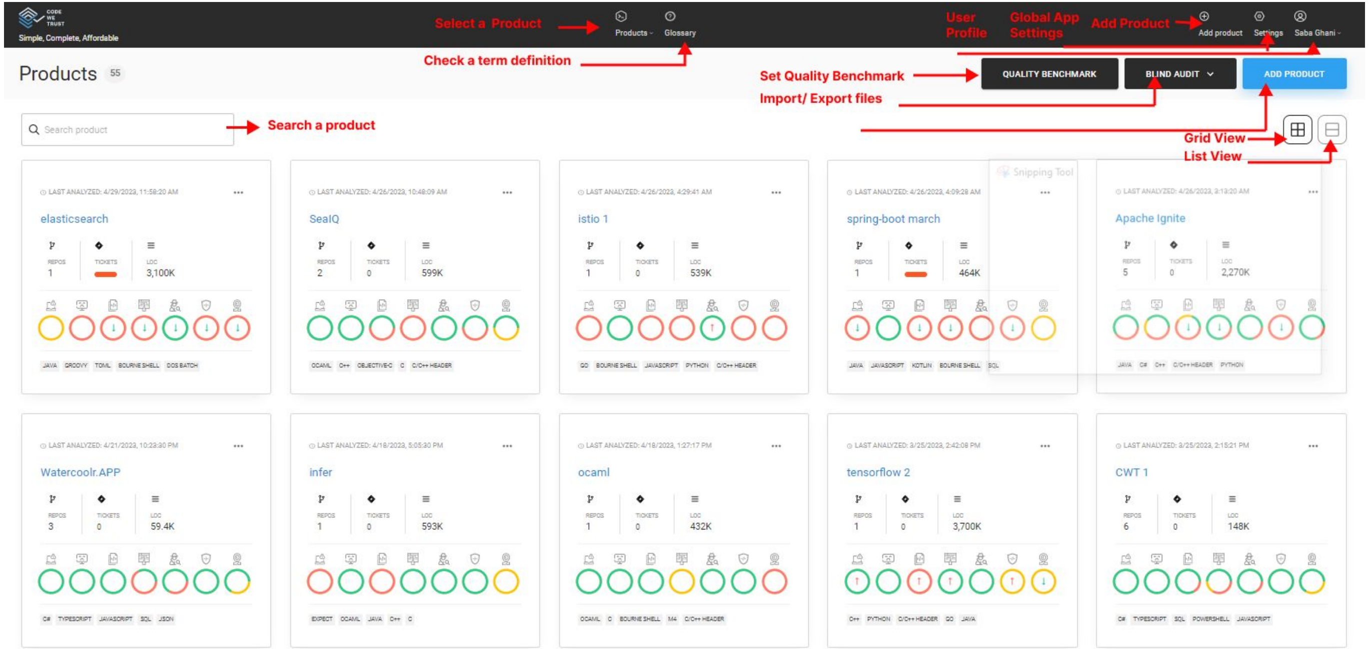
1. Login to portal: https://univpiraus-security-sdlc.dd.codewetrust-api.com/
2. Inspect the scorecards on dashboard page
3. The screenshot on the left is shown that “springboot” is analysed and few more products are already scanned
4. Click on any of the scorecards



Product Dashboard

The product dashboard page shows all the products scanned so far.

You can add new product, view profile, change/ view settings, set quality benchmark and the import or export the files using blind audit.



Products 55

Search product

LAST ANALYZED: 4/29/2023, 11:58:20 AM
elasticsearch
REPOS 1 · TICKETS · LOC 3,100K
JAVA · GROOVY · TOML · BOURNE SHELL · DOS BATCH

LAST ANALYZED: 4/26/2023, 10:48:09 AM
SealQ
REPOS 2 · TICKETS 0 · LOC 599K
OCAML · C++ · OBJECTIVE-C · C · C/C++ HEADER

LAST ANALYZED: 4/26/2023, 4:29:41 AM
istio 1
REPOS 1 · TICKETS 0 · LOC 539K
GO · BOURNE SHELL · JAVASCRIPT · PYTHON · C/C++ HEADER

LAST ANALYZED: 4/26/2023, 4:09:28 AM
spring-boot march
REPOS 1 · TICKETS · LOC 464K
JAVA · JAVASCRIPT · KOTLIN · BOURNE SHELL · SQL

LAST ANALYZED: 4/26/2023, 3:13:20 AM
Apache Ignite
REPOS 5 · TICKETS 0 · LOC 2,270K
JAVA · C# · C++ · C/C++ HEADER · PYTHON

LAST ANALYZED: 4/21/2023, 10:23:30 PM
Watercoolr.APP
REPOS 3 · TICKETS 0 · LOC 59.4K
C# · TYPESCRIPT · JAVASCRIPT · SQL · JSON

LAST ANALYZED: 4/18/2023, 5:05:30 PM
infer
REPOS 1 · TICKETS 0 · LOC 593K
EXPECT · OCAML · JAVA · C++ · C

LAST ANALYZED: 4/18/2023, 1:27:17 PM
ocaml
REPOS 1 · TICKETS 0 · LOC 432K
OCAML · C · BOURNE SHELL · M4 · C/C++ HEADER

LAST ANALYZED: 3/25/2023, 2:42:08 PM
tensorflow 2
REPOS 1 · TICKETS 0 · LOC 3,700K
C++ · PYTHON · C/C++ HEADER · GO · JAVA

LAST ANALYZED: 3/25/2023, 2:15:21 PM
CWT 1
REPOS 6 · TICKETS 0 · LOC 148K
C# · TYPESCRIPT · SQL · POWERSHELL · JAVASCRIPT

Support, References and readings

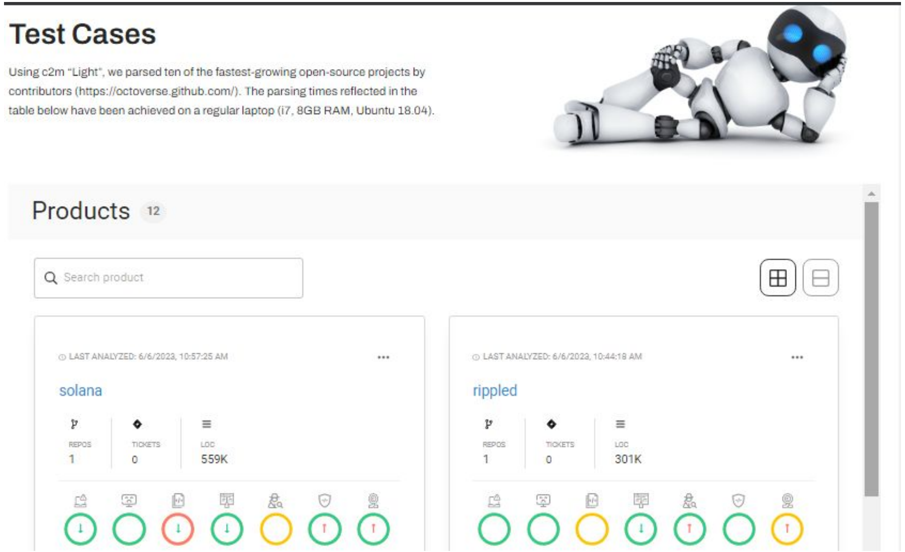
1. CodeWeTrust blog: CodeWeTrust Blog

2. CodeWeTrust Live demo:

   Test Cases | Code We Trust

3. Support Email: support@codewetrust.com

4. Slack : We have a Slack support channel : CWT_UNIVP_SLACK. Ask for invitation (support@codewetrust.com)



Test Cases

Using c2m "Light", we parsed ten of the fastest-growing open-source projects by contributors (https://octoverse.github.com/). The parsing times reflected in the table below have been achieved on a regular laptop (i7, 8GB RAM, Ubuntu 18.04).

Products 12

Search product

LAST ANALYZED: 6/6/2023, 10:57:25 AM

solana

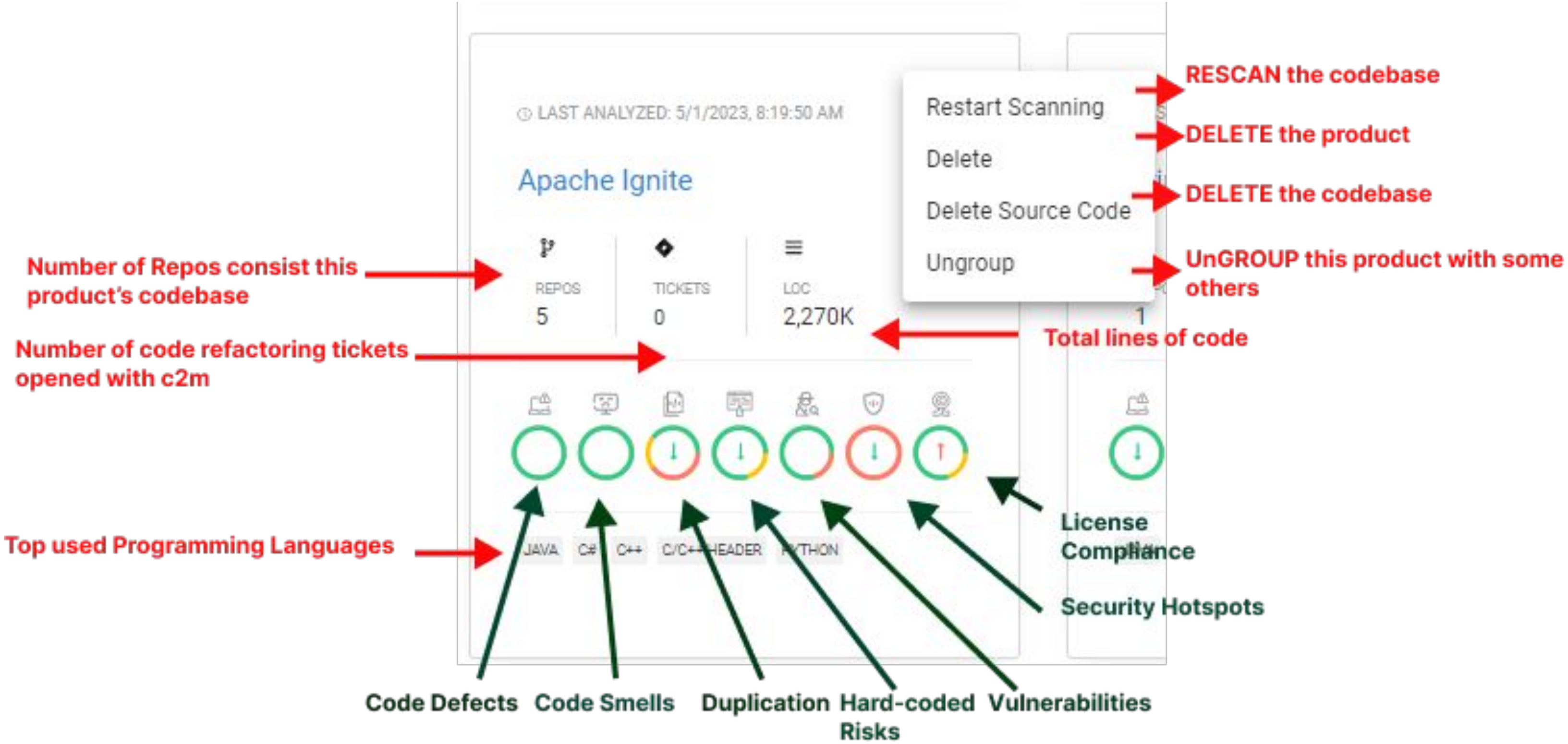
REPOS	TICKETS	LOC
1	0	559K

LAST ANALYZED: 6/6/2023, 10:44:18 AM

rippled

REPOS	TICKETS	LOC
1	0	301K

The product scorecard



LAST ANALYZED: 5/1/2023, 8:19:50 AM

Apache Ignite

REPOS 5

TICKETS 0

LOC 2,270K

Restart Scanning

Delete

Delete Source Code

Ungroup

JAVA C# C++ C/C++ HEADER PYTHON

RESCAN the codebase

DELETE the product

DELETE the codebase

UnGROUP this product with some others

Total lines of code

Number of Repos consist this product's codebase

Number of code refactoring tickets opened with c2m

Top used Programming Languages

License Compliance

Security Hotspots

Code Defects

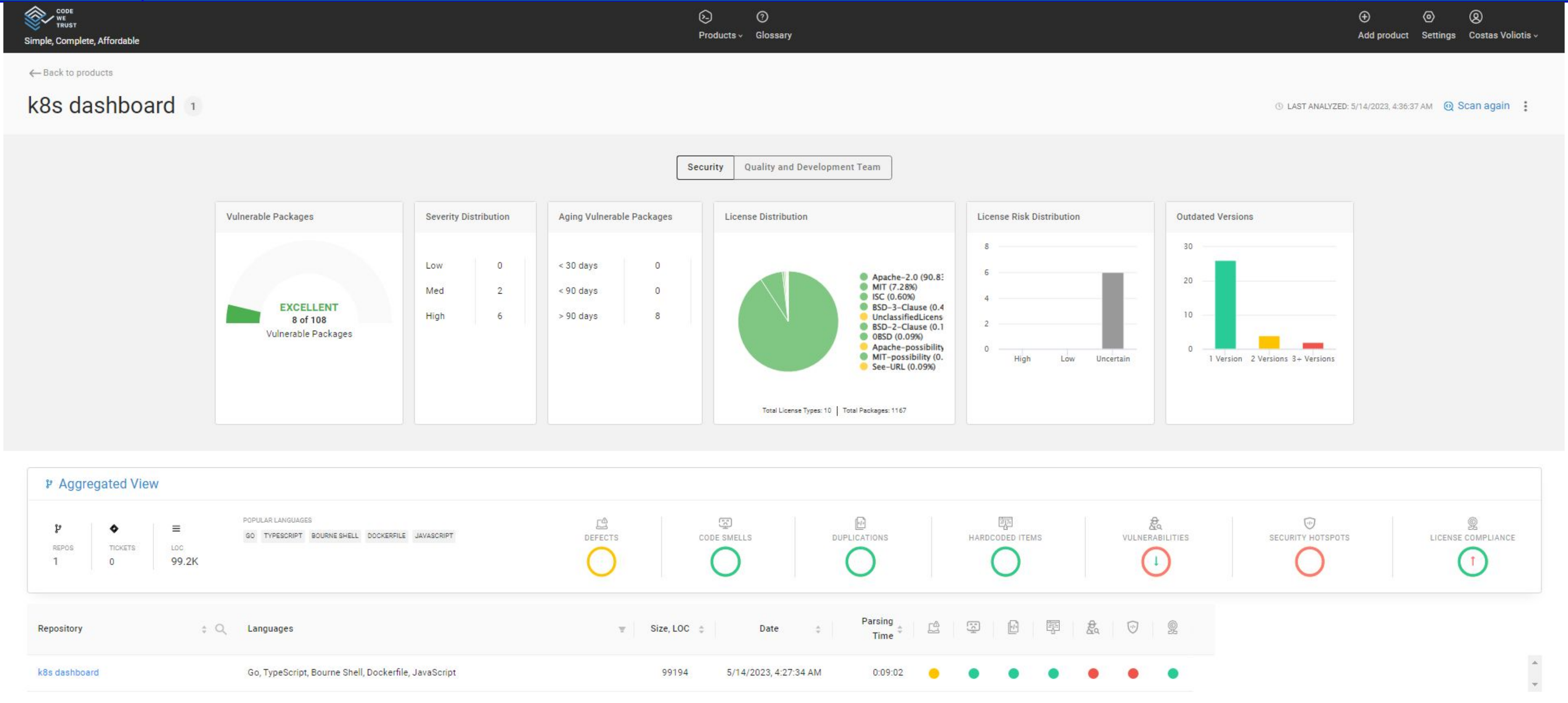
Code Smells

Duplication

Hard-coded Risks

Vulnerabilities

Product analysis overview-security



k8s dashboard 1

LAST ANALYZED: 5/14/2023, 4:36:37 AM

Vulnerable Packages

EXCELLENT
8 of 108
Vulnerable Packages

Severity Distribution

Low	0
Med	2
High	6

Aging Vulnerable Packages

< 30 days	0
< 90 days	0
> 90 days	8

License Distribution

Total License Types: 10 | Total Packages: 1167

License Risk Distribution

Outdated Versions

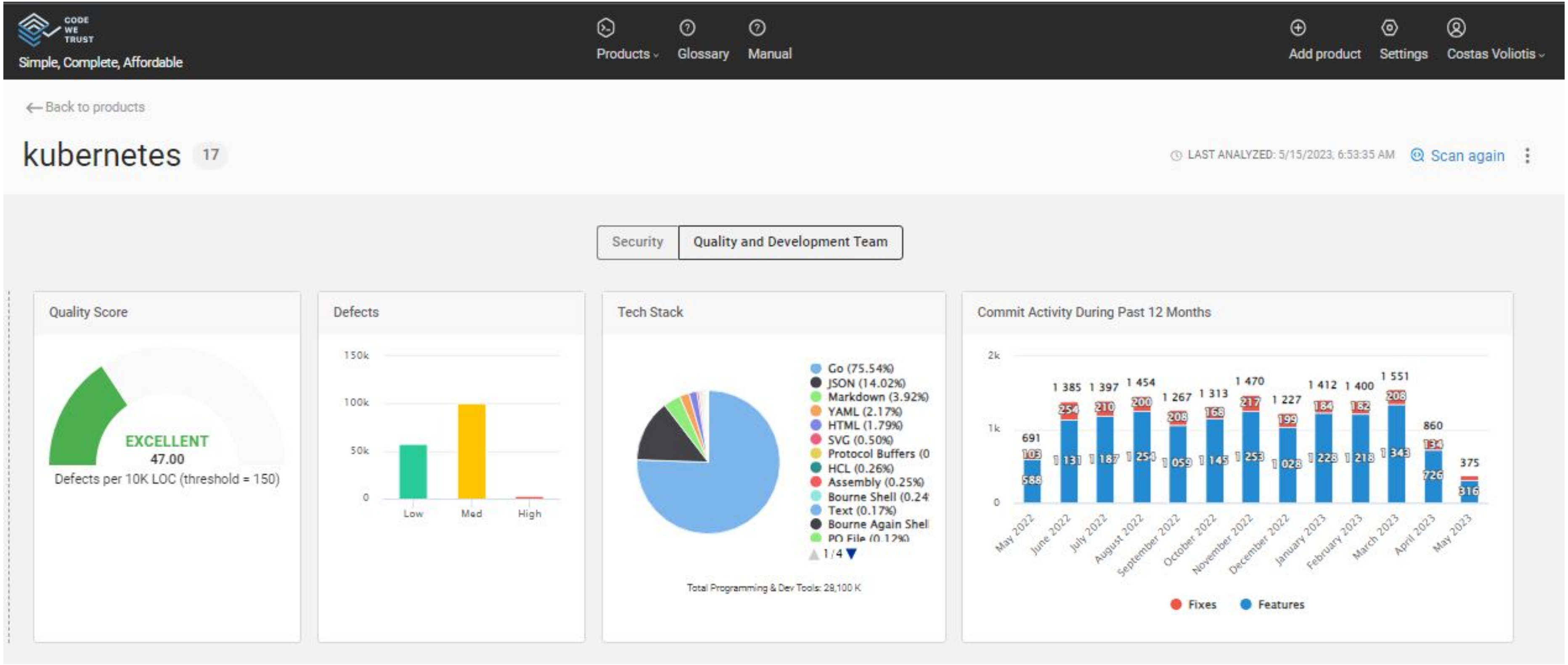
Aggregated View

REPOS: 1
TICKETS: 0
LOC: 99.2K

POPULAR LANGUAGES: GO, TYPESCRIPT, BOURNE SHELL, DOCKERFILE, JAVASCRIPT

Repository	Languages	Size, LOC	Date	Parsing Time							
k8s dashboard	Go, TypeScript, Bourne Shell, Dockerfile, JavaScript	99194	5/14/2023, 4:27:34 AM	0:09:02	●	●	●	●	●	●	●

Product analysis overview-quality



kubernetes 17

LAST ANALYZED: 5/15/2023, 6:53:35 AM

Quality Score

EXCELLENT
47.00
Defects per 10K LOC (threshold = 150)

Defects

Tech Stack

- Go (75.54%)
- JSON (14.02%)
- Markdown (3.92%)
- YAML (2.17%)
- HTML (1.79%)
- SVG (0.50%)
- Protocol Buffers (0
- HCL (0.26%)
- Assembly (0.25%)
- Bourne Shell (0.24
- Text (0.17%)
- Bourne Again Shel
- PO File (0.12%)

▲ 1/4 ▼

Total Programming & Dev Tools: 29,100 K

Commit Activity During Past 12 Months

Add a product

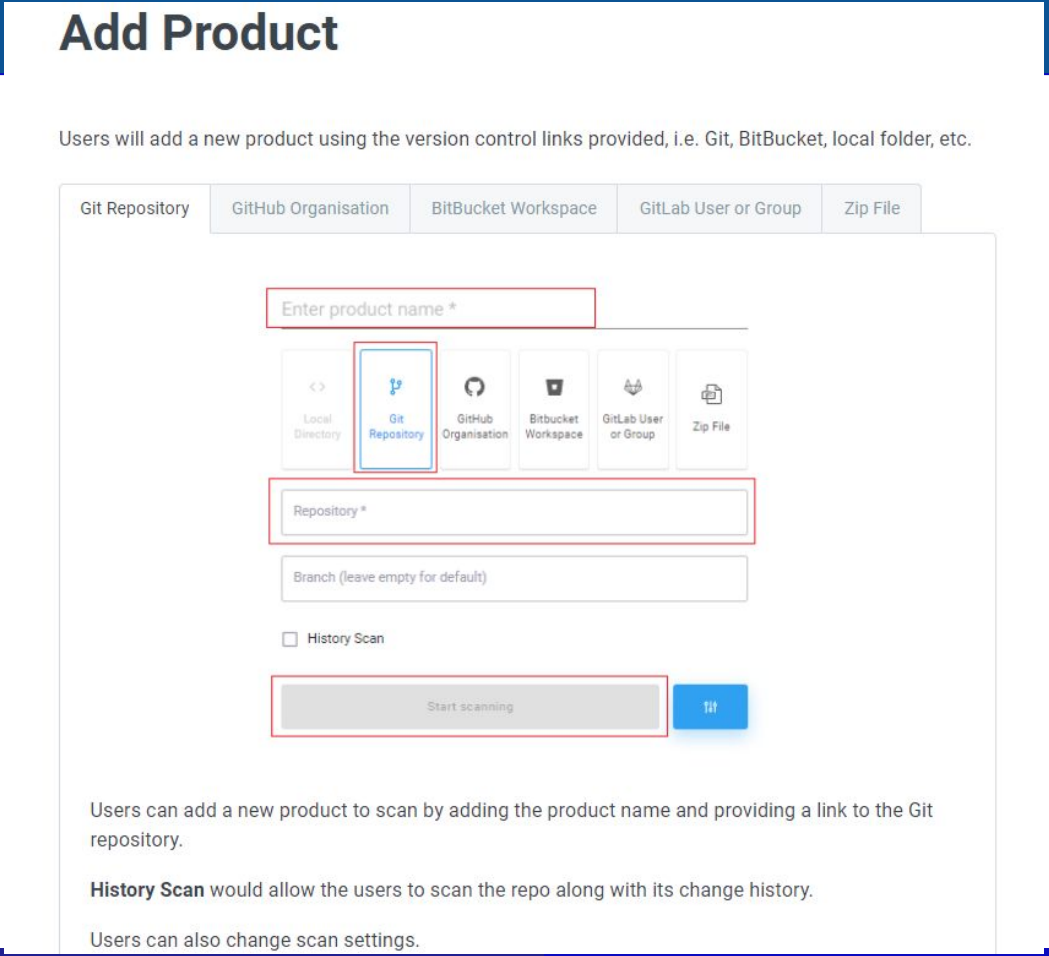
Part 3

Add Product

Users can add a new product to scan by adding the product name and providing a link to the Git repository.

History Scan would allow the users to scan the repo along with its change history.

Users can also change scan settings.



Add Product

Users will add a new product using the version control links provided, i.e. Git, BitBucket, local folder, etc.

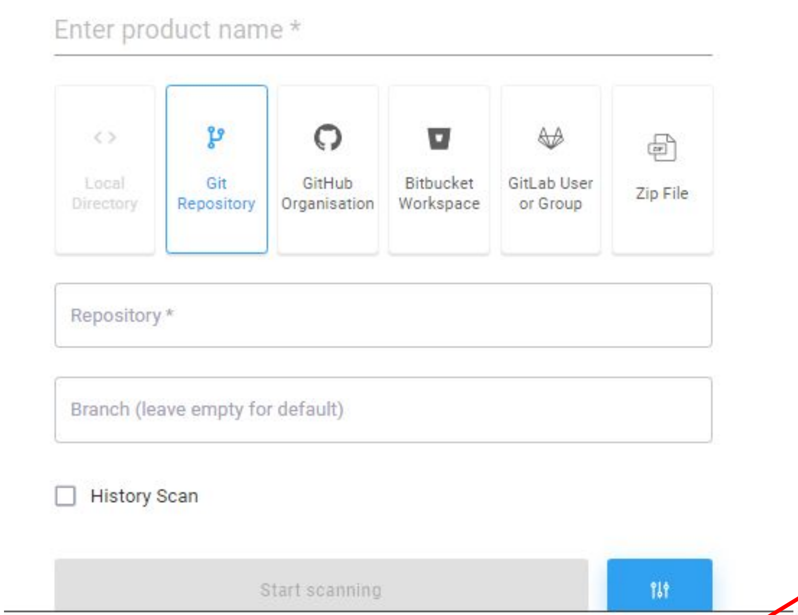
□ History Scan

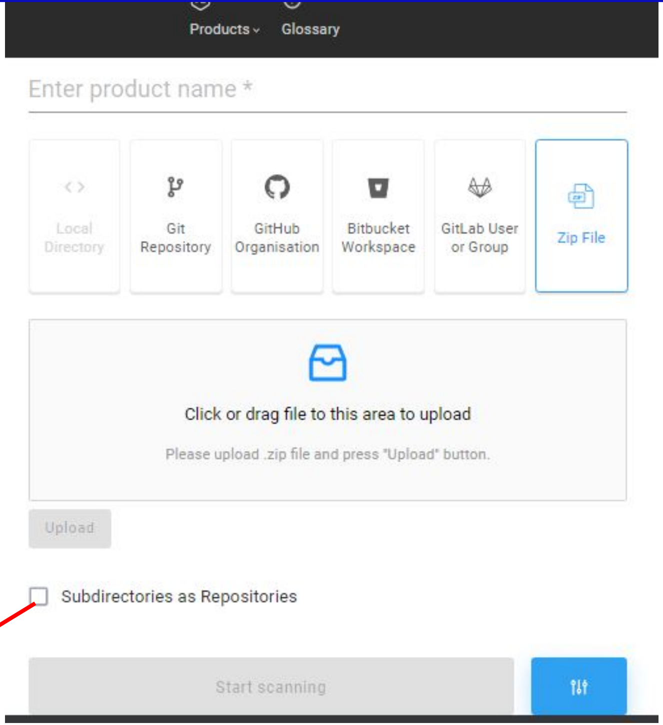
Users can add a new product to scan by adding the product name and providing a link to the Git repository.

History Scan would allow the users to scan the repo along with its change history.

Users can also change scan settings.

Add a new product



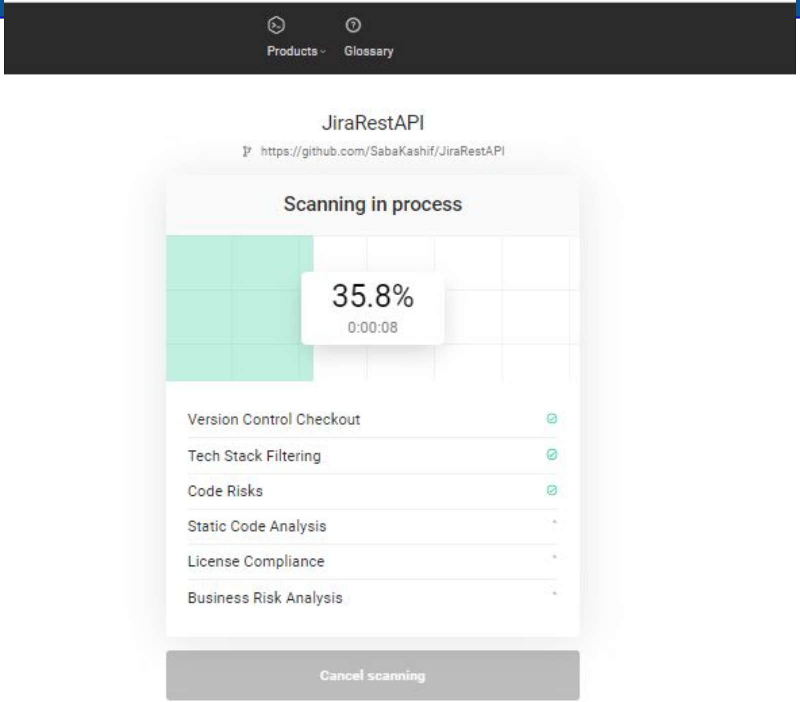


Click or drag file to this area to upload

Please upload .zip file and press "Upload" button.

To save the execution time, space and cost the the user can select subdirectories to be scanned individually.

Scan Process



JiraRestAPI

https://github.com/SabaKashif/JiraRestAPI

Scanning in process

35.8%

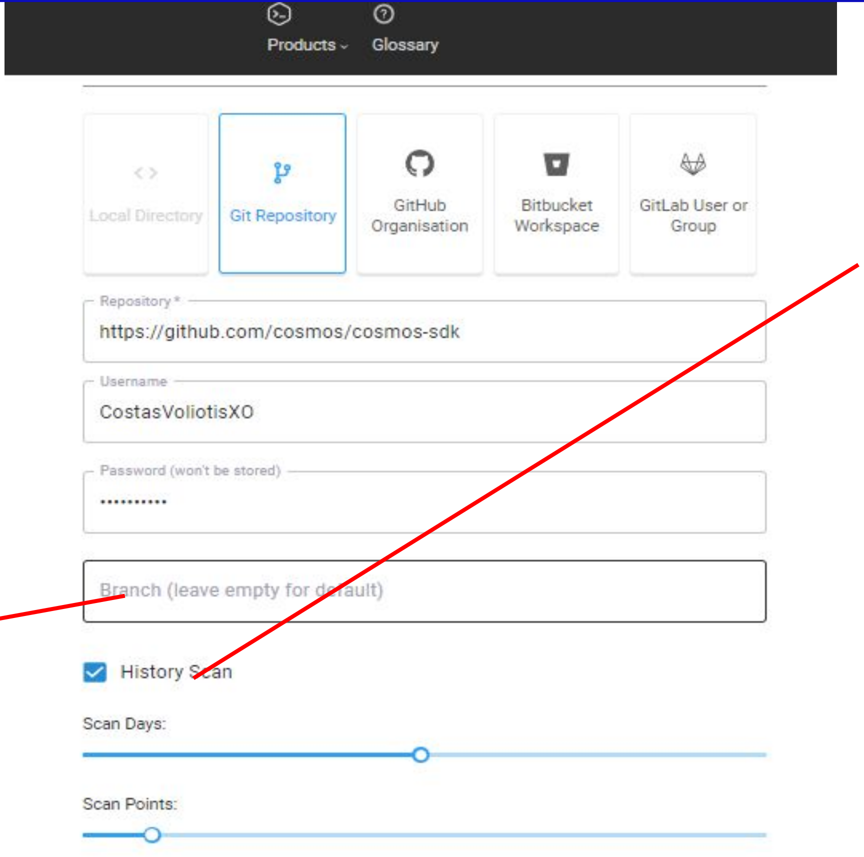
0:00:08

Version Control Checkout	✓
Tech Stack Filtering	✓
Code Risks	✓
Static Code Analysis	
License Compliance	
Business Risk Analysis	

Configure the scope of the analysis

Part 4

Historical Data & Development branch for a single repository



Repository * https://github.com/cosmos/cosmos-sdk

Username CostasVoliotisXO

Password (won't be stored) ••••••••••

Branch (leave empty for default)

☑ History Scan

Scan Days:

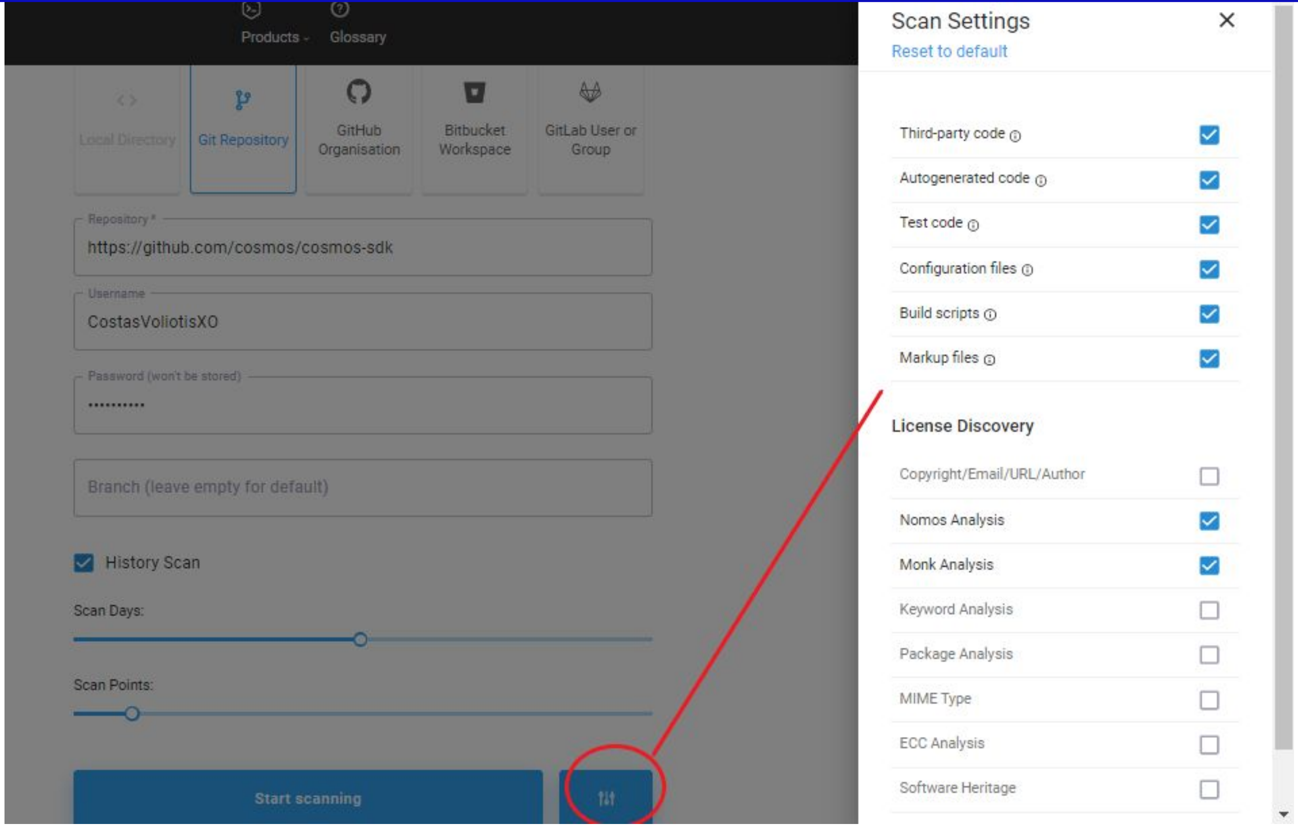
Scan Points:

Historical Data

Select Time frame and Sampling rate

Type the name of development branch

Limit the scope of scanning



Repository * https://github.com/cosmos/cosmos-sdk

Username CostasVoliotisXO

Password (won't be stored) ••••••••••

Branch (leave empty for default)

☑ History Scan

Scan Days:

Scan Points:

Scan Settings

Reset to default

- Third-party code ☑
- Autogenerated code ☑
- Test code ☑
- Configuration files ☑
- Build scripts ☑
- Markup files ☑

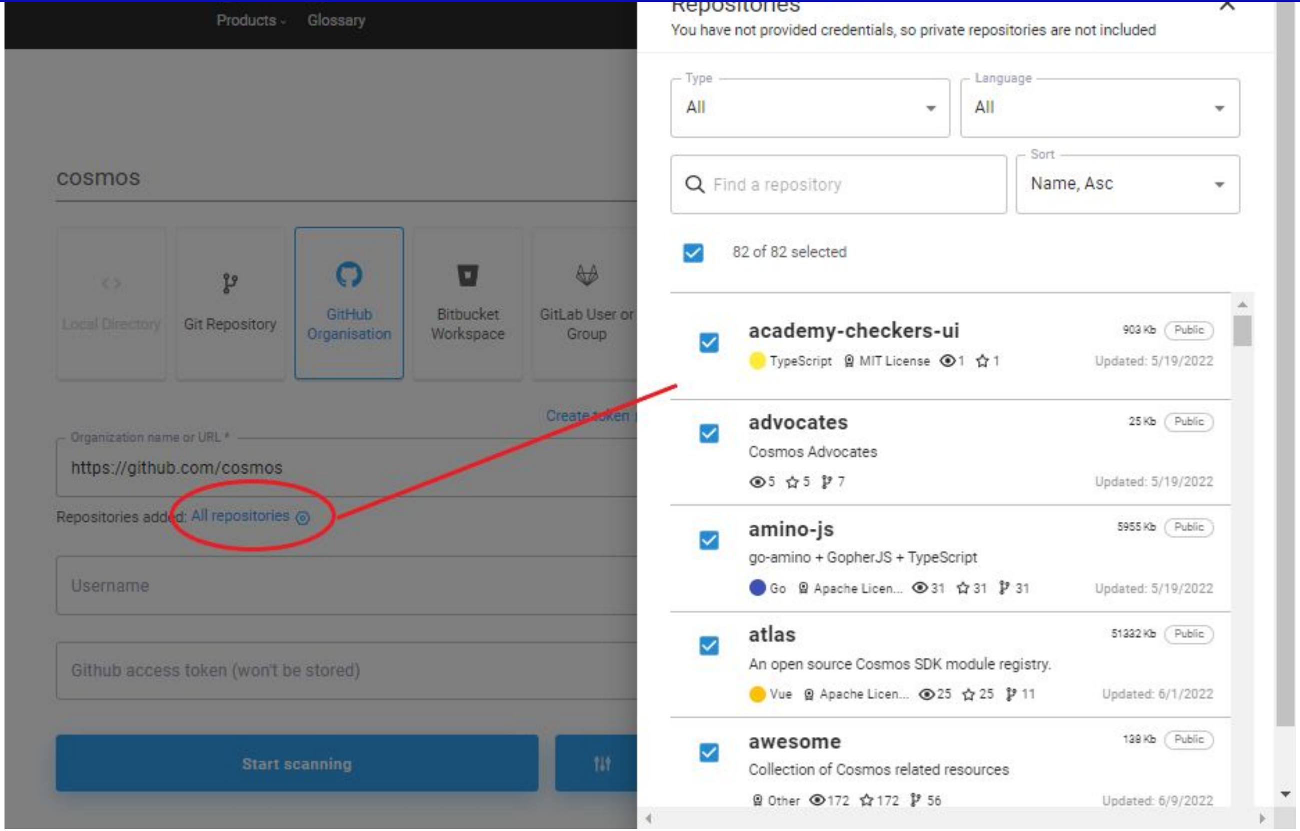
License Discovery

- Copyright/Email/URL/Author □
- Nomos Analysis ☑
- Monk Analysis ☑
- Keyword Analysis □
- Package Analysis □
- MIME Type □
- ECC Analysis □
- Software Heritage □

CODE WE TRUST

Filter the selected repositories

trustilio
Enhance your Trustworthiness



cosmos

Organization name or URL *: https://github.com/cosmos

Repositories added: All repositories

Username

Github access token (won't be stored)

Repositories

You have not provided credentials, so private repositories are not included

Type: All

Language: All

Find a repository

Sort: Name, Asc

☑ 82 of 82 selected

☑ **academy-checkers-ui** — 903 Kb — Public
TypeScript · MIT License · 1 · ☆ 1 — Updated: 5/19/2022

☑ **advocates** — 25 Kb — Public
Cosmos Advocates
5 · ☆ 5 · 7 — Updated: 5/19/2022

☑ **amino-js** — 5955 Kb — Public
go-amino + GopherJS + TypeScript
Go · Apache Licen... · 31 · ☆ 31 · 31 — Updated: 5/19/2022

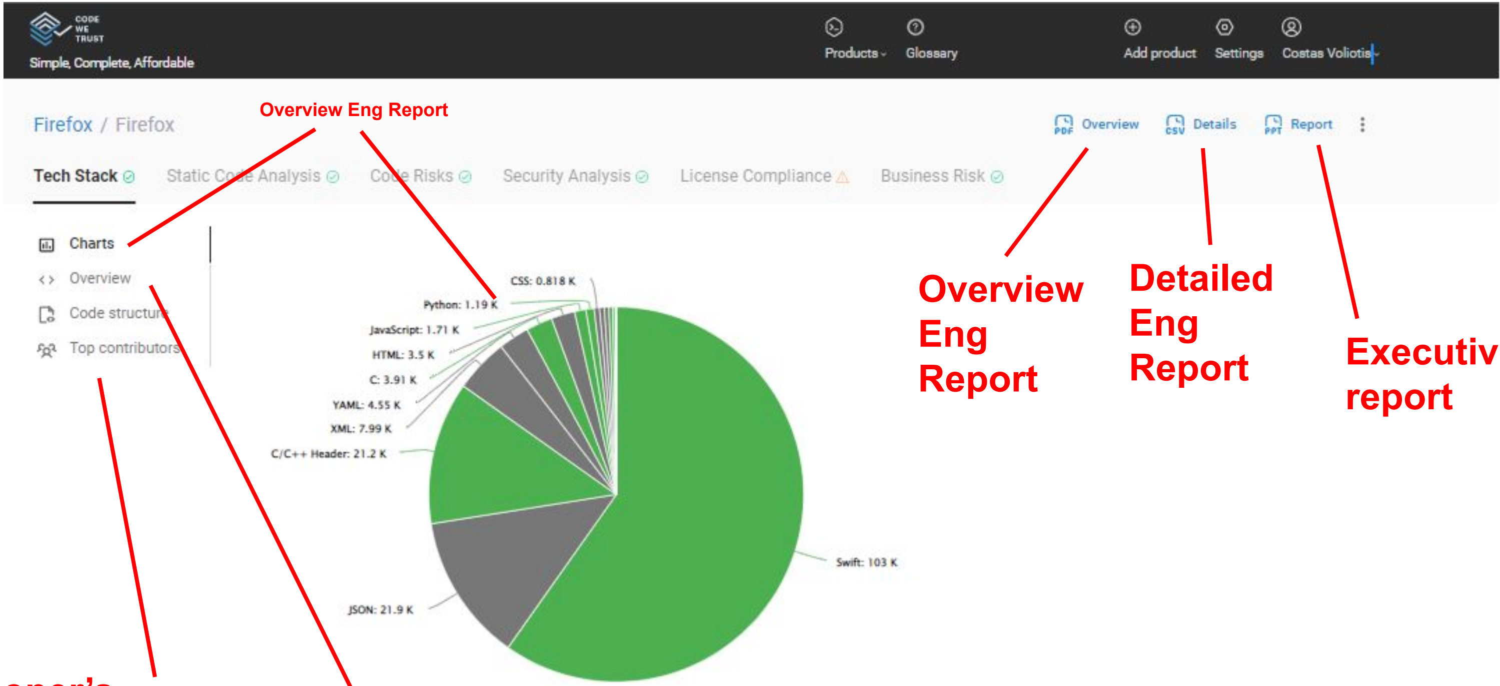
☑ **atlas** — 51332 Kb — Public
An open source Cosmos SDK module registry.
Vue · Apache Licen... · 25 · ☆ 25 · 11 — Updated: 6/1/2022

☑ **awesome** — 138 Kb — Public
Collection of Cosmos related resources
Other · 172 · ☆ 172 · 56 — Updated: 6/9/2022

Review analysis results

Part 5

Review tech stack analysis results



Overview Eng Report

Overview Eng Report

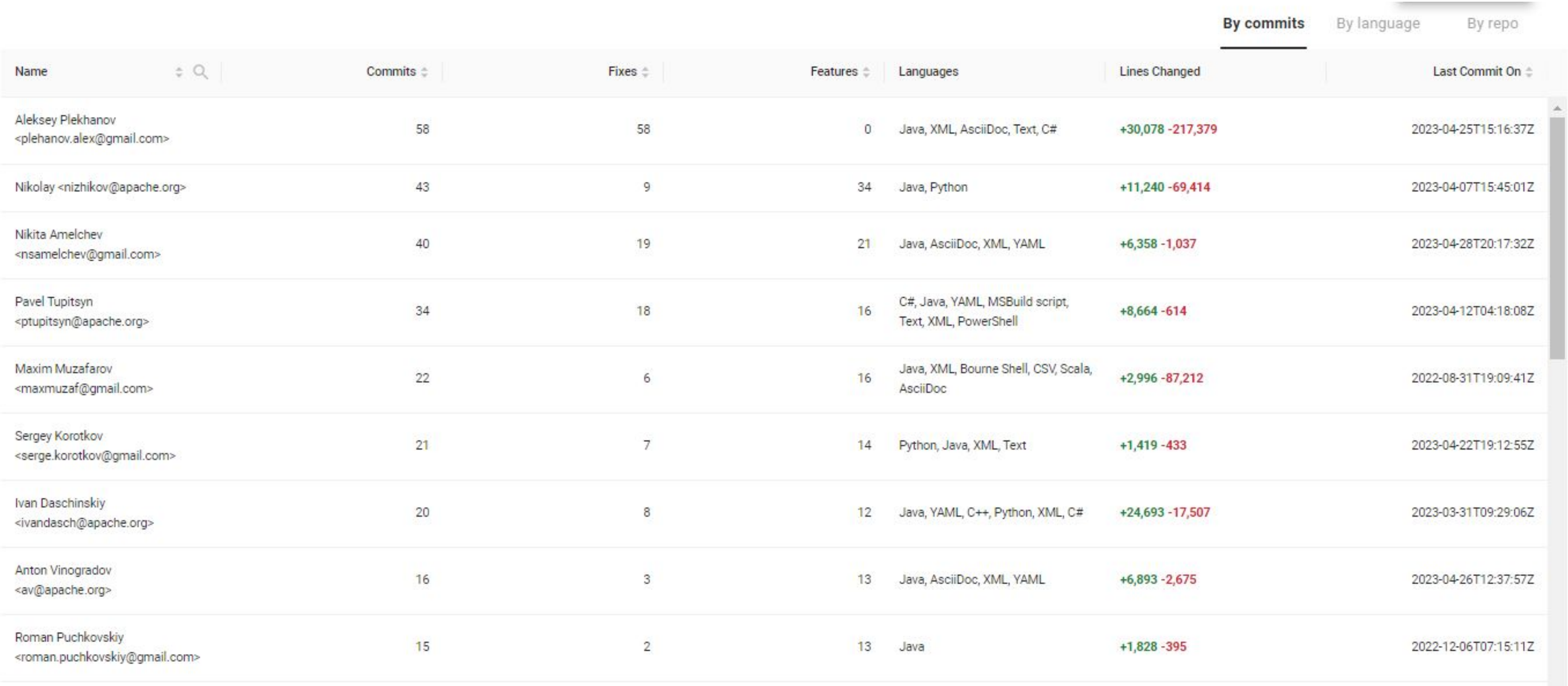
Detailed Eng Report

Executive report

Developer’s productivity review

Numerical Overview of
findings

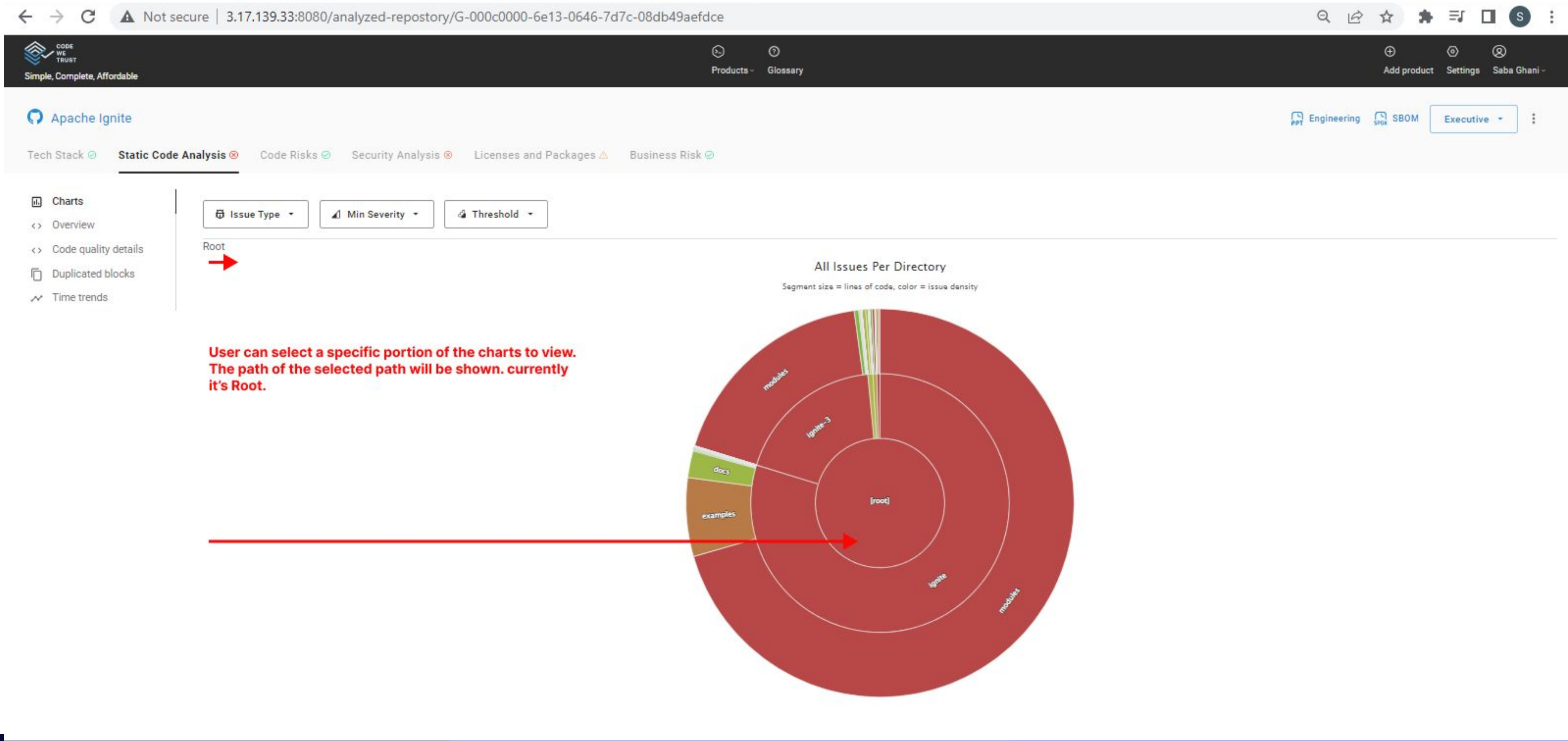
Top Contributors



By commits | By language | By repo

Name	Commits	Fixes	Features	Languages	Lines Changed	Last Commit On
Aleksey Plekhanov <plehanov.alex@gmail.com>	58	58	0	Java, XML, AsciiDoc, Text, C#	+30,078 -217,379	2023-04-25T15:16:37Z
Nikolay <nizhikov@apache.org>	43	9	34	Java, Python	+11,240 -69,414	2023-04-07T15:45:01Z
Nikita Amelchev <nsamelchev@gmail.com>	40	19	21	Java, AsciiDoc, XML, YAML	+6,358 -1,037	2023-04-28T20:17:32Z
Pavel Tupitsyn <ptupitsyn@apache.org>	34	18	16	C#, Java, YAML, MSBuild script, Text, XML, PowerShell	+8,664 -614	2023-04-12T04:18:08Z
Maxim Muzafarov <maxmuzaf@gmail.com>	22	6	16	Java, XML, Bourne Shell, CSV, Scala, AsciiDoc	+2,996 -87,212	2022-08-31T19:09:41Z
Sergey Korotkov <serge.korotkov@gmail.com>	21	7	14	Python, Java, XML, Text	+1,419 -433	2023-04-22T19:12:55Z
Ivan Daschinskiy <ivandasch@apache.org>	20	8	12	Java, YAML, C++, Python, XML, C#	+24,693 -17,507	2023-03-31T09:29:06Z
Anton Vinogradov <av@apache.org>	16	3	13	Java, AsciiDoc, XML, YAML	+6,893 -2,675	2023-04-26T12:37:57Z
Roman Puchkovskiy <roman.puchkovskiy@gmail.com>	15	2	13	Java	+1,828 -395	2022-12-06T07:15:11Z

Sunburst charts



Not secure | 3.17.139.33:8080/analyzed-repostory/G-000c0000-6e13-0646-7d7c-08db49aefdce

Apache Ignite

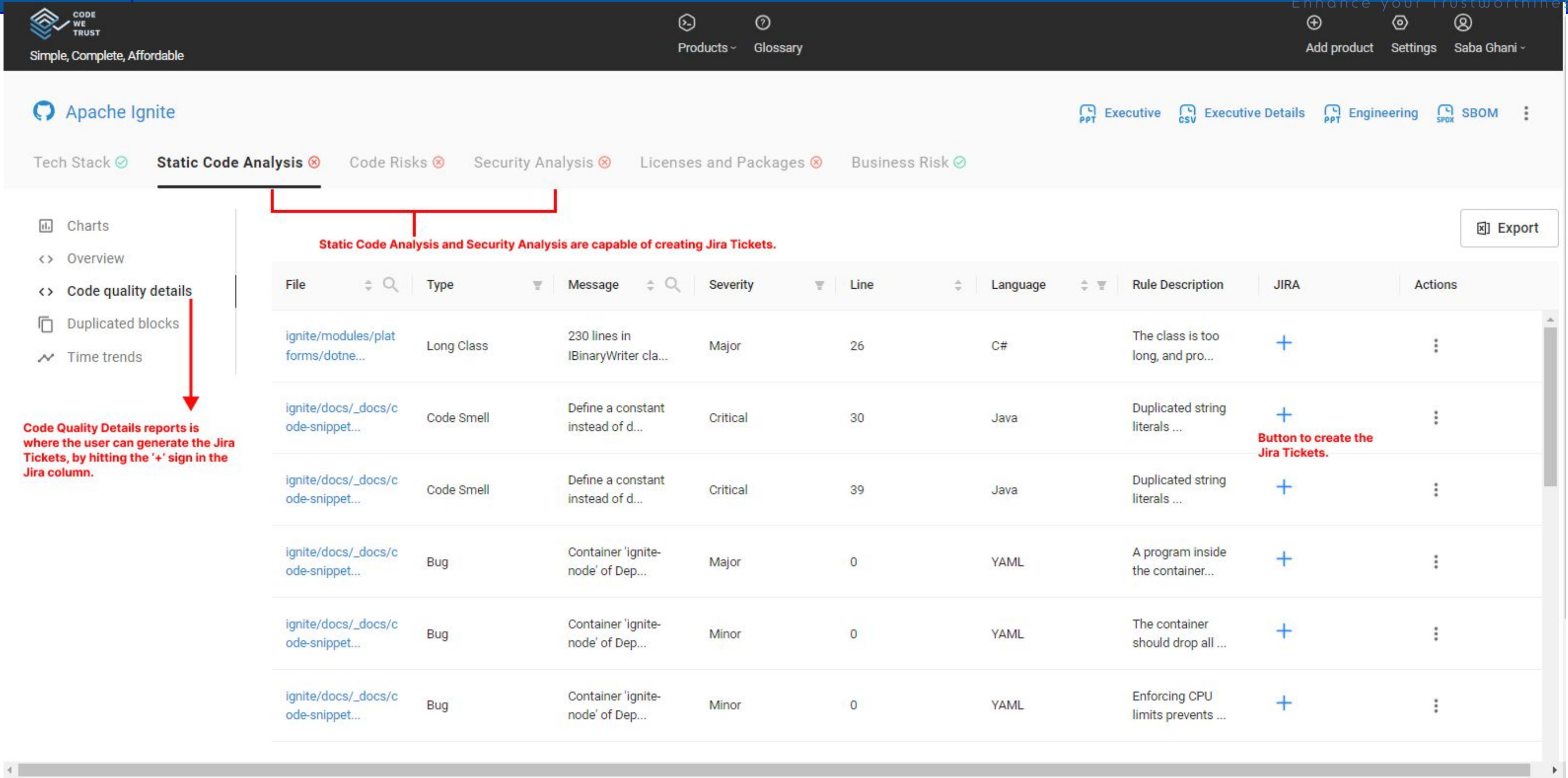
All Issues Per Directory

Segment size = lines of code, color = issue density

User can select a specific portion of the charts to view. The path of the selected path will be shown. currently it's Root.

Code Quality Details

Enhance your Trustworthiness



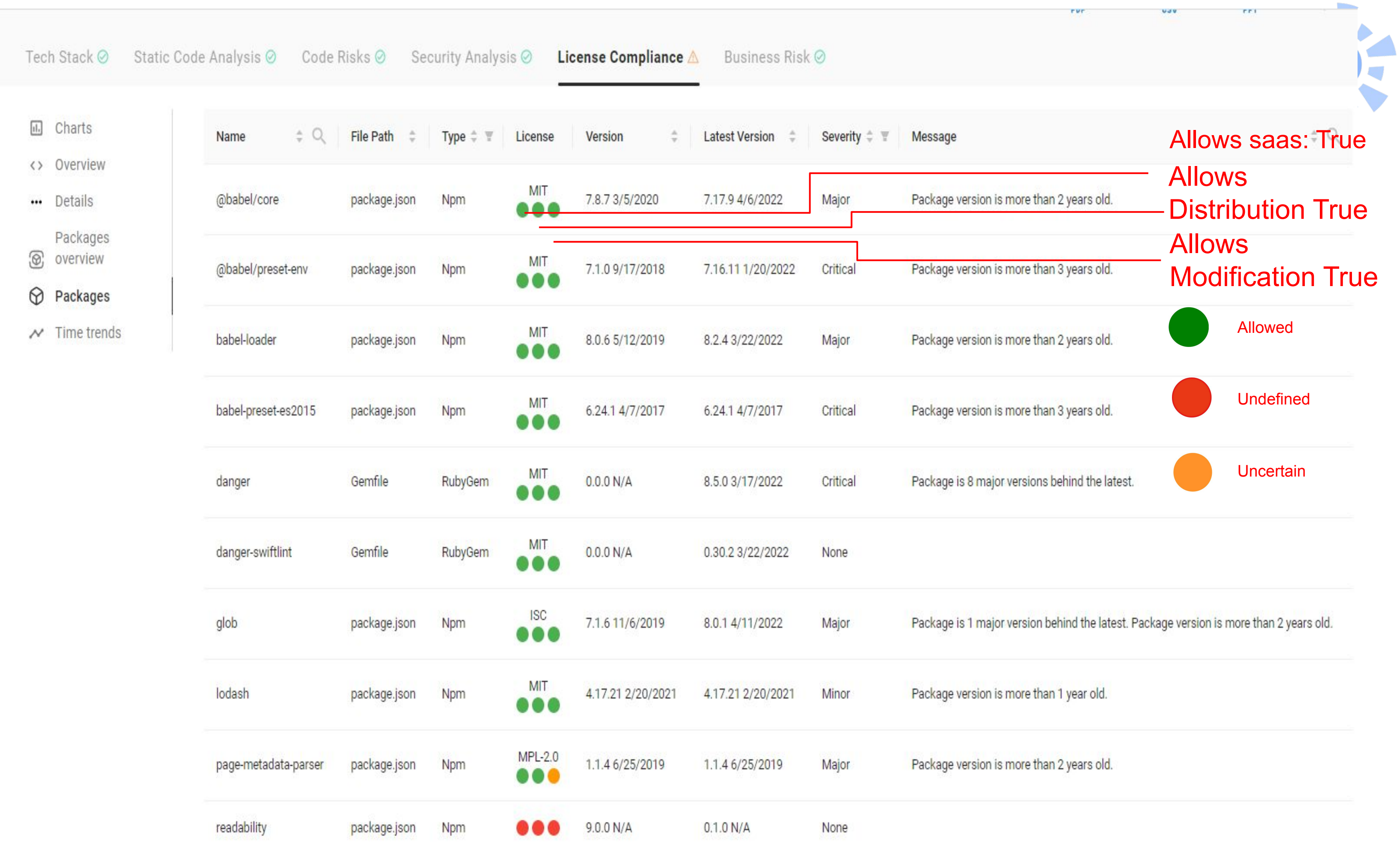
Static Code Analysis and Security Analysis are capable of creating Jira Tickets.

Code Quality Details reports is where the user can generate the Jira Tickets, by hitting the '+' sign in the Jira column.

File	Type	Message	Severity	Line	Language	Rule Description	JIRA	Actions
ignite/modules/platforms/dotne...	Long Class	230 lines in IBinaryWriter cla...	Major	26	C#	The class is too long, and pro...	+	⋮
ignite/docs/_docs/code-snippet...	Code Smell	Define a constant instead of d...	Critical	30	Java	Duplicated string literals ...	+	⋮
ignite/docs/_docs/code-snippet...	Code Smell	Define a constant instead of d...	Critical	39	Java	Duplicated string literals ...	+	⋮
ignite/docs/_docs/code-snippet...	Bug	Container 'ignite-node' of Dep...	Major	0	YAML	A program inside the container...	+	⋮
ignite/docs/_docs/code-snippet...	Bug	Container 'ignite-node' of Dep...	Minor	0	YAML	The container should drop all ...	+	⋮
ignite/docs/_docs/code-snippet...	Bug	Container 'ignite-node' of Dep...	Minor	0	YAML	Enforcing CPU limits prevents ...	+	⋮

Button to create the Jira Tickets.

Review Package Analysis results



Name	File Path	Type	License	Version	Latest Version	Severity	Message
@babel/core	package.json	Npm	MIT 🟢🟢🟢	7.8.7 3/5/2020	7.17.9 4/6/2022	Major	Package version is more than 2 years old.
@babel/preset-env	package.json	Npm	MIT 🟢🟢🟢	7.1.0 9/17/2018	7.16.11 1/20/2022	Critical	Package version is more than 3 years old.
babel-loader	package.json	Npm	MIT 🟢🟢🟢	8.0.6 5/12/2019	8.2.4 3/22/2022	Major	Package version is more than 2 years old.
babel-preset-es2015	package.json	Npm	MIT 🟢🟢🟢	6.24.1 4/7/2017	6.24.1 4/7/2017	Critical	Package version is more than 3 years old.
danger	Gemfile	RubyGem	MIT 🟢🟢🟢	0.0.0 N/A	8.5.0 3/17/2022	Critical	Package is 8 major versions behind the latest.
danger-swiftlint	Gemfile	RubyGem	MIT 🟢🟢🟢	0.0.0 N/A	0.30.2 3/22/2022	None	
glob	package.json	Npm	ISC 🟢🟢🟢	7.1.6 11/6/2019	8.0.1 4/11/2022	Major	Package is 1 major version behind the latest. Package version is more than 2 years old.
lodash	package.json	Npm	MIT 🟢🟢🟢	4.17.21 2/20/2021	4.17.21 2/20/2021	Minor	Package version is more than 1 year old.
page-metadata-parser	package.json	Npm	MPL-2.0 🟢🟢🟠	1.1.4 6/25/2019	1.1.4 6/25/2019	Major	Package version is more than 2 years old.
readability	package.json	Npm	🔴🔴🔴	9.0.0 N/A	0.1.0 N/A	None	

Allows saas: True

Allows Distribution True

Allows Modification True

🟢 Allowed

🔴 Undefined

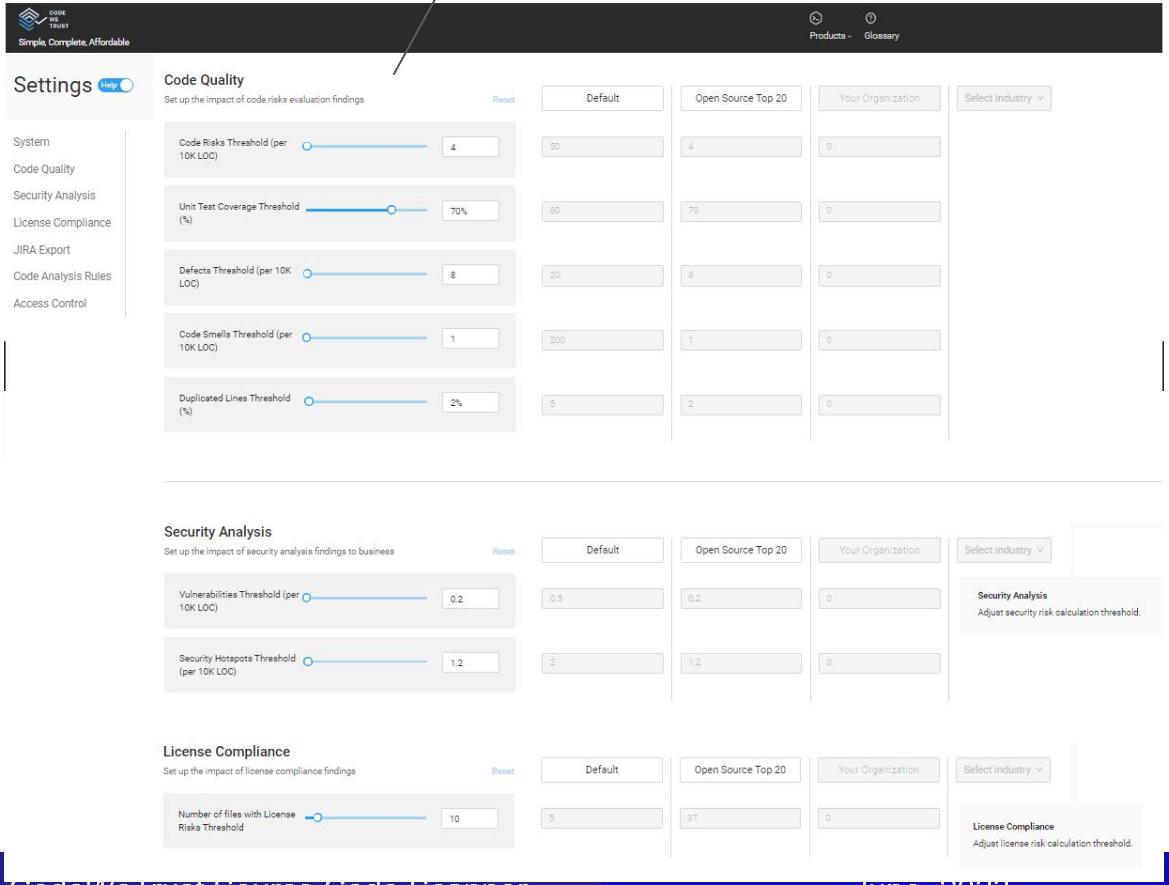
🟠 Uncertain

Define a new quality benchmark

Part 6

Quality Benchmarks

c2m version 6.0+ provides a method to define your own Quality Thresholds. a) you can choose the default quality settings calculated averaging the results of a wide selection of OSS frameworks. b) You can modify the select settings c) You can choose the quality benchmark calculated analysing 20 of the Top50 most used OSS frameworks on GitHub Annual enterprise versions will provide , the functionality to implement, import and export your own benchmarks analysing user selected reference frameworks.



Code Quality

Set up the impact of code risks evaluation findings

		Default	Open Source Top 20	Your Organization
Code Risks Threshold (per 10K LOC)	4	50	4	0
Unit Test Coverage Threshold (%)	70%	80	70	0
Defects Threshold (per 10K LOC)	8	20	8	0
Code Smells Threshold (per 10K LOC)	1	200	1	0
Duplicated Lines Threshold (%)	2%	5	2	0

Security Analysis

Set up the impact of security analysis findings to business

		Default	Open Source Top 20	Your Organization
Vulnerabilities Threshold (per 10K LOC)	0.2	0.5	0.2	0
Security Hotspots Threshold (per 10K LOC)	1.2	2	1.2	0

Security Analysis

Adjust security risk calculation threshold.

License Compliance

Set up the impact of license compliance findings

		Default	Open Source Top 20	Your Organization
Number of files with License Risks Threshold	10	5	37	0

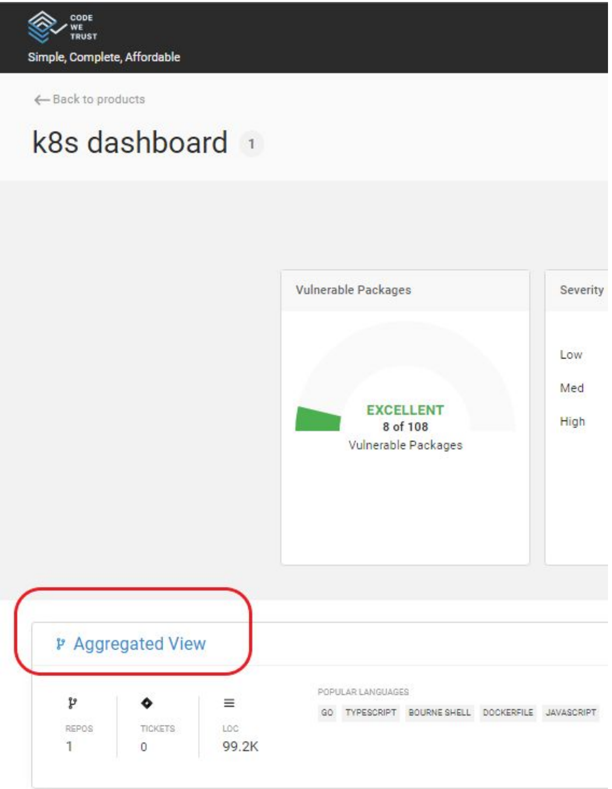
License Compliance

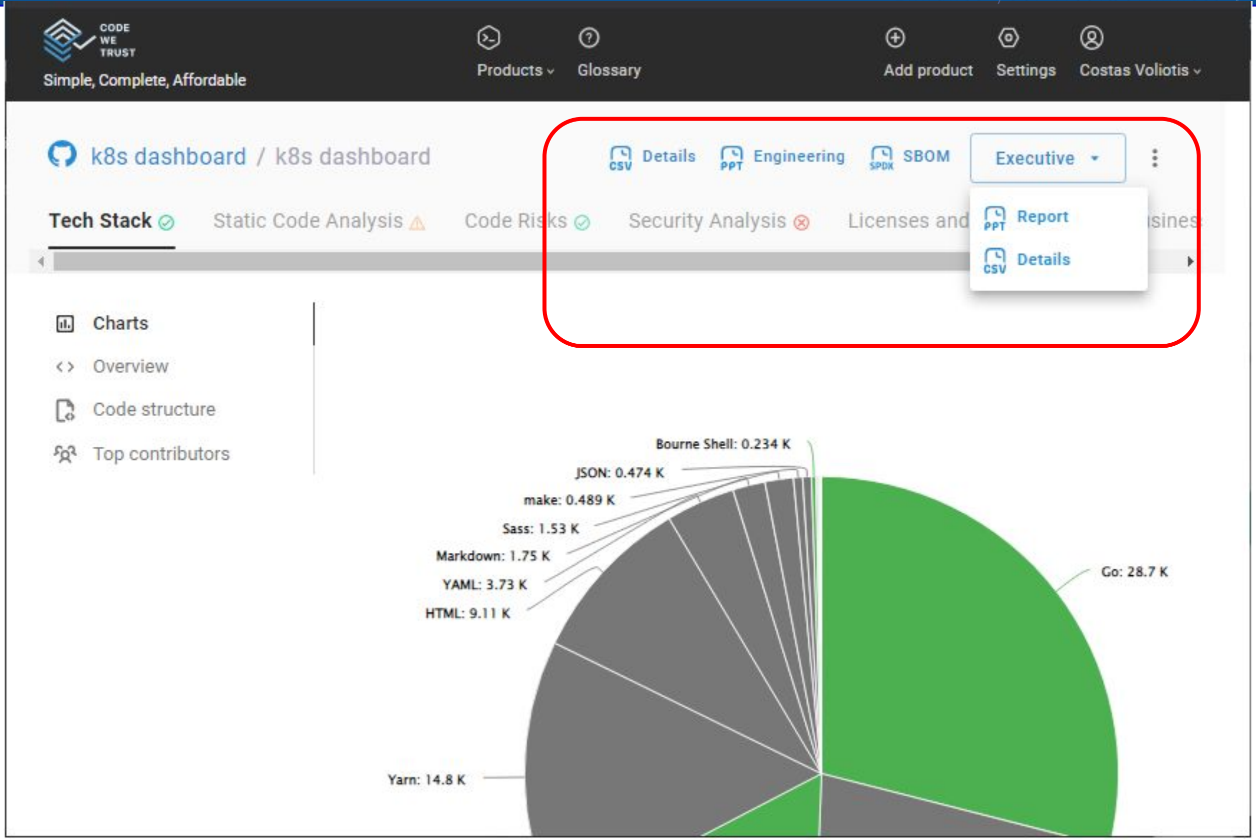
Adjust license risk calculation threshold.

Auto generated reports

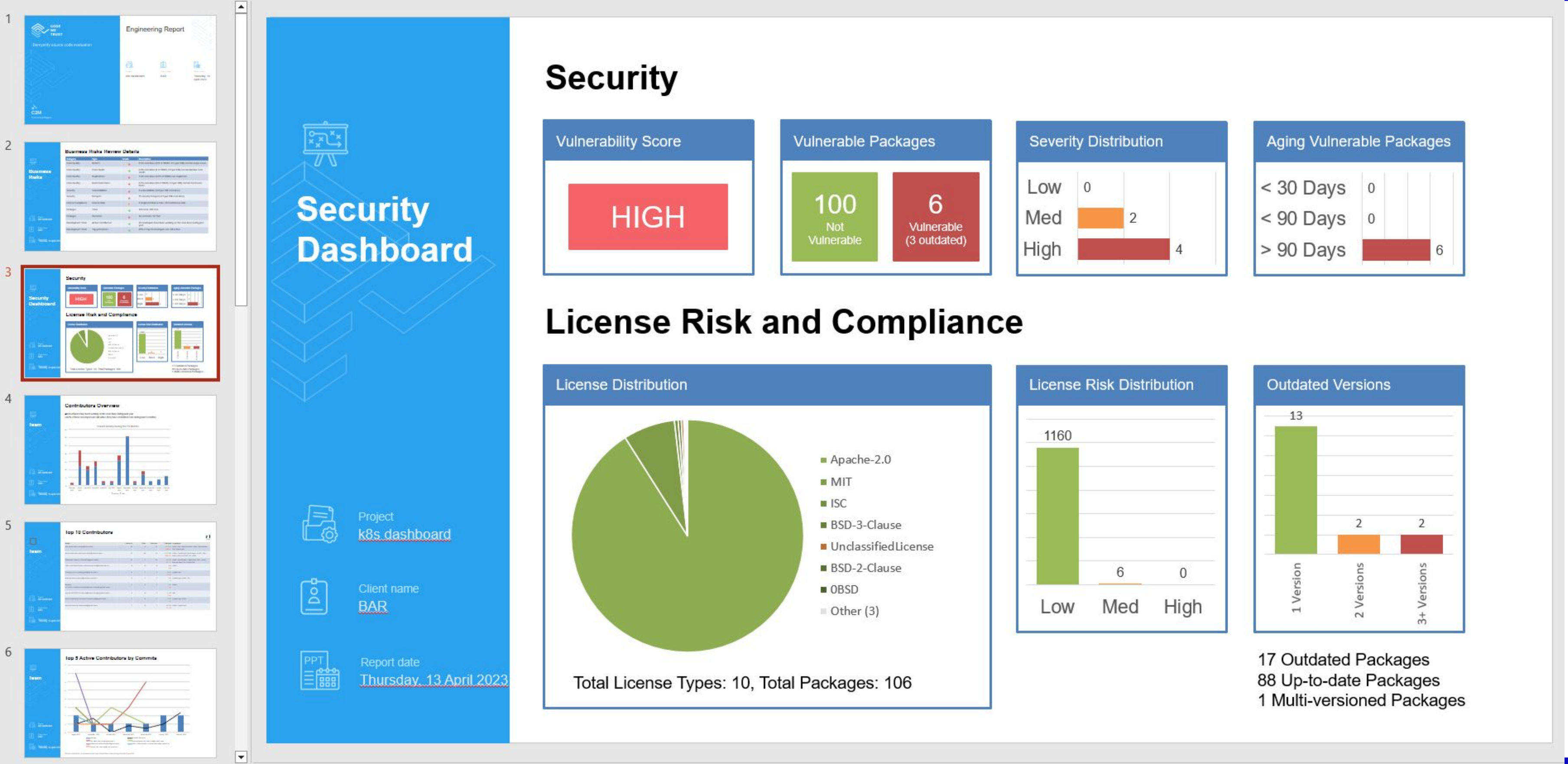
Part 7

Extract the auto generated reports





Executive report layout



Security

Vulnerability Score

HIGH

Vulnerable Packages

100 Not Vulnerable

6 Vulnerable (3 outdated)

Severity Distribution

Aging Vulnerable Packages

License Risk and Compliance

License Distribution

Total License Types: 10, Total Packages: 106

License Risk Distribution

Outdated Versions

17 Outdated Packages
88 Up-to-date Packages
1 Multi-versioned Packages

Project
k8s dashboard

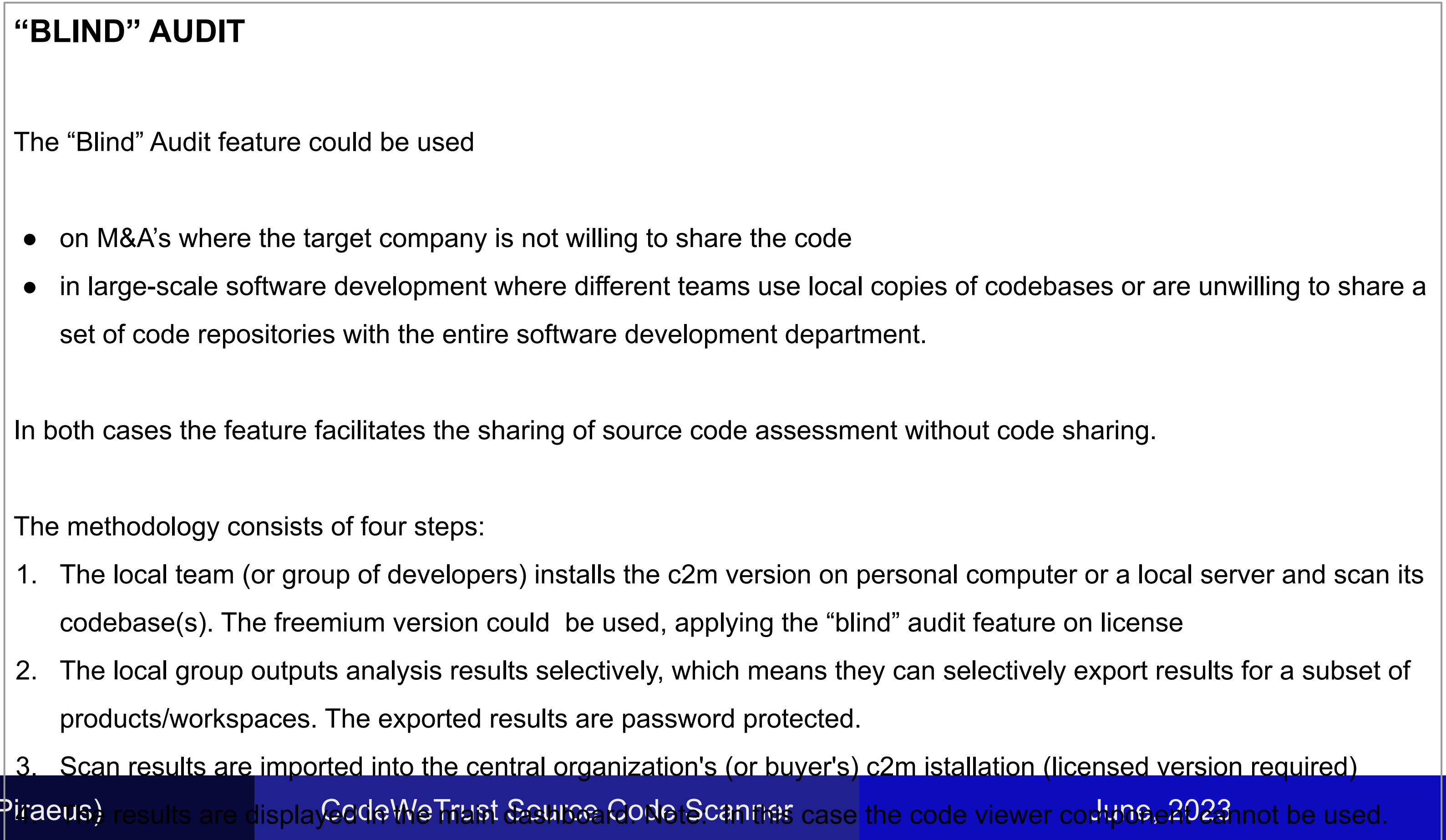
Client name
BAR

Report date
Thursday, 13 April 2023

BLIND AUDIT

Part 9

“Blind” audit



“BLIND” AUDIT

The “Blind” Audit feature could be used

- on M&A’s where the target company is not willing to share the code
- in large-scale software development where different teams use local copies of codebases or are unwilling to share a set of code repositories with the entire software development department.

In both cases the feature facilitates the sharing of source code assessment without code sharing.

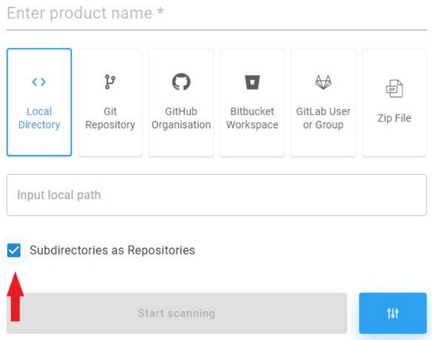
The methodology consists of four steps:

1. The local team (or group of developers) installs the c2m version on personal computer or a local server and scan its codebase(s). The freemium version could be used, applying the “blind” audit feature on license
2. The local group outputs analysis results selectively, which means they can selectively export results for a subset of products/workspaces. The exported results are password protected.
3. Scan results are imported into the central organization's (or buyer's) c2m istallation (licensed version required)
4. The results are displayed in the main dashboard. Note: in this case the code viewer component cannot be used.

“Blind “ Audit

Steps

1. Download the application from : https://www.codewetrust.com/download
2. Setup a folder preferably not on C: give it name and unzip the downloaded file on it
3. Secure the the docker engine is activated
4. After successful installation of the application add as first product the GIT repository : https://github.com/cwt-test and scan it
5. and export it as it shown below. Share it with the Auditor



Enter product name *

Input local path

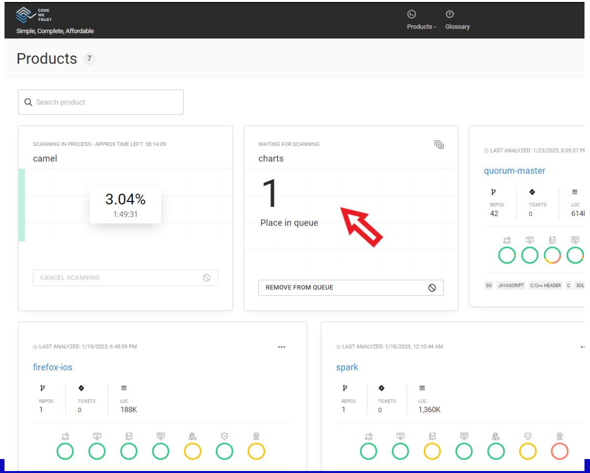
☑ Subdirectories as Repositories

Suggestions

if you scan the code from local repository it is suggested to split in logical units (front-end, back-end, tests etc) as much this is possible. Setup a different folder for each part, and scan it as a different product

Select the option subdirectories as repositories

You can kickoff the scanning of several folder without waiting for completion of parsing. The jobs will be pipelined. as shown on the screen shot on the right



Products 7

SCANNING IN PROCESS - APPROX TIME LEFT: 58:14:09
camel
3.04%
1:49:31

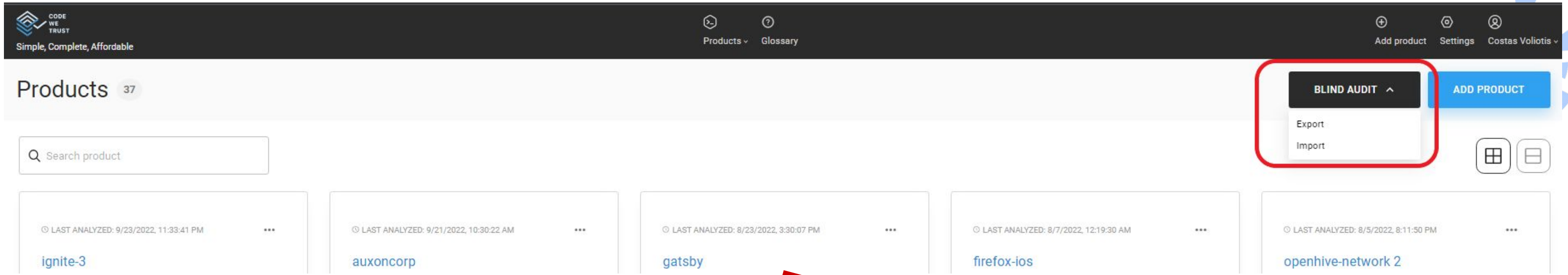
WAITING FOR SCANNING
charts
1
Place in queue

LAST ANALYZED: 1/23/2023, 8:09:37 P
quorum-master
REPOS 42 TICKETS 0 LOC 614
GO JAVASCRIPT C/C++ HEADER C SOL

LAST ANALYZED: 1/19/2023, 6:48:59 PM
firefox-ios
REPOS 1 TICKETS 0 LOC 188K

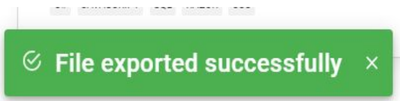
LAST ANALYZED: 1/18/2023, 12:10:44 AM
spark
REPOS 1 TICKETS 0 LOC 1,360K

“Blind” audit steps 1-2

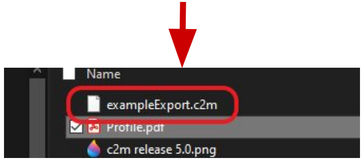


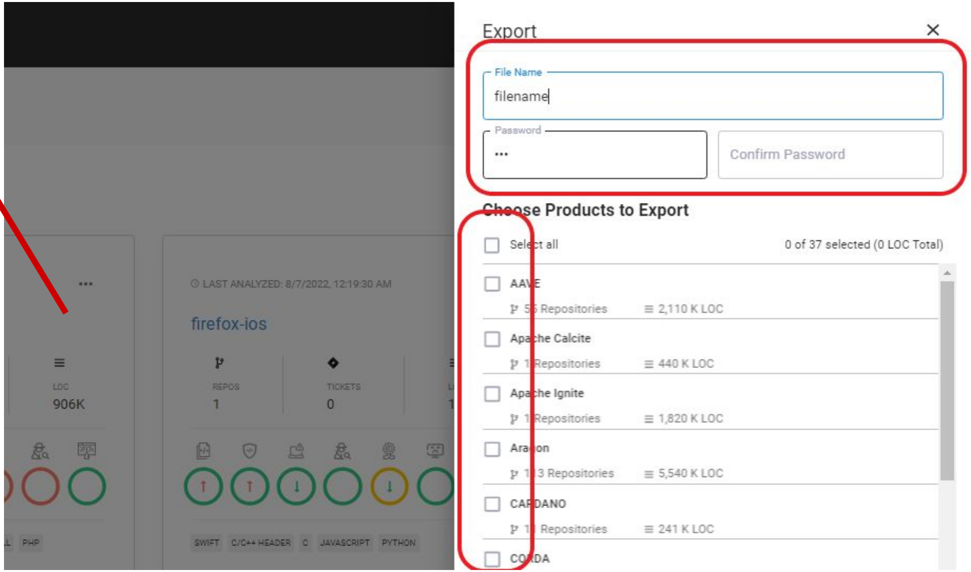
Products 37

LAST ANALYZED: 9/23/2022, 11:33:41 PM	LAST ANALYZED: 9/21/2022, 10:30:22 AM	LAST ANALYZED: 8/23/2022, 3:30:07 PM	LAST ANALYZED: 8/7/2022, 12:19:30 AM	LAST ANALYZED: 8/5/2022, 8:11:50 PM
ignite-3	auxoncorp	gatsby	firefox-ios	openhive-network 2



File exported successfully





Export

File Name: filename

Password: •••

Confirm Password

Choose Products to Export

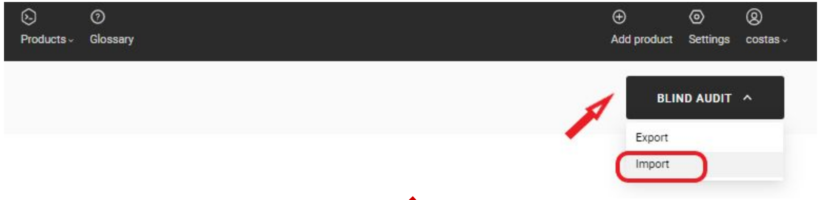
□ Select all — 0 of 37 selected (0 LOC Total)

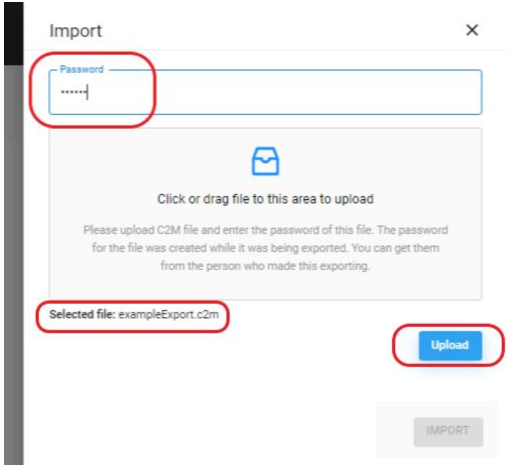
□ AAVE	55 Repositories	2,110 K LOC
□ Apache Calcite	1 Repositories	440 K LOC
□ Apache Ignite	1 Repositories	1,820 K LOC
□ Aragon	113 Repositories	5,540 K LOC
□ CARDANO	11 Repositories	241 K LOC
□ CORDA		

After the user has scan its code and selected the parts of the analysis, he is willing to share.

A password protected file with the extension .c2m is compile and exeported. (ie “yourfilename.c2m”

“Blind” audit steps 3 and 4



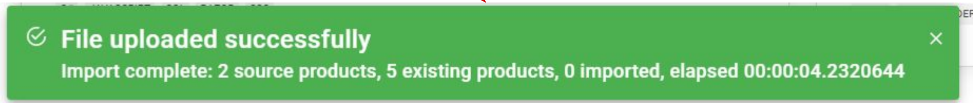


Password: ••••••

Click or drag file to this area to upload

Please upload C2M file and enter the password of this file. The password for the file was created while it was being exported. You can get them from the person who made this exporting.

Selected file: exampleExport.c2m



File uploaded successfully

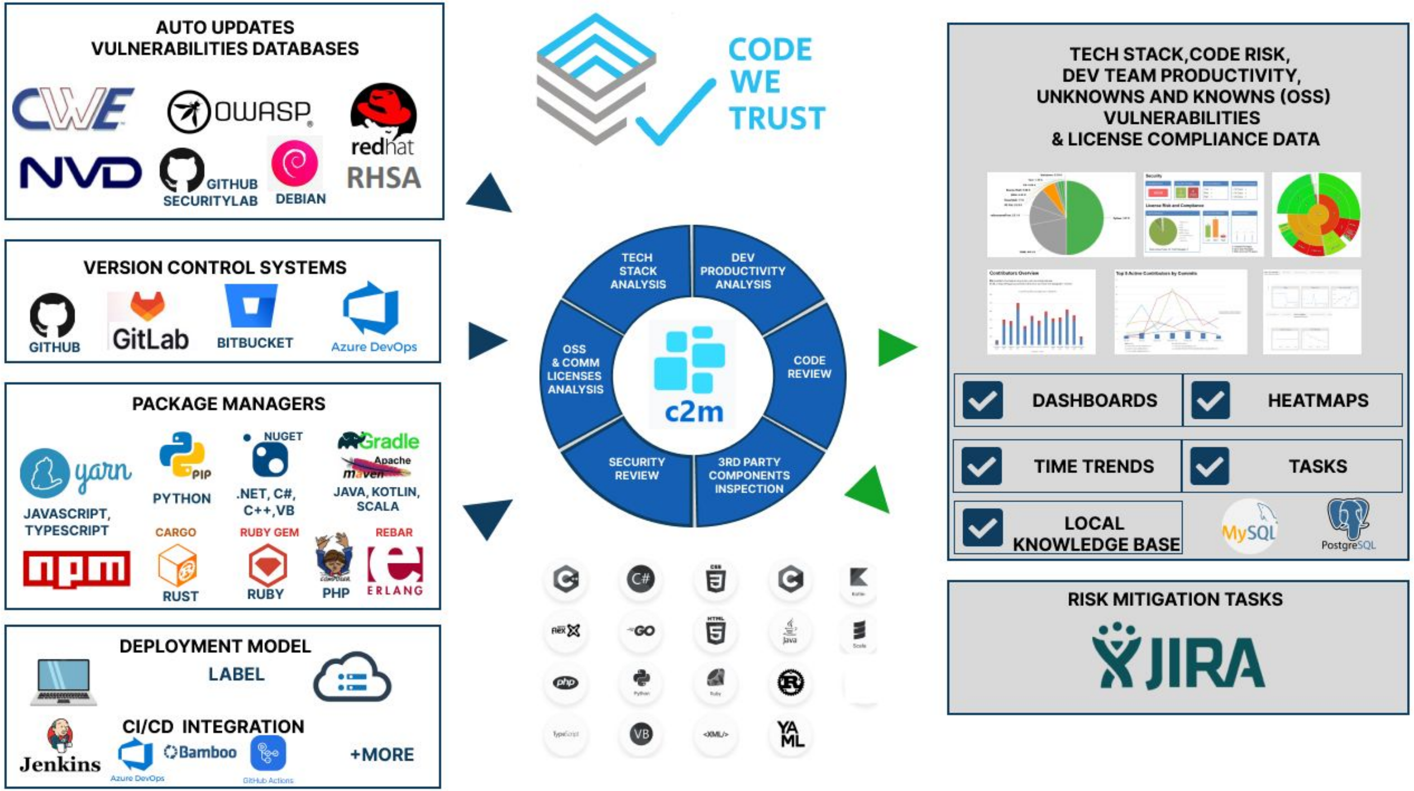
Import complete: 2 source products, 5 existing products, 0 imported, elapsed 00:00:04.2320644

The “consumer” received the results file through mail or file sharing and activates the import functionality

he has to provide teh correct password, wait for file loading 9it might take a while depends on the size of the file) and then after uploading completion has to select the “import”

CodeWeTrust overview

Enhance your Trustworthiness



AUTO UPDATES
VULNERABILITIES DATABASES

CWE, OWASP, redhat RHSA, NVD, GITHUB SECURITYLAB, DEBIAN

VERSION CONTROL SYSTEMS

GITHUB, GitLab, BITBUCKET, Azure DevOps

PACKAGE MANAGERS

- yarn: JAVASCRIPT, TYPESCRIPT
- PIP: PYTHON
- NUGET: .NET, C#, C++,VB
- Gradle, Apache maven: JAVA, KOTLIN, SCALA
- npm
- CARGO: RUST
- RUBY GEM: RUBY
- COMPOSER: PHP
- REBAR: ERLANG

DEPLOYMENT MODEL

LABEL

CI/CD INTEGRATION

Jenkins, Azure DevOps, Bamboo, GitHub Actions, +MORE

CODE WE TRUST

c2m

- TECH STACK ANALYSIS
- DEV PRODUCTIVITY ANALYSIS
- CODE REVIEW
- 3RD PARTY COMPONENTS INSPECTION
- SECURITY REVIEW
- OSS & COMM LICENSES ANALYSIS

TECH STACK, CODE RISK,
DEV TEAM PRODUCTIVITY,
UNKNOWNS AND KNOWNS (OSS)
VULNERABILITIES
& LICENSE COMPLIANCE DATA

- ☑ DASHBOARDS
- ☑ HEATMAPS
- ☑ TIME TRENDS
- ☑ TASKS
- ☑ LOCAL KNOWLEDGE BASE

MySQL, PostgreSQL

RISK MITIGATION TASKS

JIRA

Quality/Security scanner comparison matrix

FEATURE	Code WeTrust	MEND (White source)	Fossa	CAST	SNYK	Synopsis (Black Duck)	Synopsis (Coverity)	Sonar Source	Checkmarx	JetBrains Quodana
Standalone on-prem deployment Scanner+BI (Risk viewer)	✅							✅	✅	✅
Target audience	Executives Advisors Developers	Advisors Developers	Advisors Developers	Advisors	Developers Advisors	Advisors	Developers	Developers	Developers	Developers
Code reviews-Programming languages	25	0	0	15	0	0	22	30	18	7
Security (Software Composition Analysis) Programming Languages	ALL	ALL	ALL	ALL	ALL	ALL	22	0	18	7
Continuous Integration / Deployment	✅	✅			✅			✅	✅	✅
Source Code Quality Assessment	✅			✅				✅		
Full Vulnerabilities assessment (CVE, CWE)	✅	✅	✅	✅	✅					
“Blind” Audit - scanner	✅	limited		limited				limited	limited	✅
“Blind” Audit - BI	✅									
Licence Regulations Compliance Assessment	✅	✅	✅	✅	✅	✅				

CODE WE TRUST

trustilio
Enhance your Trustworthiness

WE DO APPRECIATE YOUR TIME!