Finally. *Trust* in Open Source

WWW.DARKSKYTECHNOLOGY.COM


Rocky Linux™
DARPA
BULLETPROOF
TRUST

DARPA Goals and Approach

BULLETPROOF TRUST

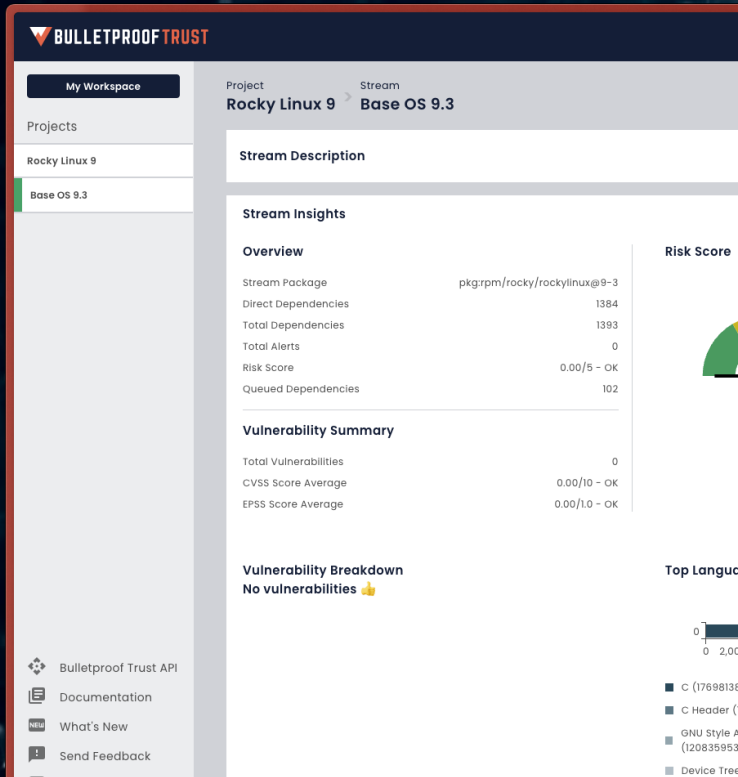
Data Collection
Large scale collection of all packages and contributor intel

Package Risk Analysis
Risk analysis of collected intel across large dataset

Independent V&V
Expert assessment of collected intel and analysis results

Alert Profile
Generate a risk “policy” by which to measure Linux distros

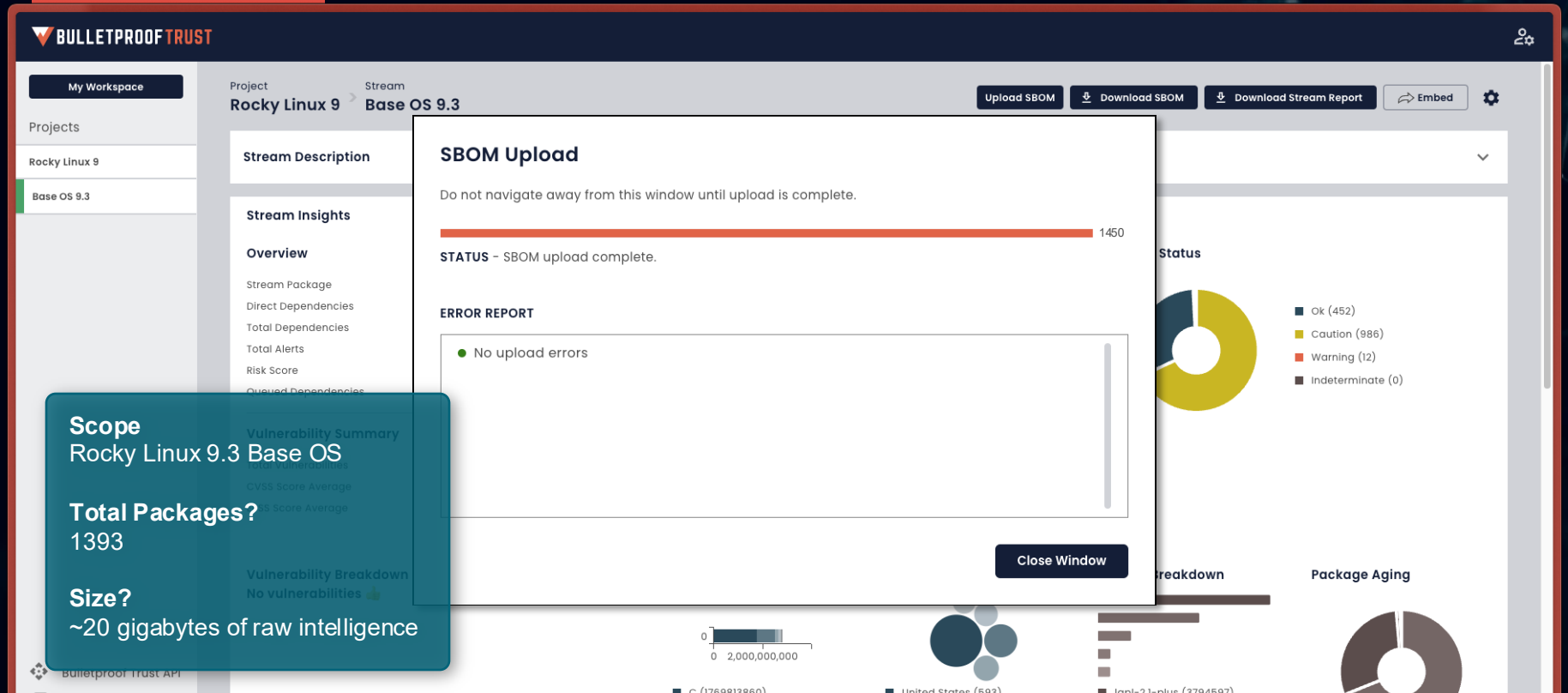
Dynamic Report
“Live” report based on policy adjustments and intel updates



BULLETPROOF TRUST

Load SBOM

Load SBOM
Obtain package list, manually create SBOM, load into Bulletproof Trust for collection and analysis.



Scope
Rocky Linux 9.3 Base OS

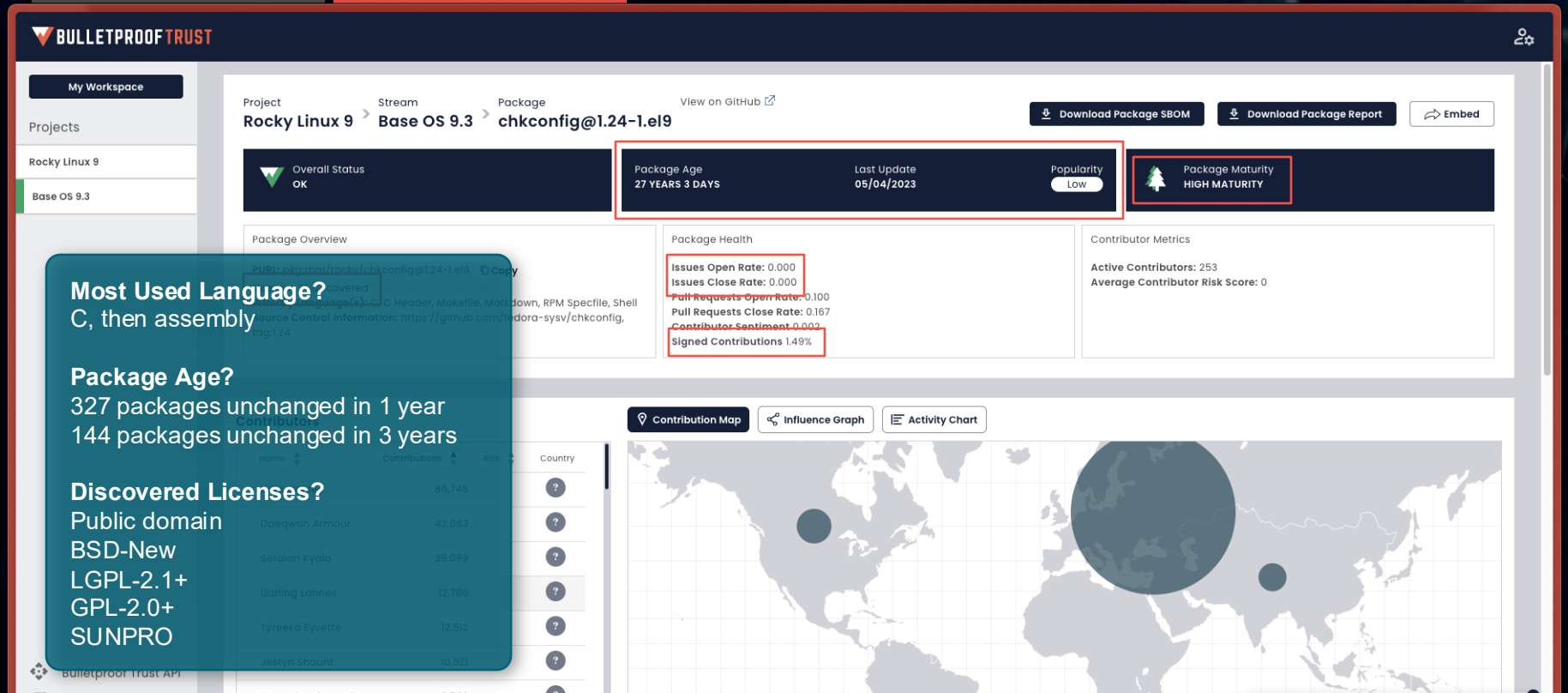
Total Packages?
1393

Size?
~20 gigabytes of raw intelligence

BULLETPROOF TRUST

Load SBOM | Package Data

Collect Package Data
General intelligence on each package: License info, package age, popularity, maturity, issues, trends, languages, etc.



Most Used Language?
C, then assembly

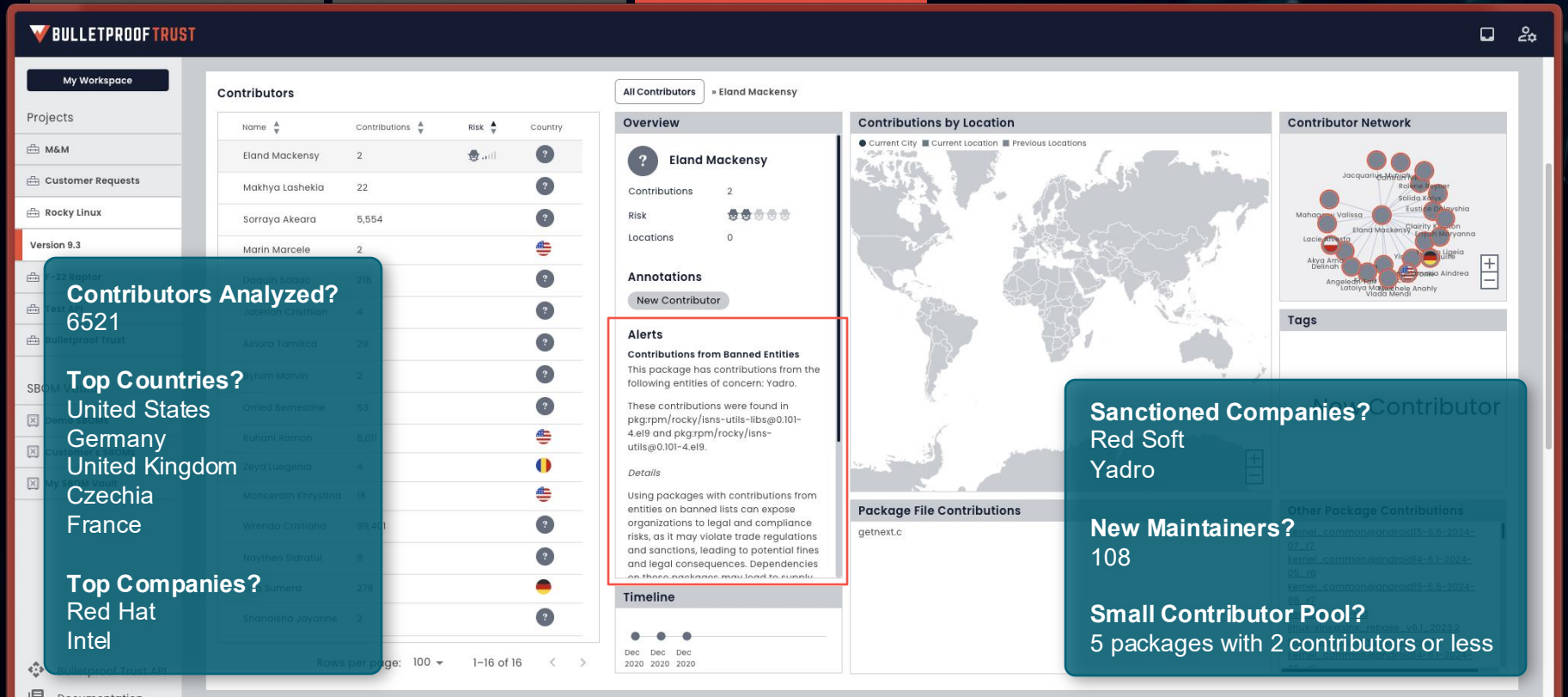
Package Age?
327 packages unchanged in 1 year
144 packages unchanged in 3 years

Discovered Licenses?
Public domain
BSD-New
LGPL-2.1+
GPL-2.0+
SUNPRO

BULLETPROOF TRUST

Load SBOM | Package Data | Contributor Data

Investigate Contributors
Collect and analyze intelligence on contributor network of connections, work/academic history, location, and behaviors.



Contributors Analyzed?
6521

Top Countries?
United States
Germany
United Kingdom
Czechia
France

Top Companies?
Red Hat
Intel

Sanctioned Companies?
Red Soft
Yadro

New Maintainers?
108

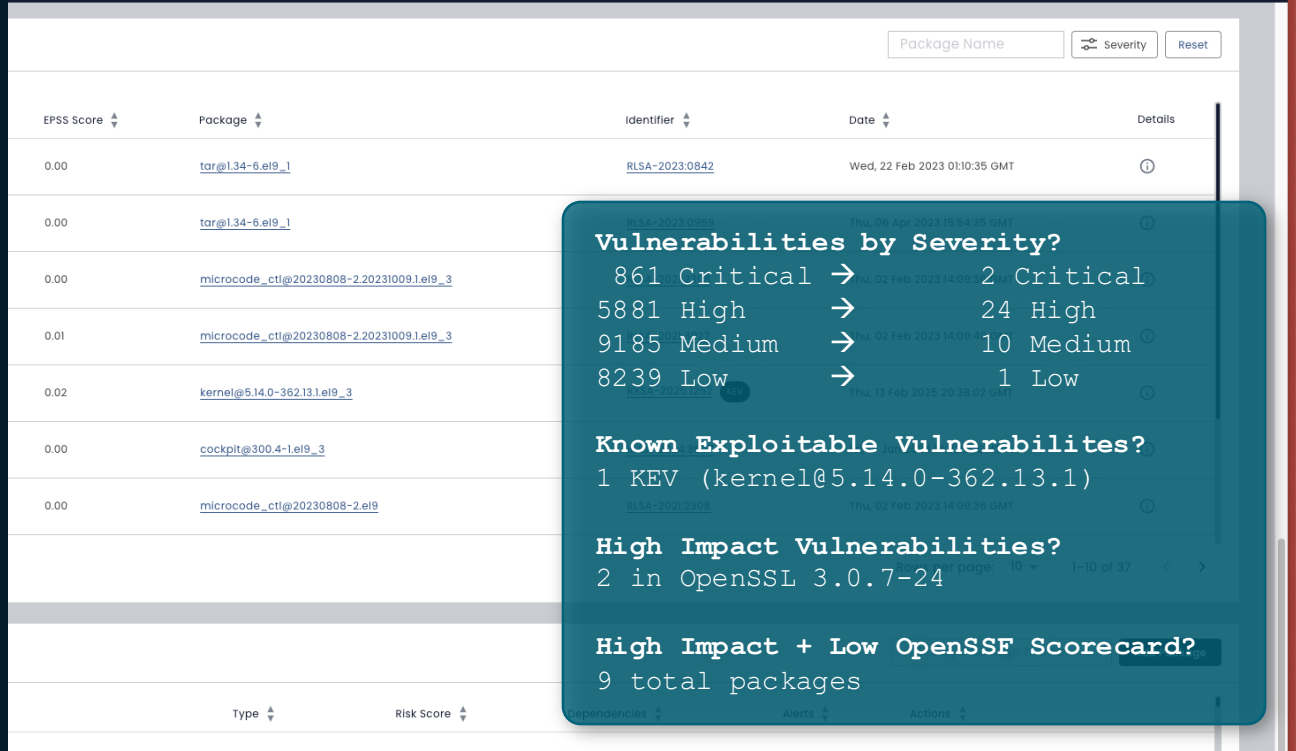
Small Contributor Pool?
5 packages with 2 contributors or less

BULLETPROOF TRUST

Package Data | Contributor Data | Vulnerabilities

Retrieve Vulnerabilities
Collect vulnerability intelligence form 28 vulnerability databases and analyze for applicability.

- National Vulnerability Database
- Github Security Advisories
- Open-Source Vulnerability Database
- AlmaLinux Vulnerability Database
- Alpine Linux Vulnerability Database
- Android Vulnerability Database
- Crates.io
- Debian Vulnerability Database
- Go Vulnerability Database
- Maven Vulnerability Database
- NPM Vulnerability Database
- Nuget Vulnerability Database
- Packagist, OSS-Fuzz, Ricjyt, Ruby, etc.



Vulnerabilities by Severity?

861 Critical	→	2 Critical
5881 High	→	24 High
9185 Medium	→	10 Medium
8239 Low	→	1 Low

Known Exploitable Vulnerabilites?
1 KEV (kernel@5.14.0-362.13.1)

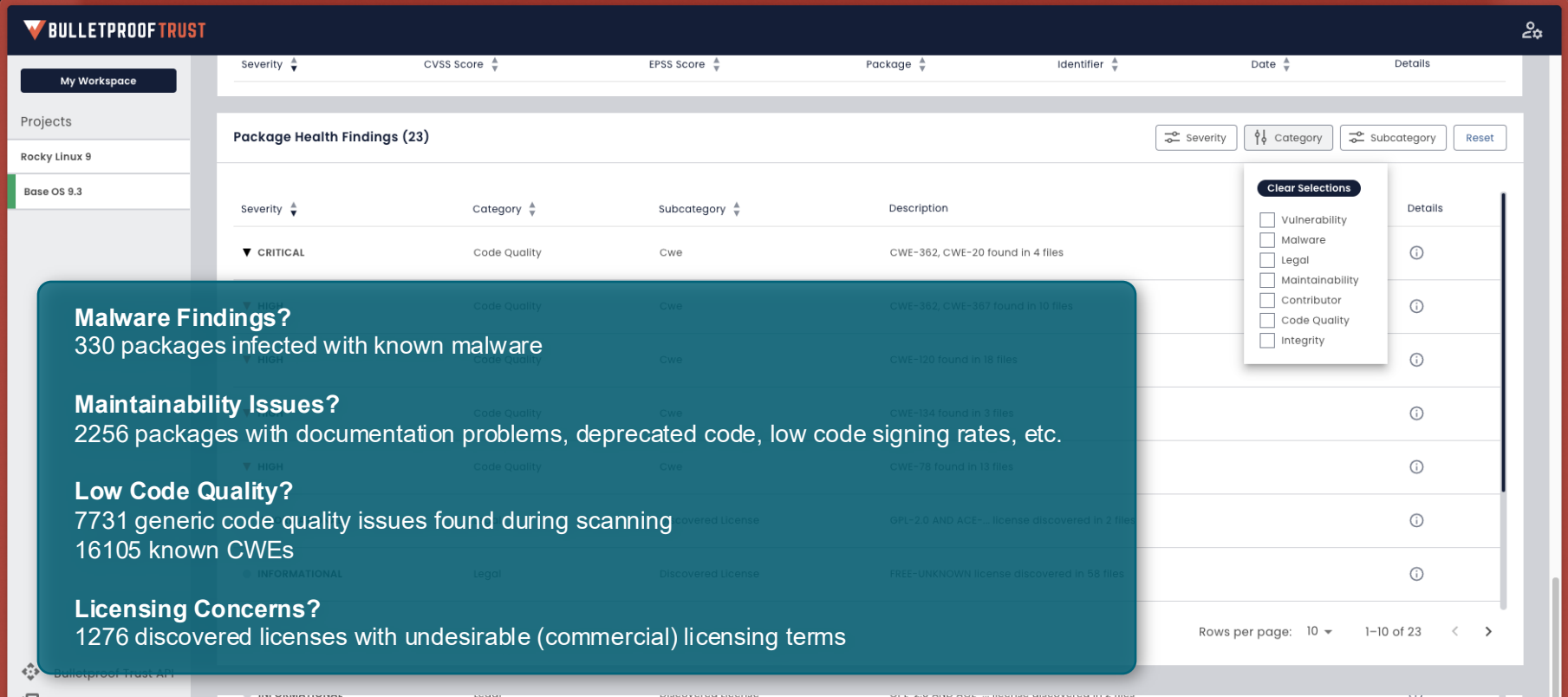
High Impact Vulnerabilities?
2 in OpenSSL 3.0.7-24

High Impact + Low OpenSSF Scorecard?
9 total packages

BULLETPROOF TRUST

Contributor Data | Vulnerabilities | Package Health

Analyze Package Health
Run a variety of code quality, documentation quality, license, malware, and other scanners to detect package health issues.



Malware Findings?
330 packages infected with known malware

Maintainability Issues?
2256 packages with documentation problems, deprecated code, low code signing rates, etc.

Low Code Quality?
7731 generic code quality issues found during scanning
16105 known CWEs

Licensing Concerns?
1276 discovered licenses with undesirable (commercial) licensing terms

BULLETPROOF TRUST

Vulnerabilities | Package Health | Alert Model

Develop Alert Model
Configure rules for severity and type of alert based on analysis and exceeding data thresholds.

BULLETPROOF TRUST

Critical Severity Alerts?

+ CRITICAL	Known KEVs
+ CRITICAL	Exploitable Vulnerabilities
+ CRITICAL	Outdated Package with Vulnerabilities
+ CRITICAL	Banned Maintainer Entity

High Severity Alerts?

+ HIGH	High Impact Vulnerabilities
+ HIGH	High Severity Vulnerability with Low OpenSSF Scorecard
+ HIGH	No License Detected
+ HIGH	Too Many Critical Package Health Findings

Medium Severity Alerts?

+ MEDIUM	Banned Contributor Entity
+ MEDIUM	Issue Growth Outpacing Contributor Pool
+ MEDIUM	Typosquatting Detected
+ MEDIUM	High Merge Rate with Vulnerabilities

Low Severity Alerts?

+ LOW	Maintainer is New Contributor
+ LOW	Undesirable Commercial License
+ LOW	Too Few Contributors

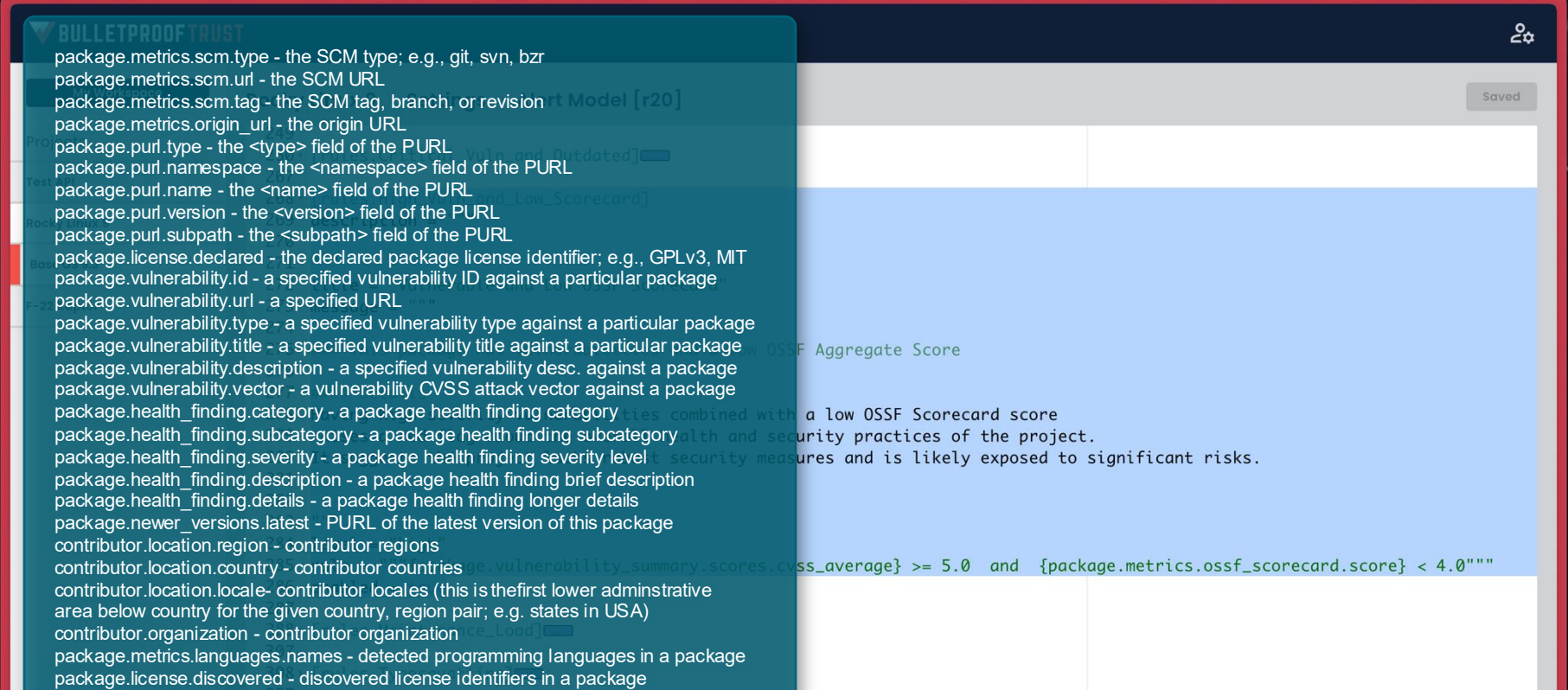
Informational Alerts?

+ INFO	Package Out of Date
+ INFO	Package Too Immature

BULLETPROOF TRUST

Vulnerabilities | Package Health | Alert Model

Customized Alertable Conditions
Updates to the alert model based on new alertable conditions to more accurately measure the risk of the distribution.



Progress & Challenges

Initial Data Collection

Preliminary Analysis

Results Review

Starting Alert Model

Package URLs?

Vulnerability Attribution?

Alert Applicability?

Next Distribution?

Finally. *Trust* in Open Source

INFO@DARKSKYTECHNOLOGY.COM