Static Code Analysis Linux Software Engineering

How do Coverity, Parasoft and Klocwork compare on their static analysis tools?

What company provides the best static code analysis tools for a Linux environment?

4 Answers

Dragon Slayer
4.3k Views

I work for a large software company with 2000+ engineers and architects. My team did a [illegible] ive analysis. This included commercial tools: Klocwork, Coverity, Parasoft, CPPCheck, and Checkmarx, & Visual Studio. We also reviewed free tools such as CPP Check. With all standard rules and MISRA rules enabled, the coverage varied:

Klocwork:	13
Coverity:	11
Parasoft:	10
Checkmarx:	5
PVS-Studio:	5
Visual Studio:	4
CPPCheck:	3

We did not get a chance to leverage HP Fortify yet.

After including KW custom rules, coverage increased to 21 patterns.

Klocwork was the most user friendly IMO. Better web reports and Visual Studio plugin than the rest. However, it does not have a Jenkins plugin. Emenda created a Klocwork plugin for Jenkins and sonarqube. Klocwork has about 500 rules for C++. We have several hundred licenses. We have great success stories with proactively solving crashes in the field and prevention based off an internal program built around addressing targeted KW vulnerabilities. We create both KAST and PATH type rules internally. We have a big complaint with software package quality and support overall.

Coverity has a small set of rules but they are generally very accurate and have a low false positive rate. The web portal and plugins are of comparable usability to Klocwork. We performed a trial and were impressed. We chose not to invest since it does not provide much more coverage than Klocwork and we already had KW licenses. Given a do-over, I'd want to talk to Coverity clients about their support experience and possibly invest with them over KW.

Klocwork has 'on the fly' analysis whereas Coverity says its not possible to do efficiently. It actually is a similar experience as Visual Studio's intellisence so long as the user has 8GB of RAM or more. Our engineers with just 4GB ram and a bunch of apps open have less than 0.5 GB free and wait up to 10 seconds for the 'on the fly' analysis to complete. Those with more RAM don't wait longer than 1-2 seconds. This can be turned off and the file, project, or solution scanned on demand like with Coverity and all the other tools.

Parasoft is somewhere in the middle from a usability perspective. Some will see it as an advantage that Parasoft bundles a unit testing framework. We felt the unit testing framework was good but too slow for our engineers to accept. Their C++ ecosystem has lots of tools grouped together and your engineers will consider the web portal and VS plugin to be noisy if they only want to leverage static code analysis.

One bonus for Parasoft is that they have open arms to import vulnerabilities from third party vendors into their ecosystem. This is a nice break from some vendors (KW) that restrict this to prevent clients from leveraging multiple vendors. It is a no brainer if Parasoft is right for you to buy a few licenses from other tools and inject the coverage into Parasoft. We have a handful of licenses and are struggling with KW to get access to instructions for importing Parasoft vulnerabilities. As result, we may buy Parasoft licenses and simply inject KW into it. (note: Coverity allows for this too. KW has the capability

Related Questions

- What is the best combination of static analysis tools for the best coverage in C and C++?
- Is there a Linux equivalent of Microsoft's PREFast static code analysis and annotation tool?
- Why Don't Software Developers Use Static Analysis Tools to Find Bug?
- Is X Any Good?: Is it useful to use Klocwork type tools?
- What are some good C++ static code analysis?
- Are there any static analysis tools for JavaScript?
- Static Code Analysis: Why don't compilers detect the errors that Cppcheck finds?
- How should I go about writing a static code analysis tool for Erlang?
- Do developers at Facebook use PHP (programming language) Static Code Analysis tools? If yes, what is the most popular php ...
- Static Code Analysis: What are good ways to analyse Java source code that contains errors?

but will not openly share instructions -- they say there is no benefit to do so from a self-interest perspective)

PVS-Studio -- we bought a few licenses of this simply to help with an imperative to upgrade 32bit apps to 64bit.

Checkmarx has an awesome feature on impact analysis. You can look at similarities in function calls and determine the earliest place to correct vulnerabilities. Say there is one function accepting unsecure user input and this is leveraged in 50 places. Checkmarx points out that fixing one function will impact 50 areas at risk. Pretty cool. However, their C++ analysis is below average (they admit this too as their weakest language). Also, their Visual Studio plugin has too many windows and is much slower compared to Parasoft, Coverity, and Klocwork that makes it "unusable." Checkmarx is a security focused company. We will re-review for RUBY, Java, etc in the future.

Written 1 Aug 2014 • View Upvotes

More Answers Below. **Related Questions**

What is the best combination of static analysis tools for the best coverage in C and C++?

Is there a Linux equivalent of Microsoft's PREFast static code analysis and annotation tool?

Why Don't Software Developers Use Static Analysis Tools to Find Bug?

Is X Any Good?: Is it useful to use Klocwork type tools?

What are some good C++ static code analysis?

Mitchell Roemer
3.6k Views

I work at Parasoft. I'm not going to compare tools here, but I'd like to encourage you to read the vendor-agnostic guide we wrote on selecting a static analysis tool that your team will actually use. (http://alm.parasoft.com/static-a...). It talks about how to move beyond "bake off" type comparisons and determine which tool is the best long-term fit for your process and priorities.

Written 2 May 2012 • View Upvotes

Sarah Vonnegut, Content Writer, Community Manager
1.6k Views

The difference between Checkmarx and some of the other tools mentioned in this thread (disclaimer: I'm a Checkmarx employee) is that Checkmarx is built with security testing at top of mind, while many of the other tools mentioned are built for quality testing first with security testing added later.

Checkmarx is very strong in mobile and scripting languages, especially JavaScript.

Here's a good article on how to choose a static code analysis tool for your specific needs:
The AppSec How-to: Choosing a SAST Tool

Written 8 Apr 2015

Cynthia Dunlop
1.3k Views

Static Code Analysis is predicated on two primary capabilities: the engine that performs the analysis and the anti-patterns that the engine references. Checkmarx's focus is a business decision driven by their board and investors because that's where they see the best return on investment. Remember: as soon as a private business take venture funding, that business is for sale.

Written 8 Apr 2015

Related Questions

Are there any static analysis tools for JavaScript?

Static Code Analysis: Why don't compilers detect the errors that Cppcheck finds?

How should I go about writing a static code analysis tool for Erlang?

Do developers at Facebook use PHP (programming language) Static Code Analysis tools? If yes, what is the most popular php static analysis tool...

Static Code Analysis: What are good ways to analyse Java source code that contains errors?

Is there a good PHP lint / static analysis tool?

What are the best tools for Python static analysis?

What are some static code analysis tools for Python, specifically to identify insecure coding practices?

Which Java linters/static code analysis tools are used in Google?

What are some good resource for writing a static analysis tool?

Why is static analysis important?

How does KDev-Python do static analysis?

Does "model checking" belong to "static analysis"?

How do I learn static program analysis?

How does static program analysis work?

Top Stories

What is the most awesome feeling?

Robledo Cabral, 20-year-old Brazilian daydreamer

4.9k Views

Reaching an epiphany -- whether it's related to finding the teeny tiny string of Java code which will allow your enormous project to work or to finally understanding the one concept you still haven't managed to decipher after hours of study.

Read More

If one could radically change one major aspect of how a city operates, what should it be?

Mark Mazzeo, Industrial Engineer

1.1k Views

Establish an urban system based on clusters. Clusters would be the foundation of urban systems, based on the idea that everything you might need and everywhere you might go around your town ought to be within walking distance, or within a mile or two. One urban center, say between 5,000 and 20,000 residents (with probably around 2,500 to 5,000 per square mile), would

Read More

What math problem with an elementary solution was unsolved for the longest period?

Alon Amit, PhD in Mathematics; Mathcircler.

25k Views • Upvoted by Thomas Karam, Mathematician, ENS Ulm, Paris • Yair Livne, Director of Product Management at Quora • Qiaochu Yuan, PhD student in Mathematics at UC Berkeley

Alon is a Most Viewed Writer in Open Problems.

Read More