Context Matters: Qualitative Insights into Developers' Approaches and Challenges with Software Composition Analysis

Elizabeth Lin, Sparsha Gowda,
William Enck, Dominik Wermke

whoami

- Completed my bachelors in CS in Taiwan
- Joined the Wolfpack Security and Privacy Research Lab (WSPR) as PhD student in 2022
- Worked on various software supply chain security projects
- https://elizabethtlin.com/
- etlin@ncsu.edu

Secure Computing Institute (SCI) @ NC State

WSPR

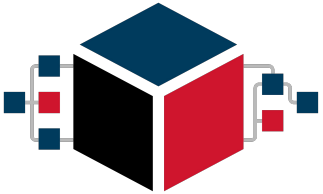
Security
Privacy

Qualitative
Research

Networks
Telecom

Cryptography

Software
Engineering



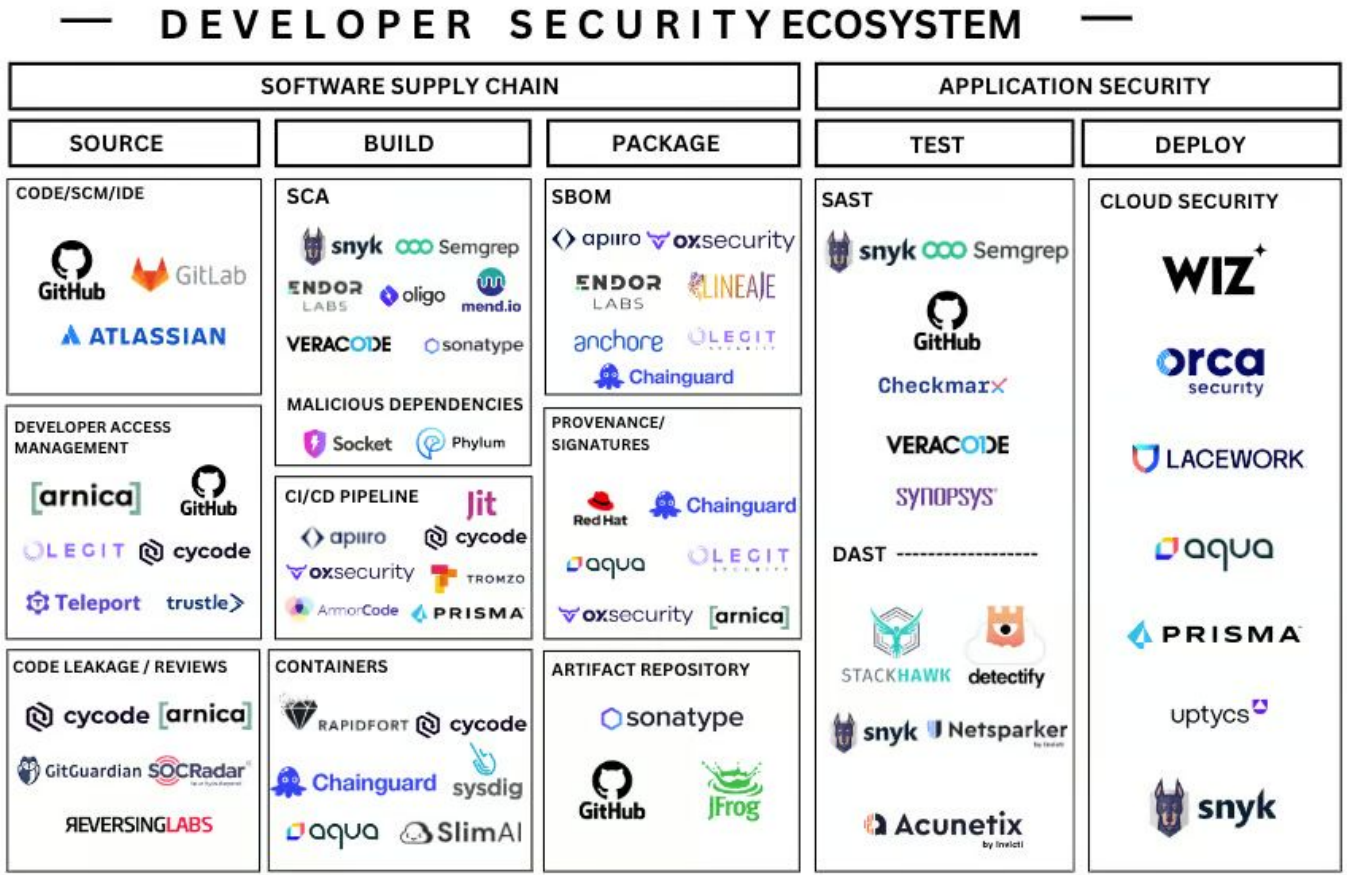
S3C2
SECURE SOFTWARE SUPPLY CHAIN CENTER

What is your experience with SCA?

SCA = Software Composition Analysis

VERACODE

sonatype

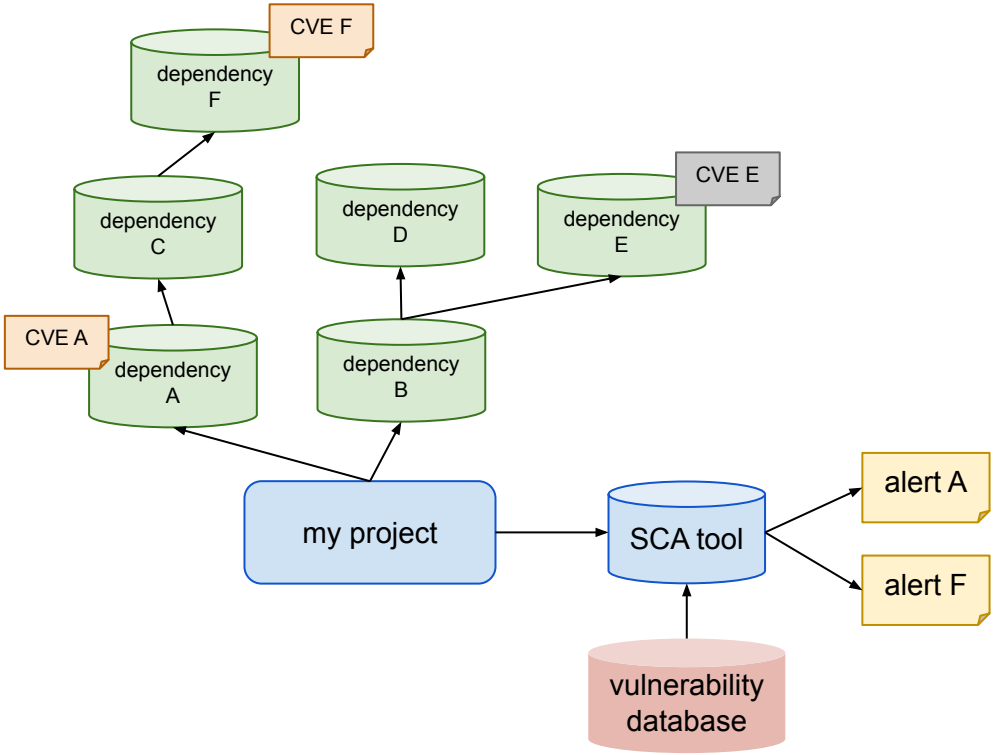


https://tldrsec.com/p/software-supply-chain-vendor-landscape

Software Supply Chain Incident

Ideal SCA

- ❑ Smooth deployment
- ❑ Identifies components correctly
- ❑ Alerts on vulnerabilities that **matter**
- ❑ Clear fix suggestions



5 elizabethtl/Online_Travel_Reservation 11 C 133 H 127 M 47 L

Project	Imported	Tested	Issues
kayak_react/package.json	6 months ago	3 days ago	9 C 69 H 77 M 10 L
kayak_kafka_backend/package.json	6 months ago	7 days ago	1 C 36 H 17 M 3 L
kayak_kafka_frontend/package.json	6 months ago	4 days ago	1 C 24 H 25 M 5 L
Code analysis	6 months ago	5 days ago	0 C 4 H 8 M 29 L
kayak_react/src/components/user/HotelList/bootstrap/package.json	6 months ago	6 days ago	0 C 0 H 0 M 0 L

Which result do I look at?

Issues 165 Fixes Dependencies 1065

DEPENDENCY	LATEST	LAST PUBLISHED	ISSUES
babel-traverse@6.26.0			69 C 0 H 0 M 0 L
elliptic@6.4.0			10 C 4 H 4 M 0 L
hawk@6.0.2			3 C 3 H 0 M 0 L
handlebars@4.0.11			1 C 6 H 2 M 0 L
macaddress@0.2.8			1 C 0 H 1 M 0 L
lodash@4.17.4			0 C 2.0k H 1.0k M 0 L
ansi-regex@2.1.1			0 C 516 H 0 M 0 L
es5-ext@0.10.35			0 C 91 H 0 M 0 L
ua-parser-js@0.7.17			0 C 72 H 72 M 0 L
braces@1.8.5			0 C 30 H 0 M 30 L

Which alert do I look at first?

babel-traverse - Incomplete List of Disallowed Inputs

SCORE 786

VULNERABILITY | CWE-184 | CVE-2023-45133 | CVSS 9.3 | CRITICAL | SNYK-JS-BABELTRAVERSE-5962463

Introduced through react-scripts@1.0.13

Exploit maturity PROOF OF CONCEPT

Overview

Affected versions of this package are vulnerable to Incomplete List of Disallowed Inputs when using plugins that rely on the `path.evaluate()` or `path.evaluateTruthy()` internal Babel methods.

Note:

This is only exploitable if the attacker uses known affected plugins such as `@babel/plugin-transform-runtime`, `@babel/preset-env` when using its `useBuiltIns` option, and any "polyfill provider" plugin that depends on `@babel/helper-define-polyfill-provider`. No other plugins under the `@babel/` namespace are impacted, but third-party plugins might be.

*Users that only compile trusted code are **not** impacted.*

Ignore | Fix this vulnerability

Only exploitable if …?

babel-traverse - Incomplete List of Disallowed Inputs

VULNERABILITY | CWE-184 | CVE-2023-45133 | CVSS 9.3 CRITICAL | SNYK-JS-BABELTRAVERSE-5962463

Introduced through react-scripts@1.0.13 Exploit maturity

Show less detail

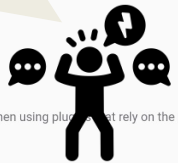
Detailed paths and remediation

- Introduced through: kayak_react@1.0.0 › react-scripts@1.0.13 › babel-core@6.25.0 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@3.0.0
- Introduced through: kayak_react@1.0.0 › react-scripts@1.0.13 › babel-eslint@7.2.3 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@3.4.1
- Introduced through: kayak_react@1.0.0 › react-scripts@1.0.13 › babel-core@6.25.0 › babel-template@6.26.0 › babel-travers
  Fix: Upgrade to react-scripts@3.0.0

Maybe more CVE information will help

- Snyk: CVSS v3.1 9.3 - Critical Severity
- NVD: CVSS v3.1 8.8 - High Severity

Why are the scores different? Learn how Snyk evaluates vulnerability scores



Overview

Affected versions of this package are vulnerable to Incomplete List of Disallowed Inputs when using plu[illegible]t rely on the `path.evaluateTruthy()` internal Babel methods.

Note:

This is only exploitable if the attacker uses known affected plugins such as `@babel/plugin-transform-runtime`, `@babel/pre` option, and any "polyfill provider" plugin that depends on `@babel/helper-define-polyfill-provider`. No other plugins under impacted, but third-party plugins might be.

*Users that only compile trusted code are **not** impacted.*

Ignore | Fix this vulnerability

CVE-2023-45133 PUBLISHED

View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: GitHub (maintainer security advisories) –

Published: 2023-10-12 **Updated:** 2023-10-19
Title: Babel Vulnerable To Arbitrary Code Execution When Compiling Specifically Crafted Malicious Code

Description

Babel is a compiler for writingJavaScript. In `@babel/traverse` prior to versions 7.23.2 and 8.0.0-alpha.4 and all versions of `babel-traverse`, using Babel to compile code that was specifically crafted by an attacker can lead to arbitrary code execution during compilation, when using plugins that rely on the `path.evaluate()`or `path.evaluateTruthy()` internal Babel methods. Known affected plugins are `@babel/plugin-transform-runtime`; `@babel/preset-env` when using its `useBuiltIns` option; and any "polyfill provider" plugin that depends on `@babel/helper-define-polyfill-provider`, such as `babel-plugin-polyfill-corejs3`, `babel-plugin-polyfill-corejs2`, `babel-plugin-polyfill-es-shims`, `babel-plugin-polyfill-regenerator`. No other plugins under the `@babel/` namespace are impacted, but third-party plugins might be. Users that only compile trusted code are not impacted. The vulnerability has been fixed in `@babel/traverse@7.23.2` and `@babel/traverse@8.0.0-alpha.4`. Those who cannot upgrade `@babel/traverse` and are using one of the affected packages mentioned above should upgrade them to their latest version to avoid triggering the vulnerable code path in affected `@babel/traverse` versions: `@babel/plugin-transform-runtime` v7.23.2, `@babel/preset-env` v7.23.2, `@babel/helper-define-polyfill-provider` v0.4.3, `babel-plugin-polyfill-corejs2` v0.4.6, `babel-plugin-polyfill-corejs3` v0.8.5, `babel-plugin-polyfill-es-shims` v0.10.0, `babel-plugin-polyfill-regenerator` v0.5.3.

C **babel-traverse** - Incomplete List of Disallowed Inputs

SCORE 786

VULNERABILITY | CWE-184 | CVE-2023-45133 | CVSS 9.3 | CRITICAL | SNYK-JS-BABELTRAVERSE-5962463

Introduced through react-scripts@1.0.13

Exploit maturity PROOF OF CONCEPT

Show less detail

Detailed paths and remediation

- **Introduced through:** kayak_react@1.0.0 › react-scripts@1.0.13 › babel-core@6.25.0 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@3.0.0
- **Introduced through:** kayak_react@1.0.0 › react-scripts@1.0.13 › babel-eslint@7.2.3 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@3.4.1
- **Introduced through:** kayak_react@1.0.0 › react-scripts@1.0.13 › babel-core@6.25.0 › babel-template@6.26.0 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@3.0.0
- **Introduced through:** kayak_react@1.0.0 › react-scripts@1.0.13 › babel-jest@20.0.3 › babel-core@6.25.0 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@2.0.3
- **Introduced through:** kayak_react@1.0.0 › react-scripts@1.0.13 › babel-core@6.25.0 › babel-helpers@6.24.1 › babel-template@6.26.0 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@3.0.0
- **Introduced through:** kayak_react@1.0.0 › react-scripts@1.0.13 › babel-jest@20.0.3 › babel-core@6.25.0 › babel-template@6.26.0 › babel-traverse@6.26.0
  Fix: Upgrade to react-scripts@2.0.3
- **Introduced through:** kayak_react@1.0.0 › react-scripts@1.0.13 › babel-preset-react-app@3.1.0 › babel-plugin-dynamic-import-node@1.1.0 › babel-template@6.26.0 › babel-traverse@6.26.0

Do I update?

Which version do I update to?

H **lodash** - Prototype Pollution

VULNERABILITY | •••

SCORE
731

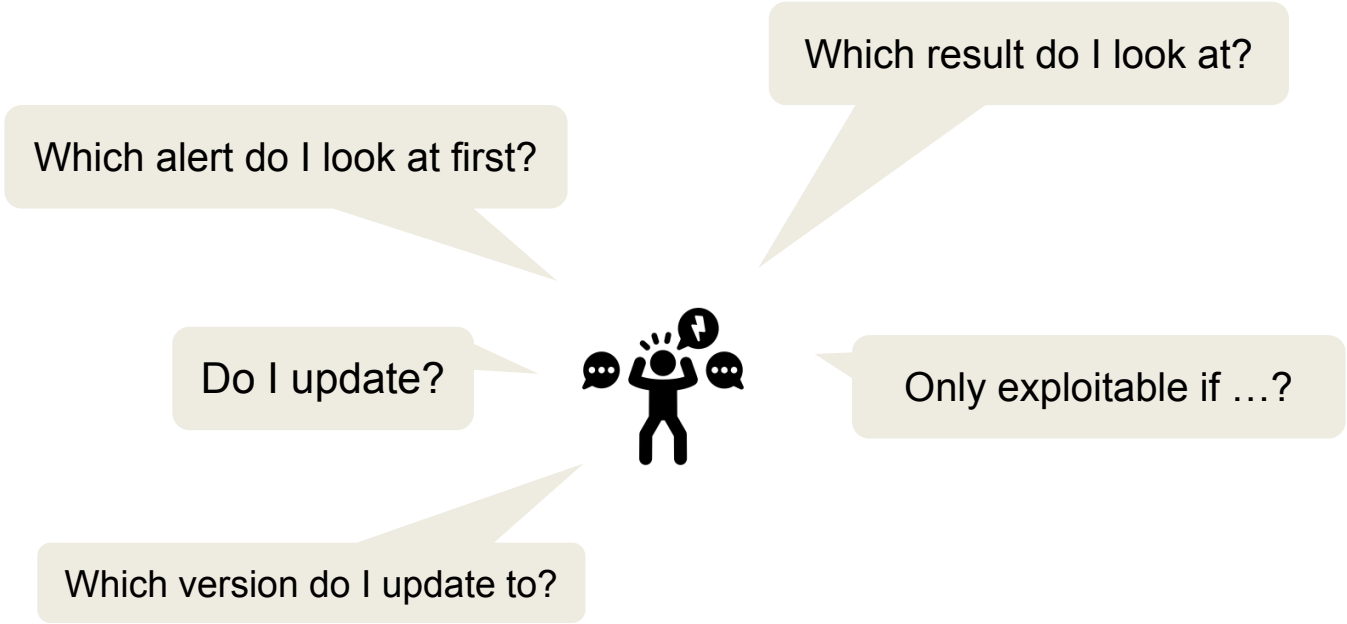
Introduced through	react-chartjs-2@2.6.4, react-redux@5.0.6 and others	**Exploit maturity**	PROOF OF CONCEPT
Fixed in	lodash@4.17.20		

Show less detail

Detailed paths and remediation

- **Introduced through:** kayak_react@1.0.0 › react-chartjs-2@2.6.4 › lodash@4.17.4
  Fix: Upgrade to react-chartjs-2@3.2.0
- **Introduced through:** kayak_react@1.0.0 › react-redux@5.0.6 › lodash@4.17.4
  Fix: Upgrade to react-redux@5.1.0
- **Introduced through:** kayak_react@1.0.0 › redux@3.7.2 › lodash@4.17.4
  Fix: Upgrade to redux@4.0.0

Which dependency do I update?


Which result do I look at?
Which alert do I look at first?
Do I update?
Only exploitable if …?
Which version do I update to?

User Study

RQ1: How do users interact with SCA tools?

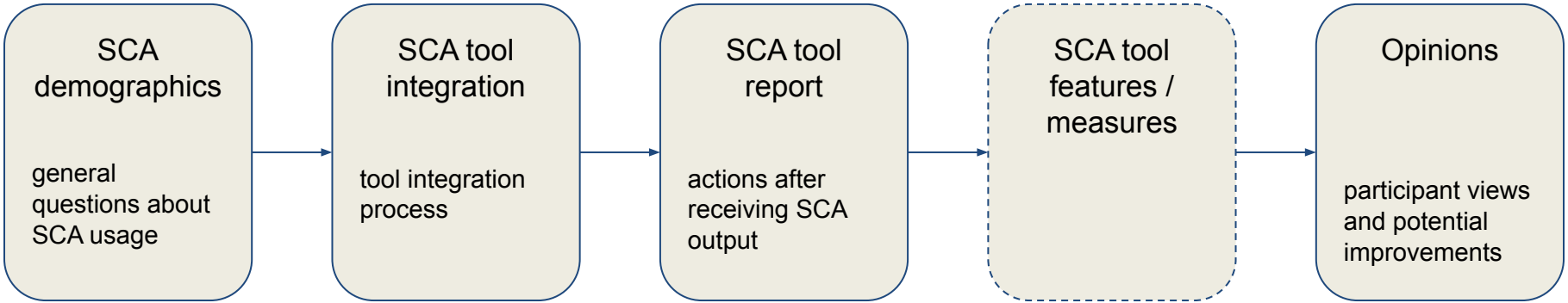
RQ2: What are the challenges when deploying SCA tools?

RQ3: What are the challenges when acting on SCA results?

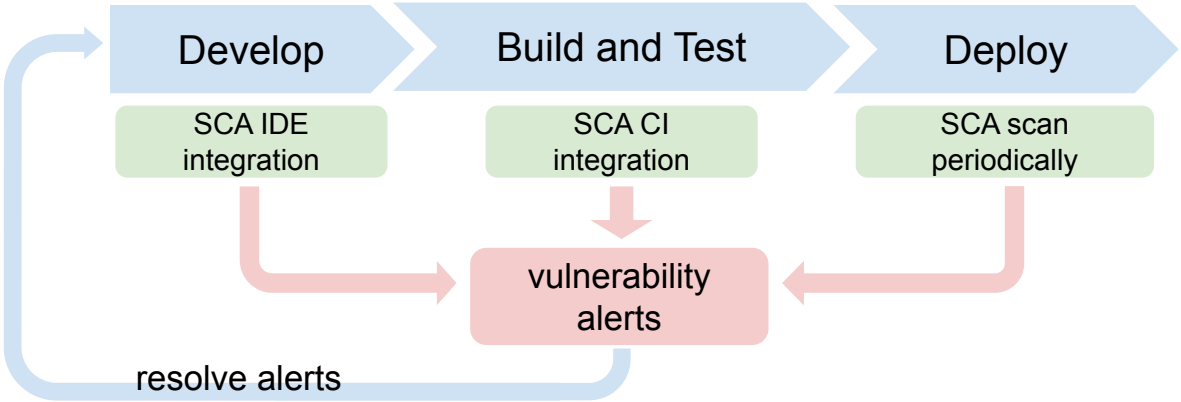
RQ4: How can the SCA process be improved?

User Study

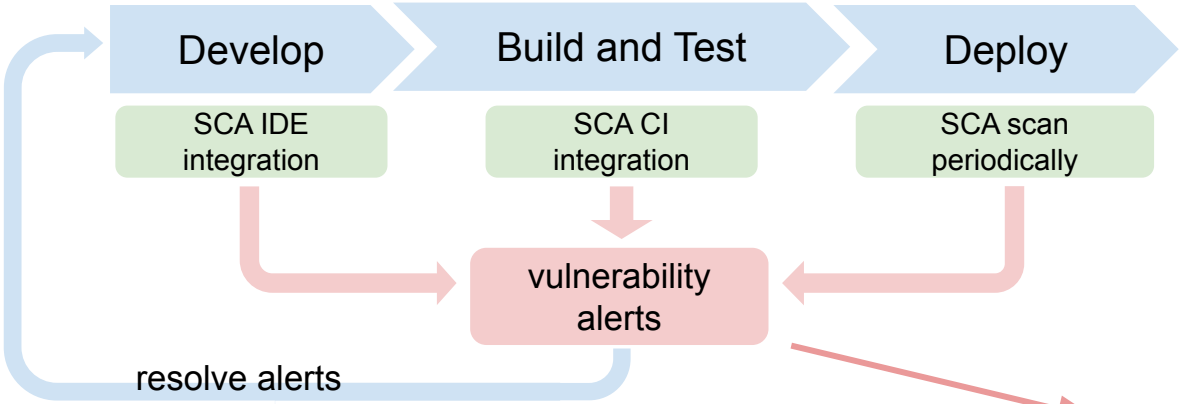
- 20 industry professionals with SCA experience
- ~45 minute semi-structured interview



Main Finding: Context Matters

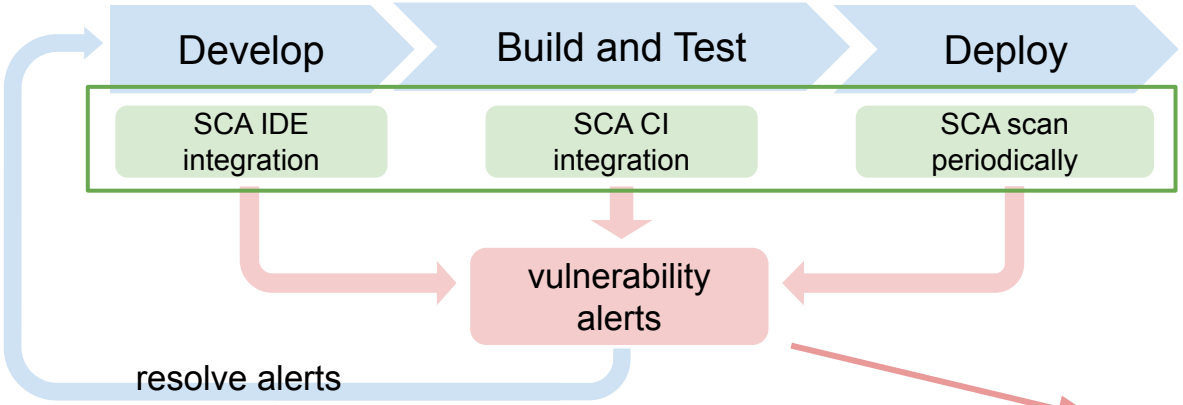


Main Finding: Context Matters



Theme 1
More information is needed to evaluate the risk and impact of the vulnerability alert.

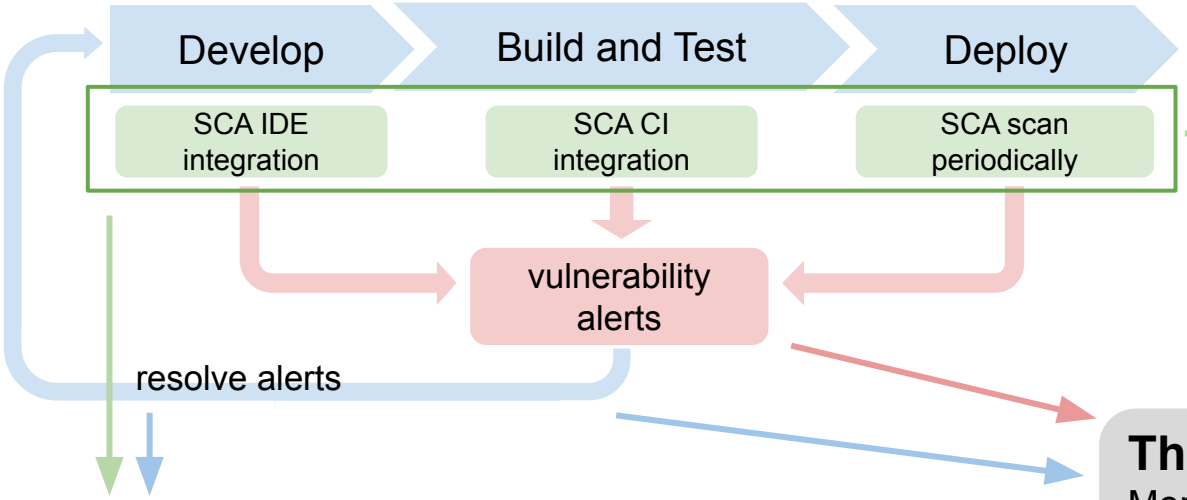
Main Finding: Context Matters



Theme 2
When and how the SCA scan runs in the development cycle matter.

Theme 1
More information is needed to evaluate the risk and impact of the vulnerability alert.

Main Finding: Context Matters



Theme 2
When and how the SCA scan runs in the development cycle matter.

Theme 1
More information is needed to evaluate the risk and impact of the vulnerability alert.

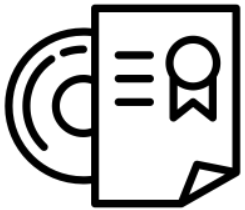
Theme 3
Integration of SCA and communication of the results can generate overhead if there is not enough context present.

How do users interact with SCA tools?

How do users interact with SCA tools?

Reasons for using SCA

Software Vulnerabilities

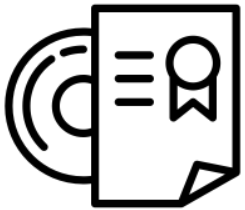


Compliance and Licensing

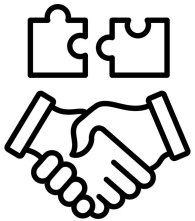
How do users interact with SCA tools?

Reasons for using SCA

Software Vulnerabilities



Compliance and Licensing



Mergers Acquisitions

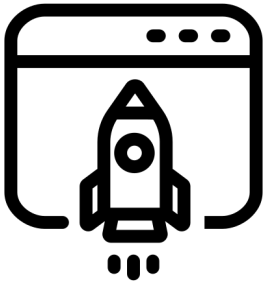
"We're buying a company or we're being bought, and you basically have to prove that your stack, if your stack is somewhat decently built"

Export Controls

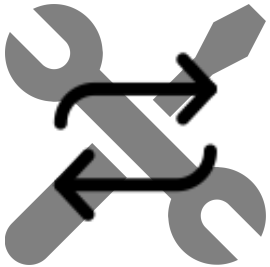
"U.S. laws very strict on certain cryptographic algorithms"

How do users interact with SCA tools?

Selecting SCA tools



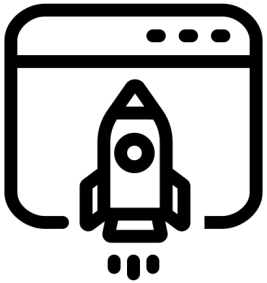
Ease of Deployment



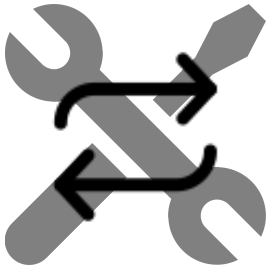
Switch Tools

How do users interact with SCA tools?

Selecting SCA tools



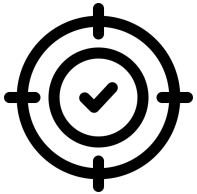
Ease of Deployment



Switch Tools

Tool Requirements

“The scan requirements to run T05 were very difficult to fulfill for some languages and for the varying build processes that we used”

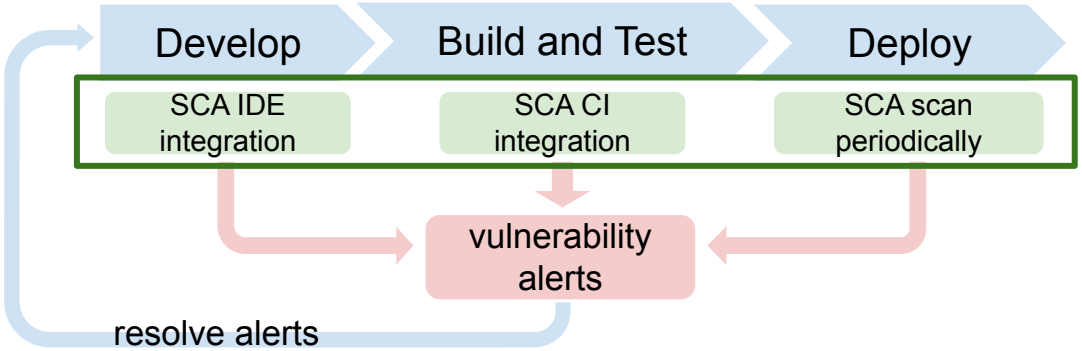


Result Accuracy

“It was not uncommon that the database would be reporting something wrong [. . .] it would match a component to an incorrect component”

How do users interact with SCA tools?

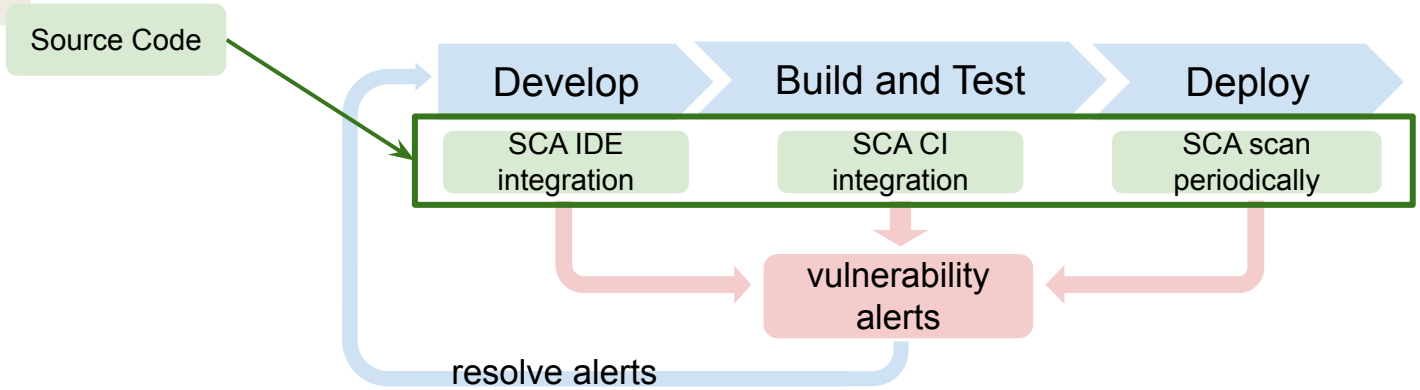
Input to SCA tools



How do users interact with SCA tools?

Input to SCA tools

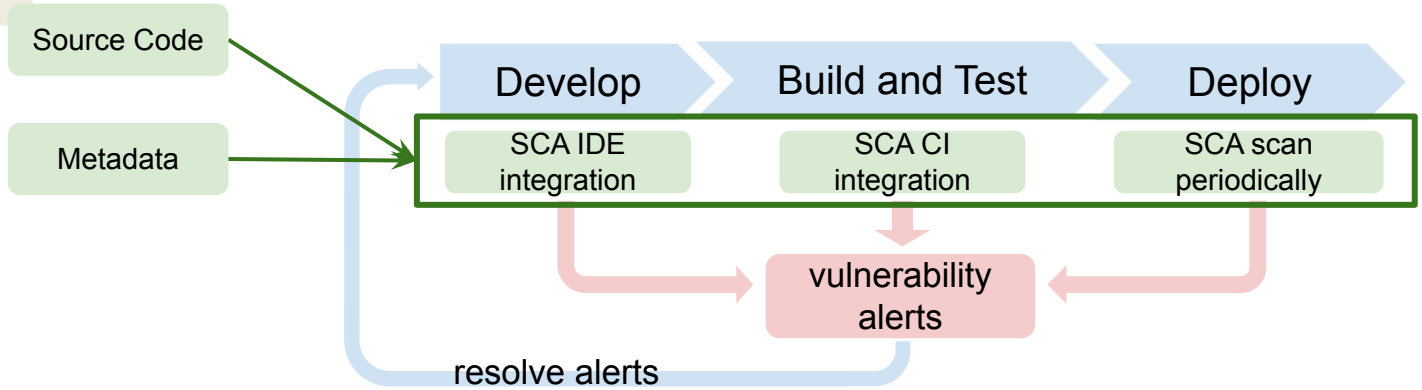
"We didn't use the cloud version because we didn't want the code to go outside"



How do users interact with SCA tools?

Input to SCA tools

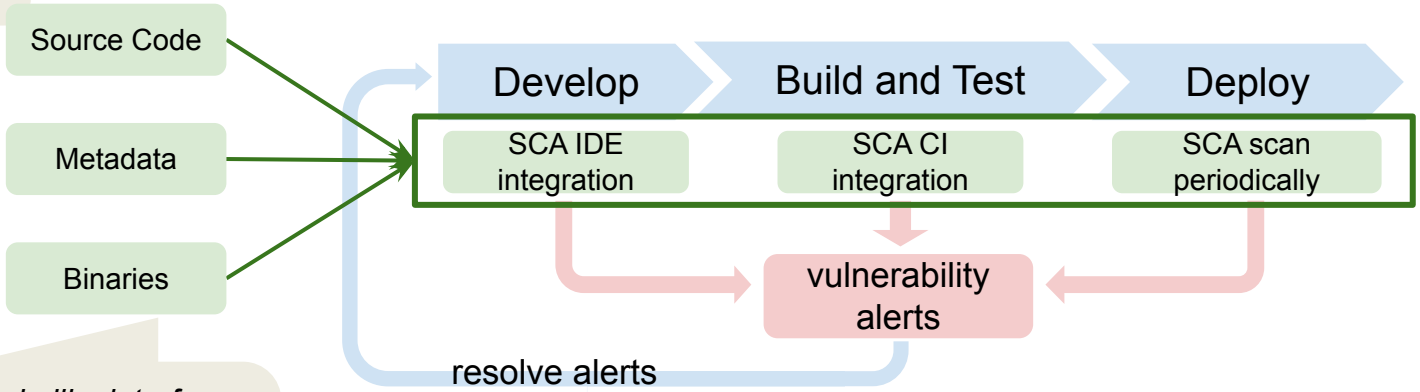
"We didn't use the cloud version because we didn't want the code to go outside"



How do users interact with SCA tools?

Input to SCA tools

"We didn't use the cloud version because we didn't want the code to go outside"



"You have lots of generated code like interfaces for the user interface. And that's just a lot of generated code where the tools that create the user interface, when you generate them, they just output a lot of boilerplate"

What are the challenges when deploying SCA tools?

What are the challenges when deploying SCA tools?

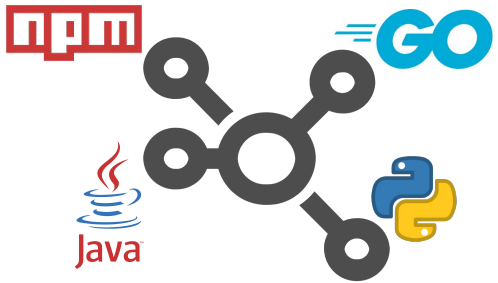
Legacy Languages
Unsupported Scripts

"We need to go and either pre-process things ourselves. We need to work with the supplier to add support for new file formats"

What are the challenges when deploying SCA tools?

Legacy Languages
Unsupported Scripts

"We need to go and either pre-process things ourselves. We need to work with the supplier to add support for new file formats"



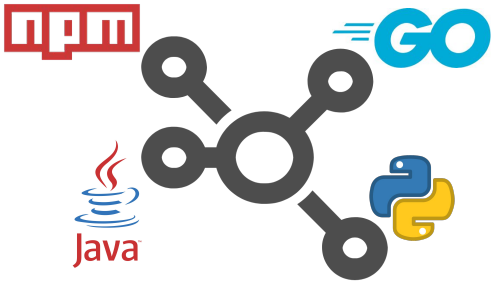
Different
Ecosystems

"All the package managers are different. So you have to have exceptions for each one and you have to figure out what those exceptions are"

What are the challenges when deploying SCA tools?

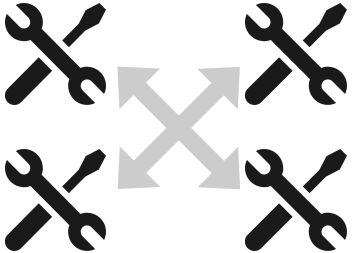
Legacy Languages
Unsupported Scripts

"We need to go and either pre-process things ourselves. We need to work with the supplier to add support for new file formats"



Different
Ecosystems

"All the package managers are different. So you have to have exceptions for each one and you have to figure out what those exceptions are"

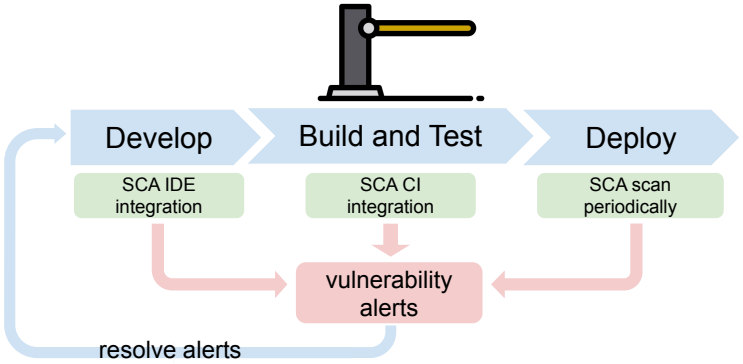


Using Multiple Tools

"Integration [of different SCA tools] is near impossible"

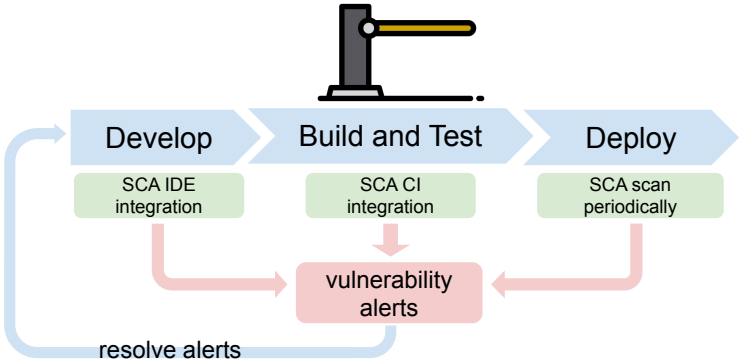
What are the challenges when deploying SCA tools?

SCA in CI/CD pipelines (pull request, code commits)



What are the challenges when deploying SCA tools?

SCA in CI/CD pipelines (pull request, code commits)

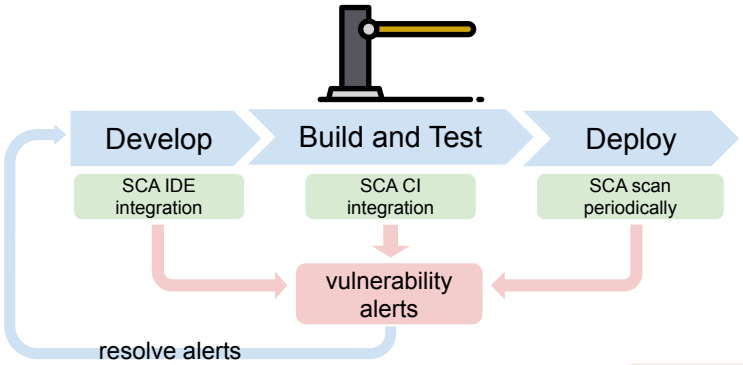


Failed Builds

"You get a temporary implicit block, usually not for super long, but enough that, you know, for every developer that's kind of annoying"

What are the challenges when deploying SCA tools?

SCA in CI/CD pipelines (pull request, code commits)



Failed Builds

"You get a temporary implicit block, usually not for super long, but enough that, you know, for every developer that's kind of annoying"

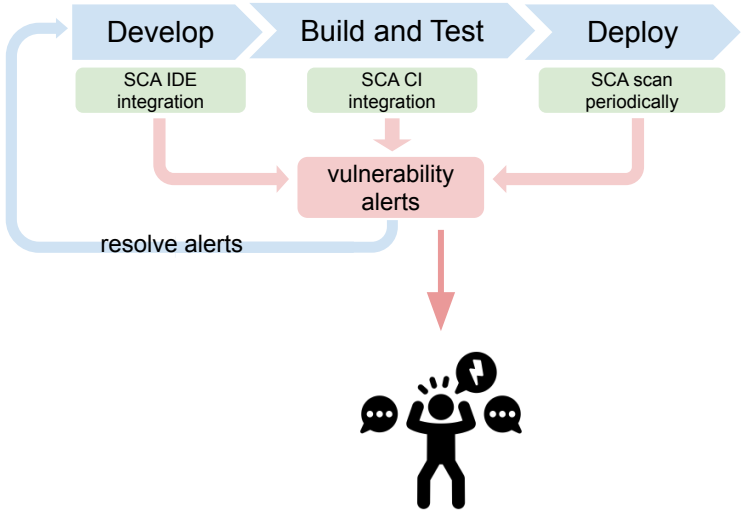
Halting Pipelines

"Previously, we had it set up with a custom action that like, when you push the code, it would do the scanning. Now we have like scheduled it. It's going to run every week automatically once to scan everything. We don't have it on each push anymore [. . .] It doesn't become a blocker"

What are the challenges when acting on SCA results?

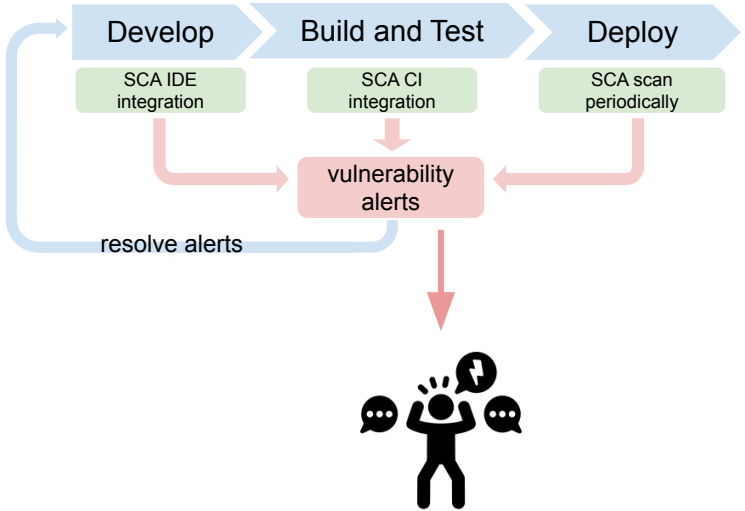
What are the challenges when acting on SCA results?

Interpreting results for vulnerability impact



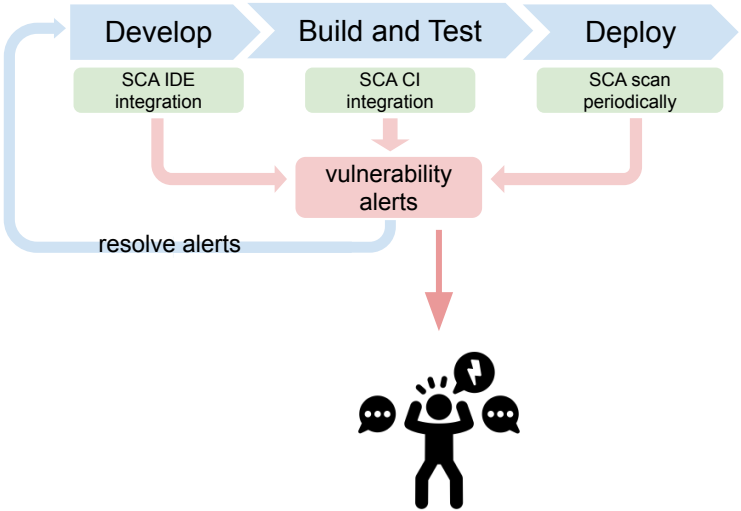
What are the challenges when acting on SCA results?

Interpreting results for vulnerability impact



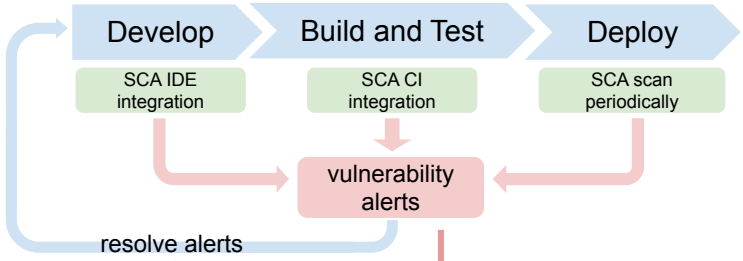
What are the challenges when acting on SCA results?

Interpreting results for vulnerability impact

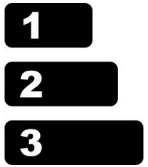


What are the challenges when acting on SCA results?

Interpreting results for vulnerability impact



"I really want to verify because if, when I'm talking to lawyers, I want to be able to explain like, this decision was made and this is why."



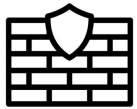
Prioritization

Severity Metrics

Time Effort

Impact

Additional Context for Alerts



Reachability

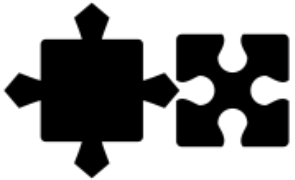
Exploitability

What are the challenges when acting on SCA results?

Fixing vulnerabilities

What are the challenges when acting on SCA results?

Fixing vulnerabilities

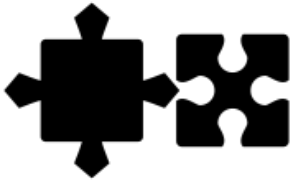


Version Compatibility Issues

“You would introduce a breaking change if you were to up the version.”

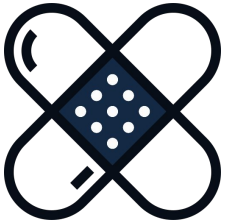
What are the challenges when acting on SCA results?

Fixing vulnerabilities



Version Compatibility Issues

"You would introduce a breaking change if you were to up the version."



Patch Additional Effort

"We forked it and we took out the vulnerable piece"

What are the challenges when acting on SCA results?

Not fixing vulnerabilities

What are the challenges when acting on SCA results?

Not fixing vulnerabilities

"I do think that many SCA findings do not present an actual risk to an application"

Engineer decides there is no impact

What are the challenges when acting on SCA results?

Not fixing vulnerabilities

"I do think that many SCA findings do not present an actual risk to an application"

Engineer decides there is no impact

Security risk vs. Business risk

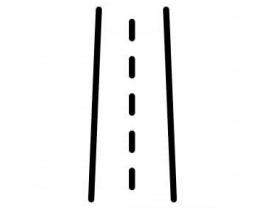
What are the challenges when acting on SCA results?

Not fixing vulnerabilities

"I do think that many SCA findings do not present an actual risk to an application"

Engineer decides there is no impact

Security risk vs. Business risk



No alternative available

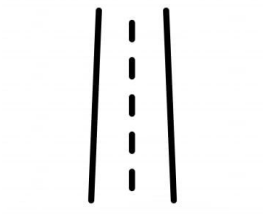
What are the challenges when acting on SCA results?

Not fixing vulnerabilities

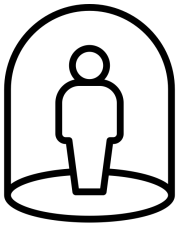
"I do think that many SCA findings do not present an actual risk to an application"

Engineer decides there is no impact

Security risk vs. Business risk



No alternative available

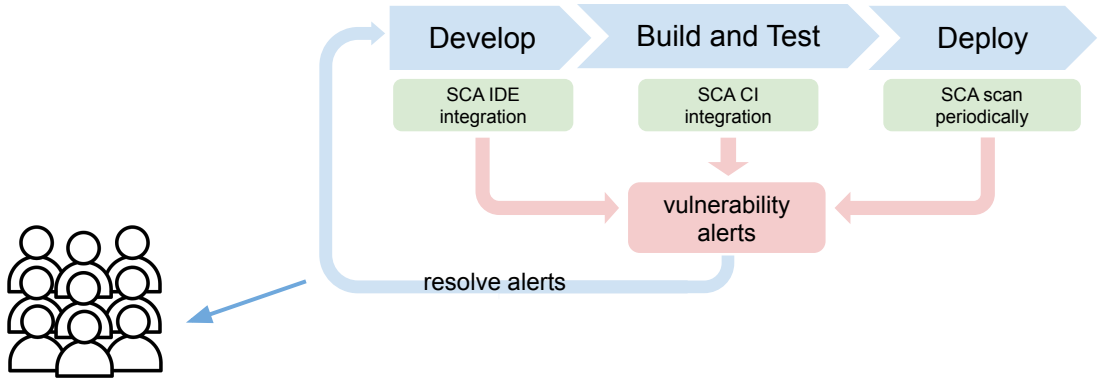


Remove network access

"The risk of that can be negated if you basically just make sure that it doesn't have a connection to the internet"

What are the challenges when acting on SCA results?

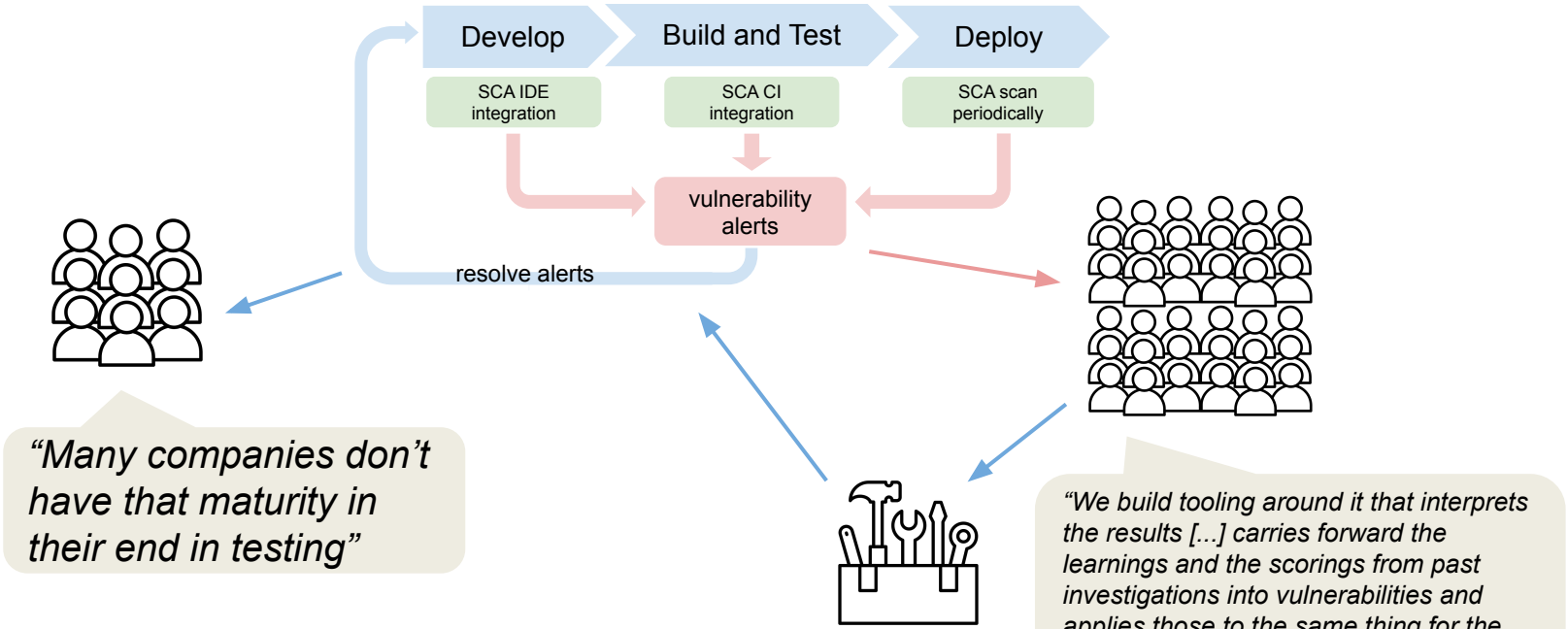
Small vs. Large organizations' approach



"Many companies don't have that maturity in their end in testing"

What are the challenges when acting on SCA results?

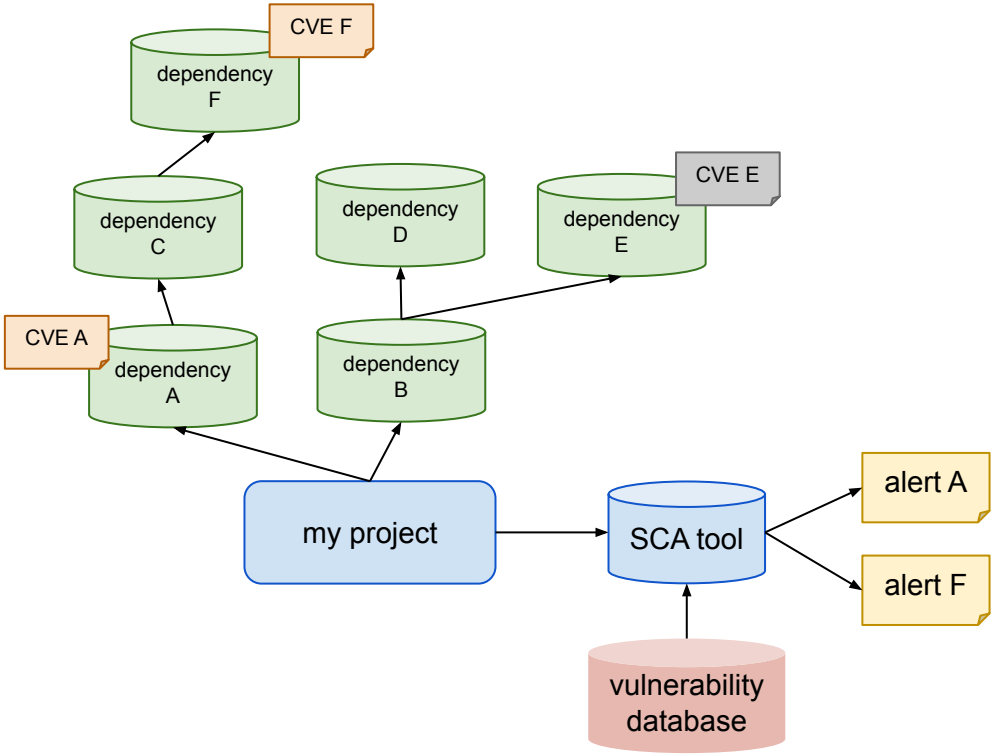
Small vs. Large organizations' approach



How can the SCA process be improved?

Ideal SCA

- ❑ Smooth deployment
- ❑ Identifies components correctly
- ❑ Alerts on vulnerabilities that **matter**
- ❑ Clear fix suggestions



Suggestions for SCA tools

Provide more context

Reachability

Infrastructure

Network

Exploitability

Suggestions for SCA tools

Provide more context

Reachability

Infrastructure

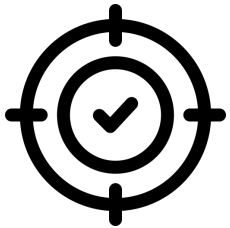
Network

Exploitability

“SCA combined with SAST is very helpful. And if you add your infrastructure configuration context also, it becomes a lot more helpful to prioritize things”

Suggestions for SCA tools

Incorporate user feedback



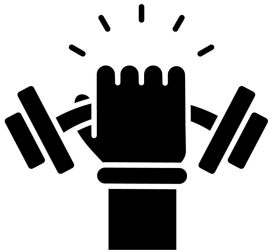
No perfect tool

Learn from user input

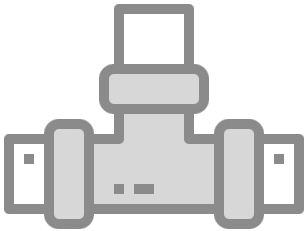
“Having more intelligence to them where you can better train them to say, hey, this isn’t an issue for us in this context. So don’t flag this as an issue next time around.”

Suggestions for SCA users

No tool is perfect



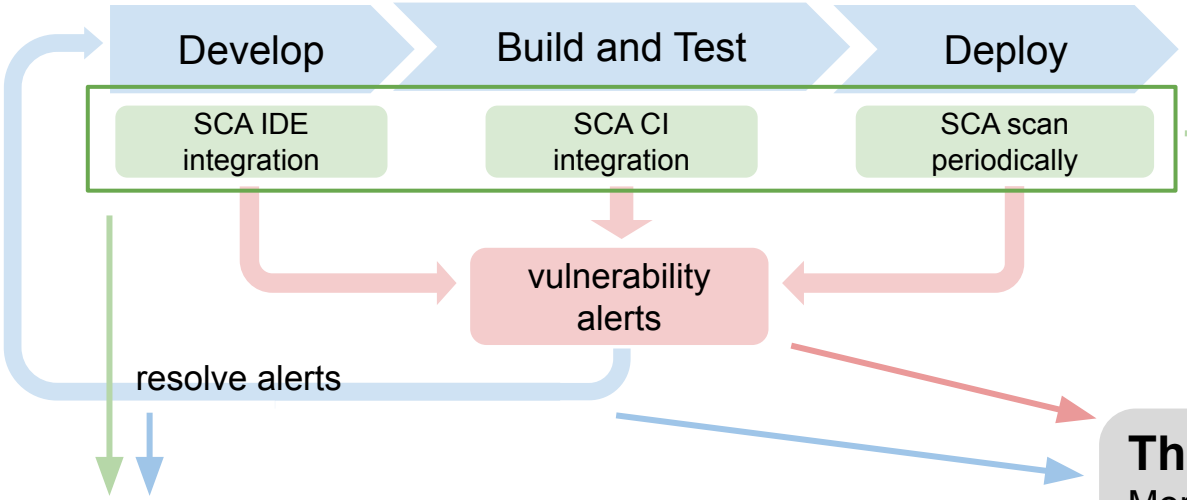
Understand strengths and weaknesses of each tool



Find a tool that works with your pipeline

Work with multiple teams to communicate vulnerability results

Summary



Theme 2
When and how the SCA scan runs in the development cycle matter.

Theme 1
More information is needed to evaluate the risk and impact of the vulnerability alert.

Theme 3
Integration of SCA and communication of the results can generate overhead if there is not enough context present.

Summary

Improve SCA tools with more context

Reachability

Infrastructure

Network

Exploitability

Learn from user input

When integrating SCA

Understand strengths and weaknesses of each tool

Find a tool that works with your pipeline

Work with multiple teams to communicate vulnerability results

Happy to talk more!

I’m interested in full time opportunities in the next 6~12 months

Other research

- UntrustIDE: Exploiting Vulnerabilities in VS Code Extensions
- Software Bills of Materials Are Required. Are We There Yet?
- VFCFinder: Seamlessly Pairing Security Advisories and Patches

https://elizabethtlin.com/