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

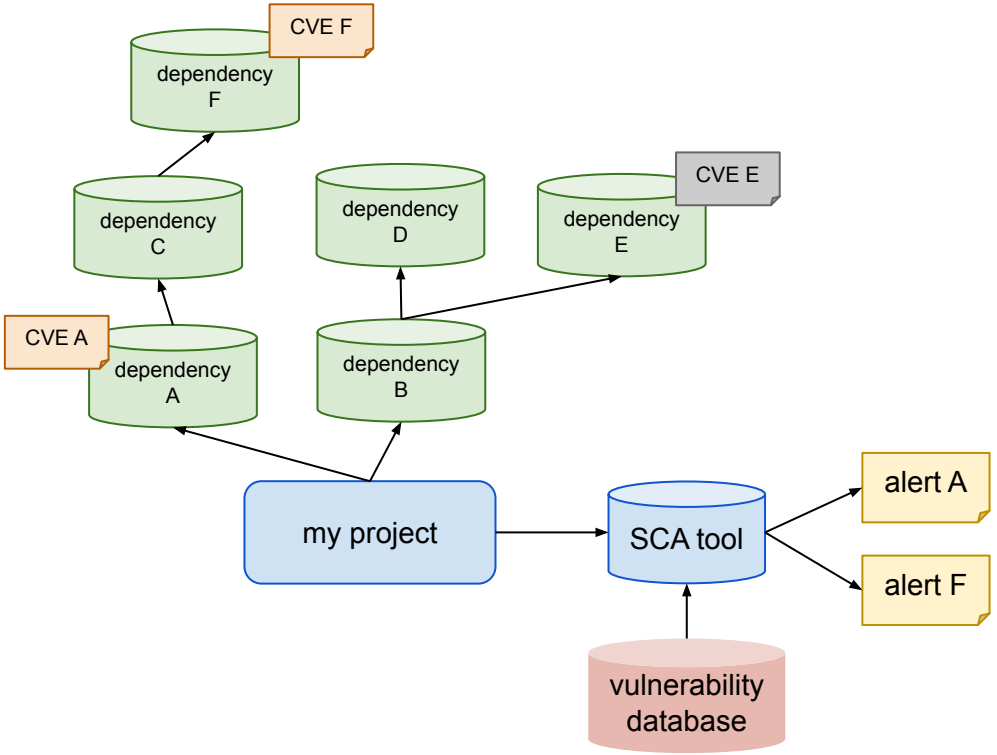
Elizabeth Lin, Sparsha Gowda,
William Enck, Dominik Wermke

Usenix Security 2025

Managing vulnerabilities in open source libraries and components is an important software supply chain task.

Ideal Software Composition Analysis (SCA)

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



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?

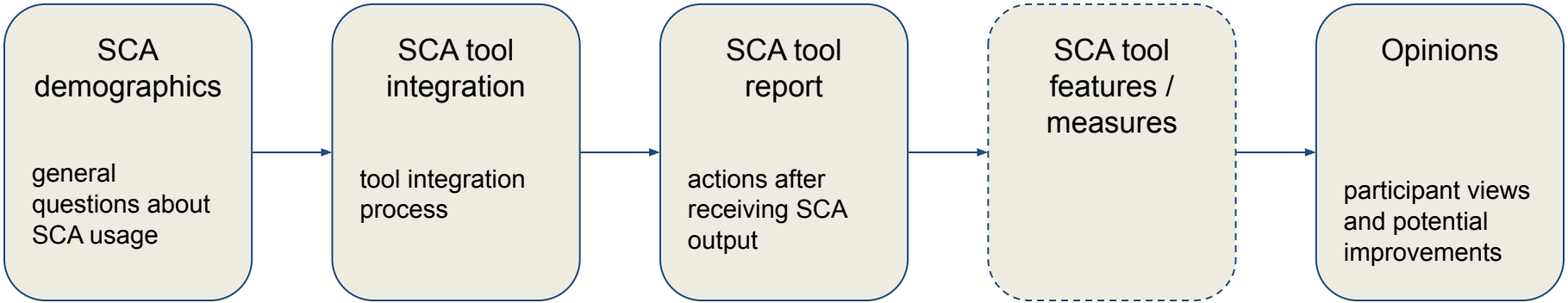
RQ2: What are the challenges when deploying SCA tools?

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

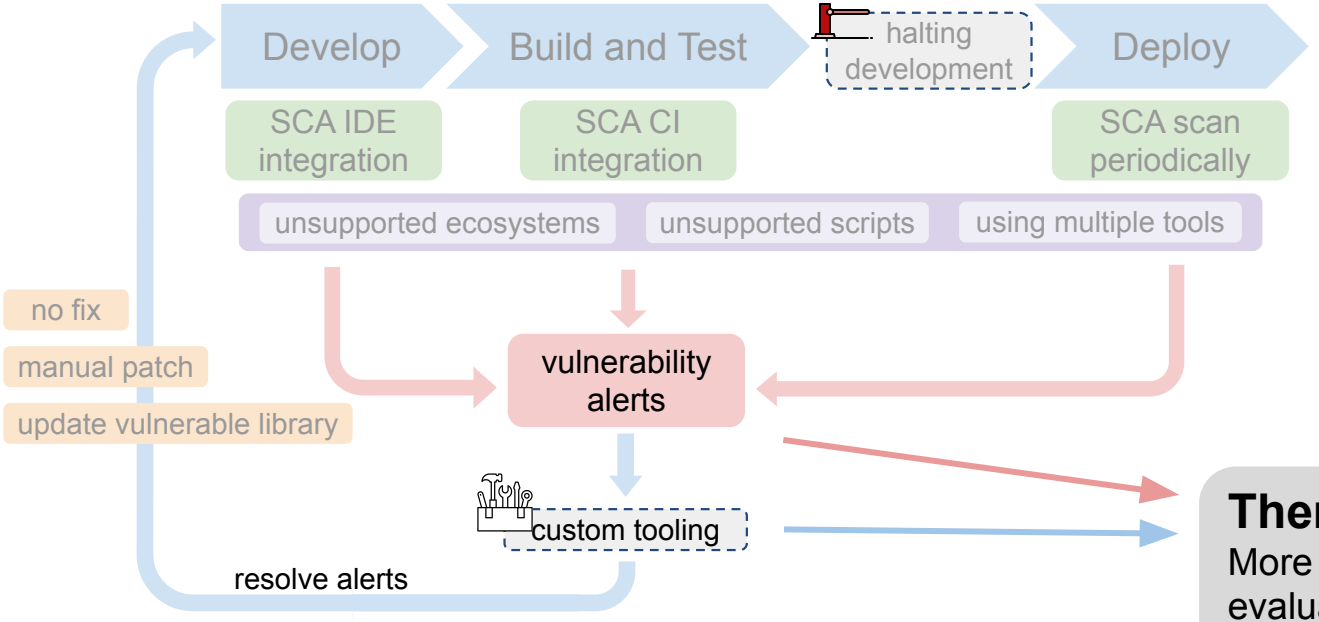
RQ4: How can the SCA process be improved?

User Study

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



Main Finding: Context Matters



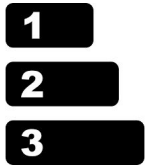
Theme 1

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

Theme 1

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

"I will look at the findings from the SCA tool and triage them and determine which ones need to be tickets that would then go to the engineering team for remediation."

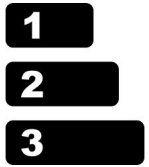


Prioritization

Theme 1

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

"I will look at the findings from the SCA tool and triage them and determine which ones need to be tickets that would then go to the engineering team for remediation."



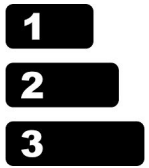
Prioritization

Severity Metrics

Theme 1

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

"I will look at the findings from the SCA tool and triage them and determine which ones need to be tickets that would then go to the engineering team for remediation."



Prioritization

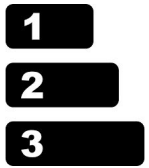
Severity Metrics

Time Effort

Theme 1

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

"I will look at the findings from the SCA tool and triage them and determine which ones need to be tickets that would then go to the engineering team for remediation."



Prioritization

Severity Metrics

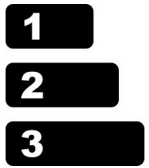
Time Effort

Impact

Theme 1

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

"I will look at the findings from the SCA tool and triage them and determine which ones need to be tickets that would then go to the engineering team for remediation."



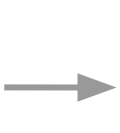
Prioritization

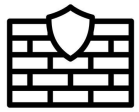
Severity Metrics

Time Effort

Impact

Additional Context for Alerts

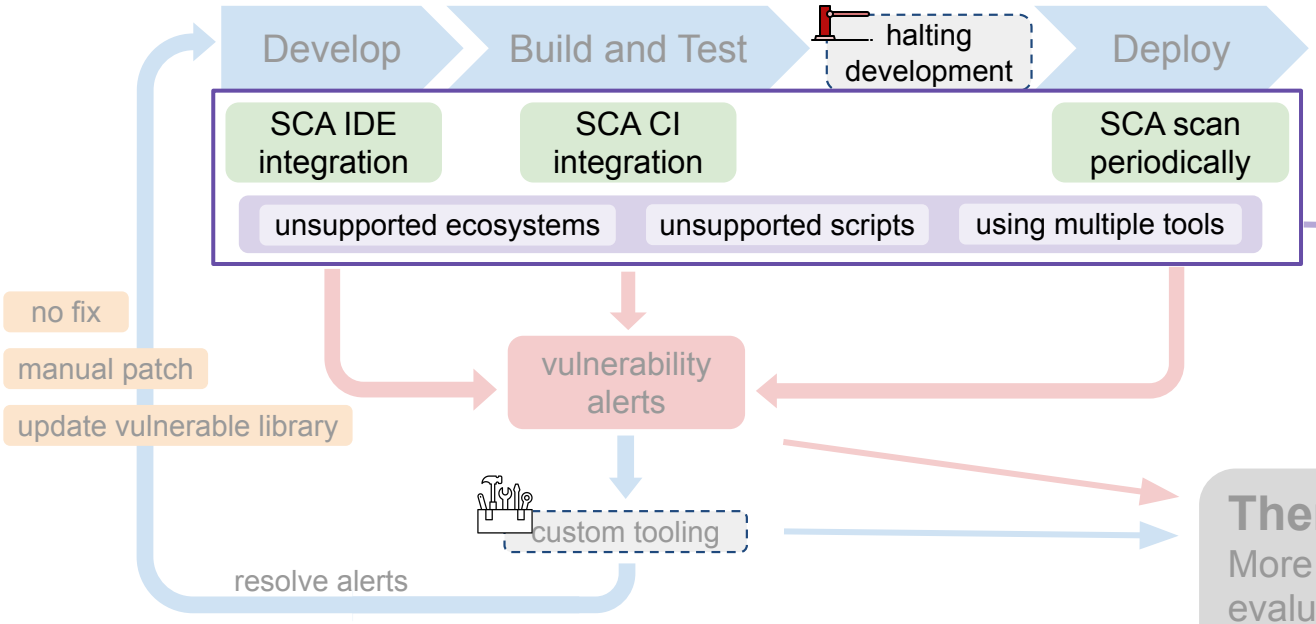




Reachability

Exploitability

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 2

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

Legacy Languages
Unsupported Scripts

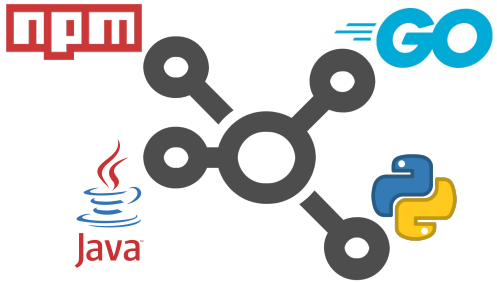
“We need to go and either pre-process things ourselves. We need to work with the supplier to add support for new file formats”

Theme 2

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

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

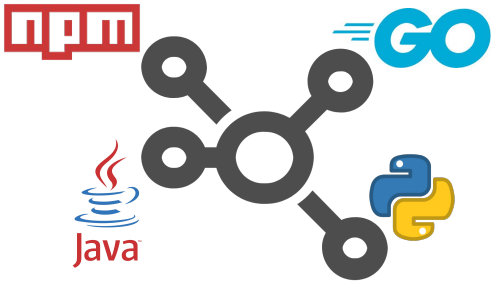
"All the package managers are different. So you have to have exceptions for each one and you have to figure out what those exceptions are"

Theme 2

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

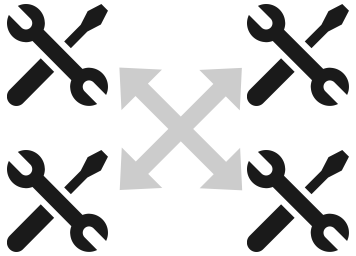
Legacy Languages
Unsupported Scripts

"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"

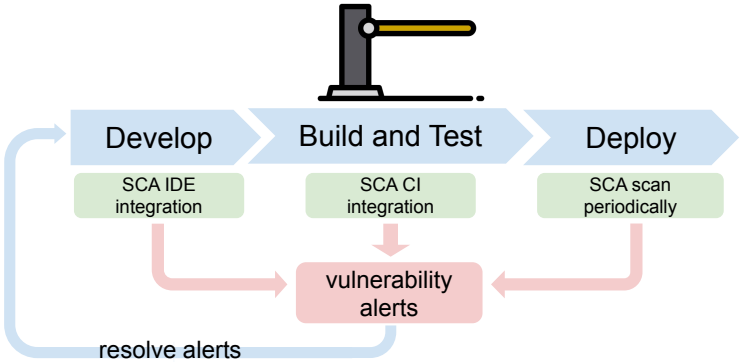


Using Multiple Tools

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

Theme 2

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

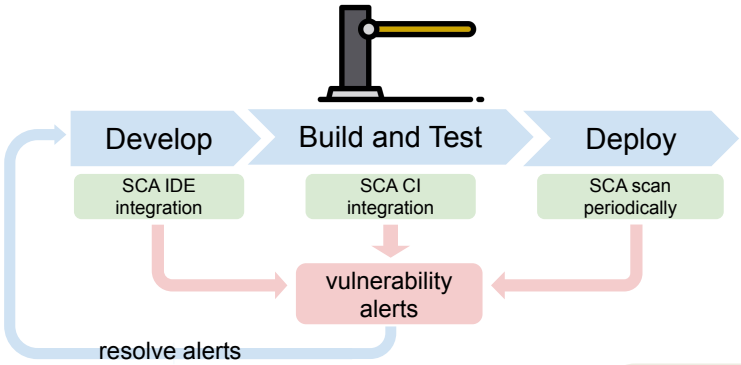


Failed Builds

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

Theme 2

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



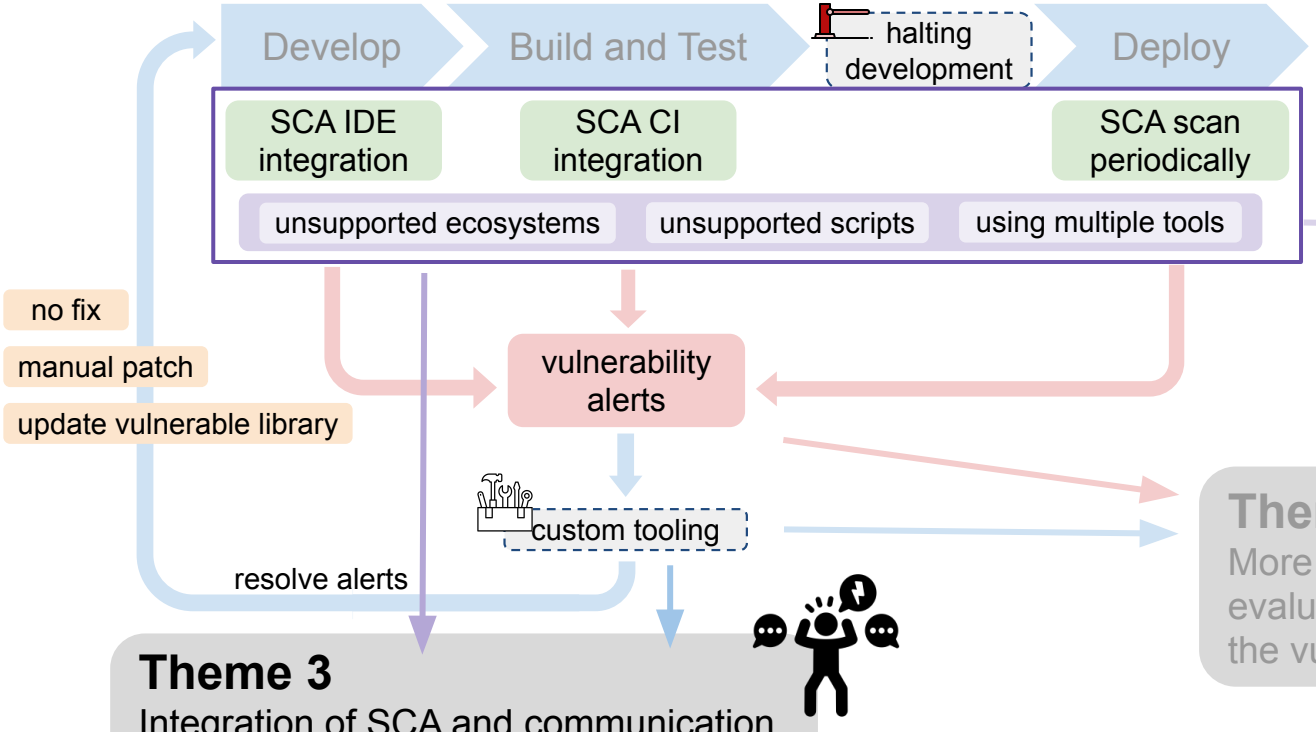
Failed Builds

"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"

Main Finding: Context Matters



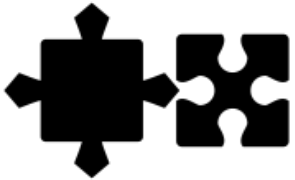
Theme 2
When and how the SCA scan runs in the development cycle matter.

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.

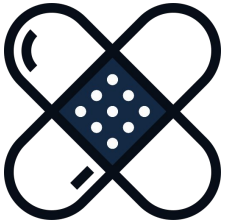
Theme 3

Integration of SCA and communication of the results can generate overhead



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"

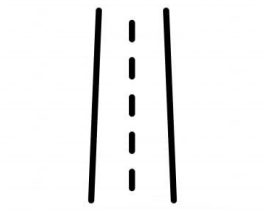
Theme 3

Integration of SCA and communication of the results can generate overhead

"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

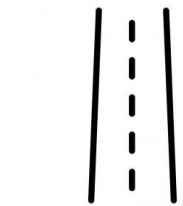
Theme 3

Integration of SCA and communication of the results can generate overhead

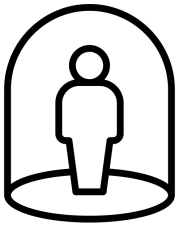
"I do think that many SCA findings do not present an actual risk to an application"

Engineer decides there is no impact

Security risk vs. Business risk



No alternative available

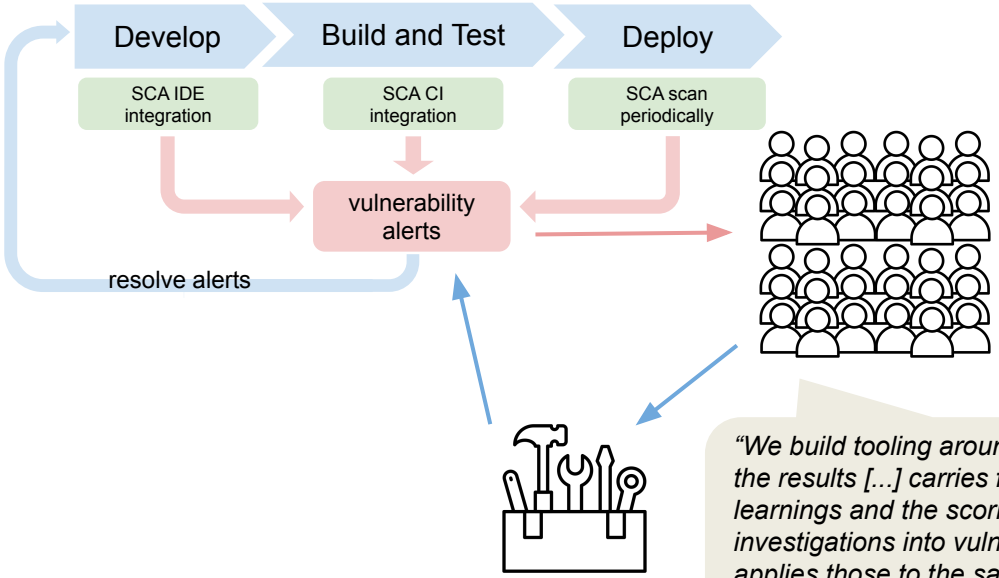


Remove network access

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

Theme 3

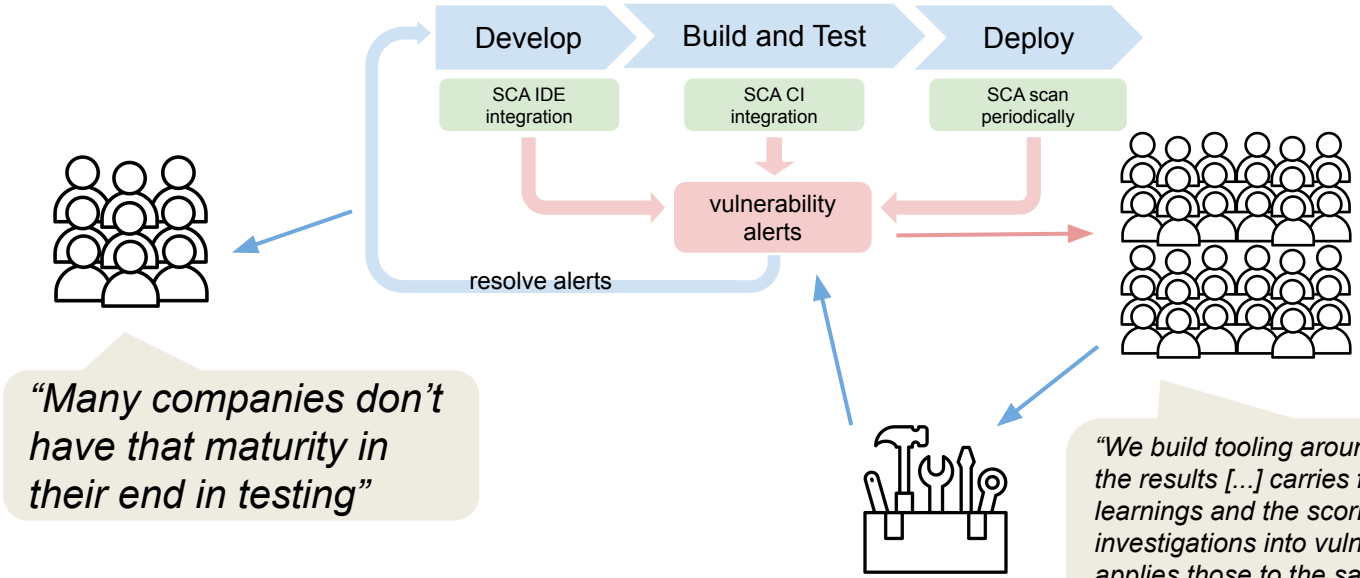
Integration of SCA and communication of the results can generate overhead



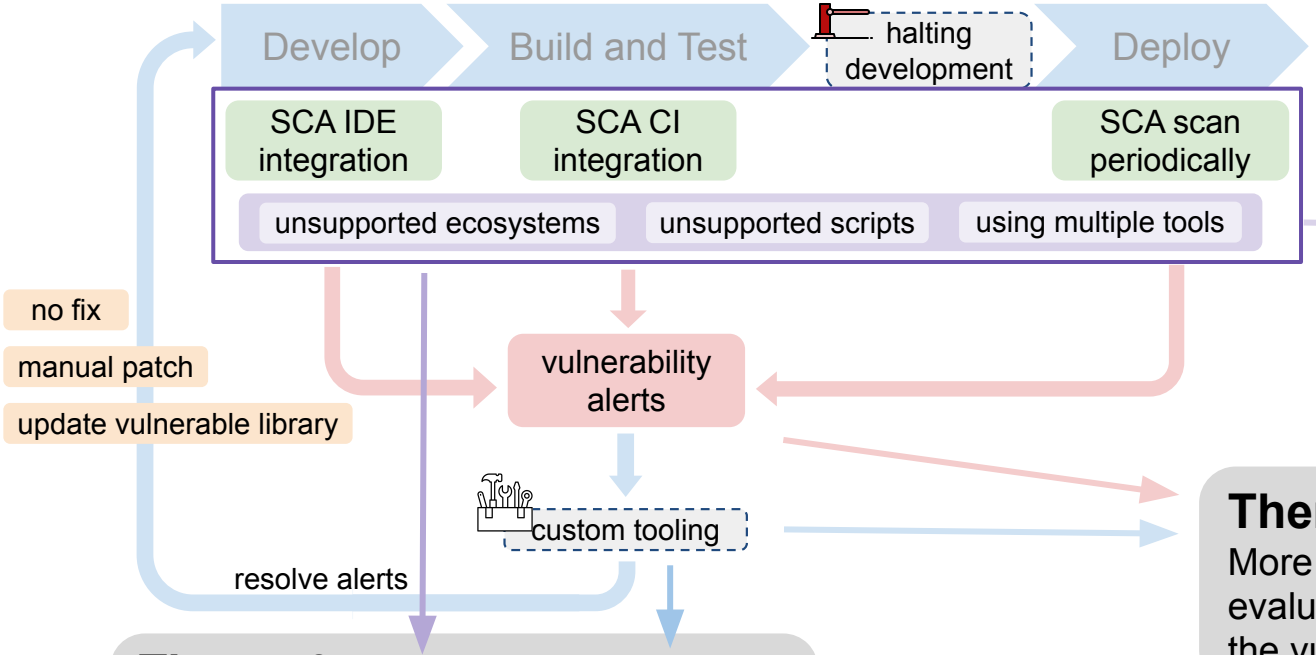
"We build tooling around it that interprets the results [...] carries forward the learnings and the scorings from past investigations into vulnerabilities and applies those to the same thing for the same code base for later versions of it"

Theme 3

Integration of SCA and communication of the results can generate overhead



Main Finding: Context Matters



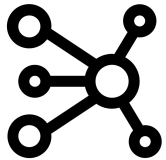
Theme 2
When and how the SCA scan runs in the development cycle matter.

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.

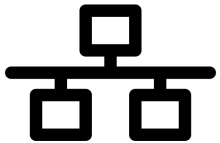
Summary

Improve SCA tools with more context



Reachability

Infrastructure

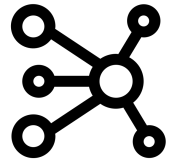


Network Configurations

Exploitability

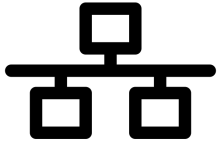
Summary

Improve SCA tools with more context



Reachability

Infrastructure



Network Configurations

Exploitability

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

Context Matters:

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

Elizabeth Lin,
Sparsha Gowda,
William Enck,
Dominik Wermke

Full paper

Blog post