[arnica] OWASP

The Carrot vs. The Stick: Making a Positive Impact on the Security + Developer Relationship

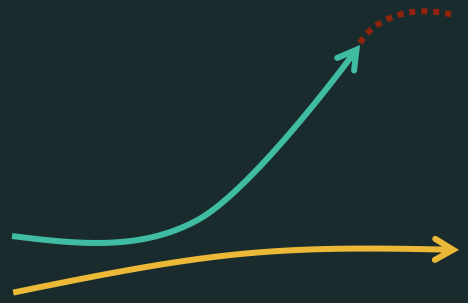
Nir Valtman
Co-Founder & CEO

Same World, Different Perceptions

Devs Need

Fast Development & Delivery

Agile & Iterative Changes



Security Interpret

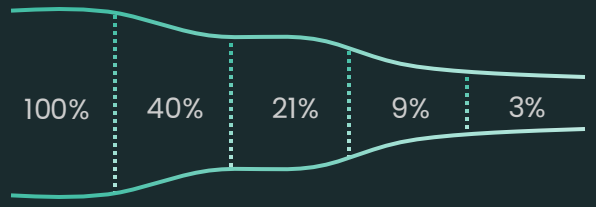
Risks in Production

More Reviews, More Friction

Security Need

Full Risk Visibility & Prioritization

Govern & Enforce Secure Delivery



Devs Interpret

Noise & Alert Fatigue

Slow Software Delivery

[arnica]

AppSec Is Misaligned With Modern SDLC

Low Dev Adoption

Opt-in functionality: ~22% of developers adopt a security IDE plugin

Late Feedback

Feedback is provided on pull/merge requests, after the feature is written

Ownership Gap

82% of all security risks were authored by devs no longer in the company

arnica

HOW TO SOLVE ADOPTION & LATE FEEDBACK

Private, Blameless & Shameless Feedback via IM

Trigger

Notify developer when a code risk is detected on `git push`, finding changes, or SLA

Condition

Business importance, severity, fixability, exploitability, etc.

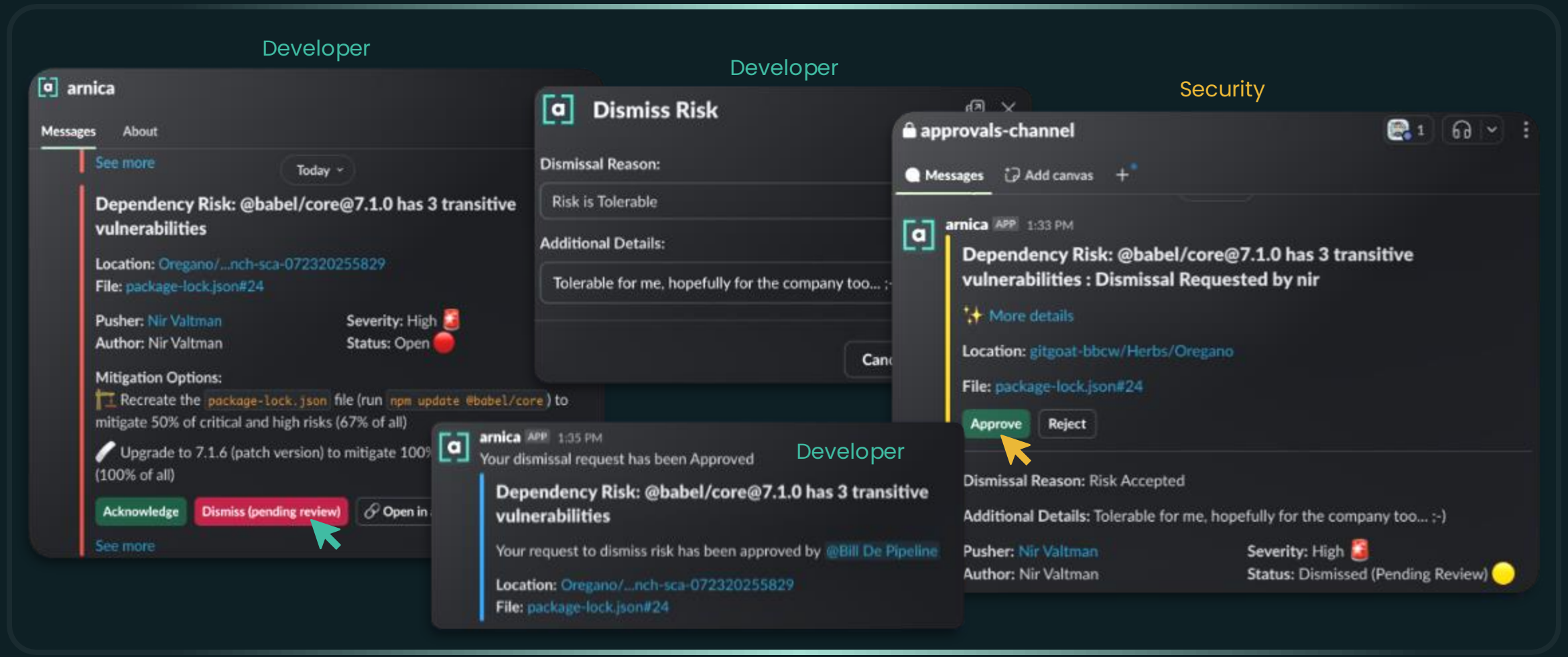
Action

Enforce fix, suggest fix alternatives, or generate AI code fixes

[arnica]

HOW TO SOLVE ADOPTION & LATE FEEDBACK

Dismiss Risks Before Pull Requests, In Feature Branches



arnica

Merged **Pull request from feature-branch-sca-071720251634-fix #188**

billdp-gg merged 1 commit into `main` from `feature-branch-sca-0717…` last week

arnica-github-connector bot commented last week

W00t W00t! 😎 - 1 code risk was fixed in this branch

SOLVE OWNERSHIP

Celebrate Remediation

🎉 Kudos to: @nir-valtman

SCA (Software Composition Analysis)

Severity	Status	Description
High	🟡 In Progress	@babel/core@7.1.0

Loved it? 😍 Follow us or share your experience on LinkedIn or X.

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

Notifications Customize

Unsubscribe

You're receiving notifications because you modified the open/close state.

2 participants

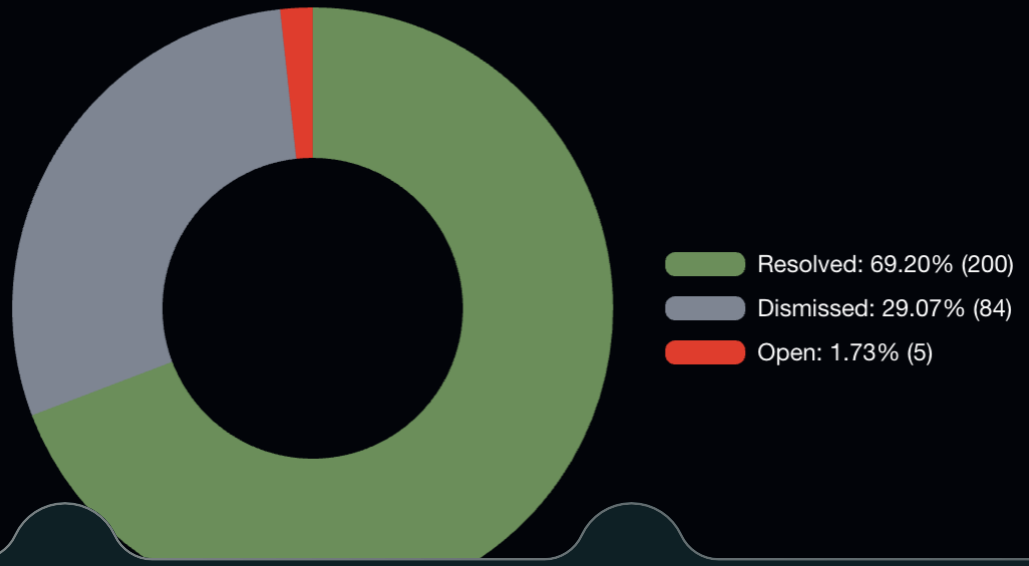
Lock conversation

SOLVE OWNERSHIP

Measure Good Behavior

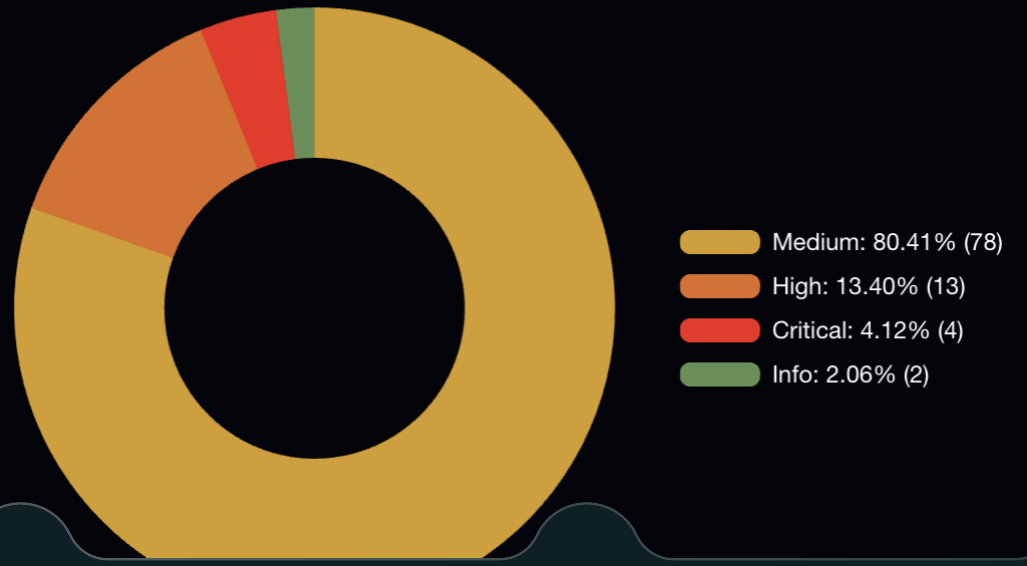
Authored risks ⓘ

In SLA branches



Risks resolved ⓘ

In feature branches



AI Code Fixes?

Find Best Reviewer

Security Champions?

Validate Contribution

Developer Attrition?

Classify Next Best Fit

0 New Risks Policy?

Automate Workflows

[arnica]

Measure The Developer-Native Workflow Impact

78%

Resolved Before
Pull/Merge Request

92%

Never Merged
To Production

[arnica]

Thank You