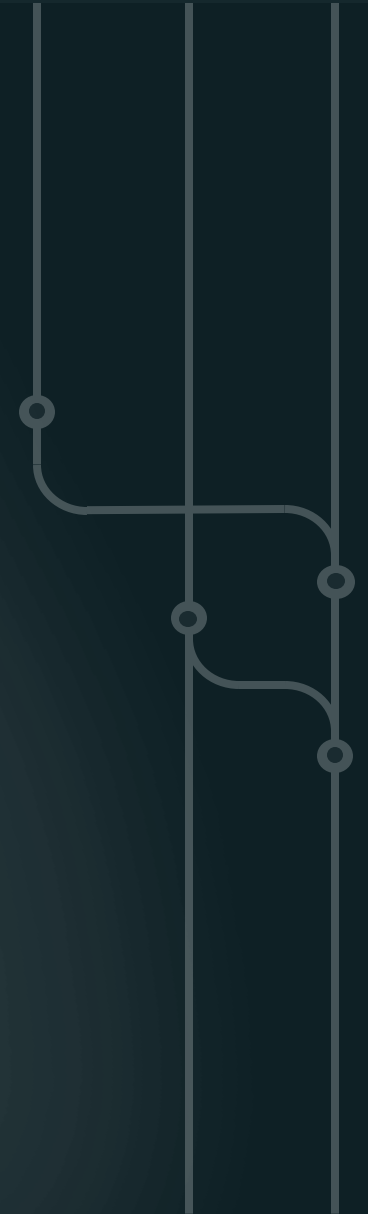


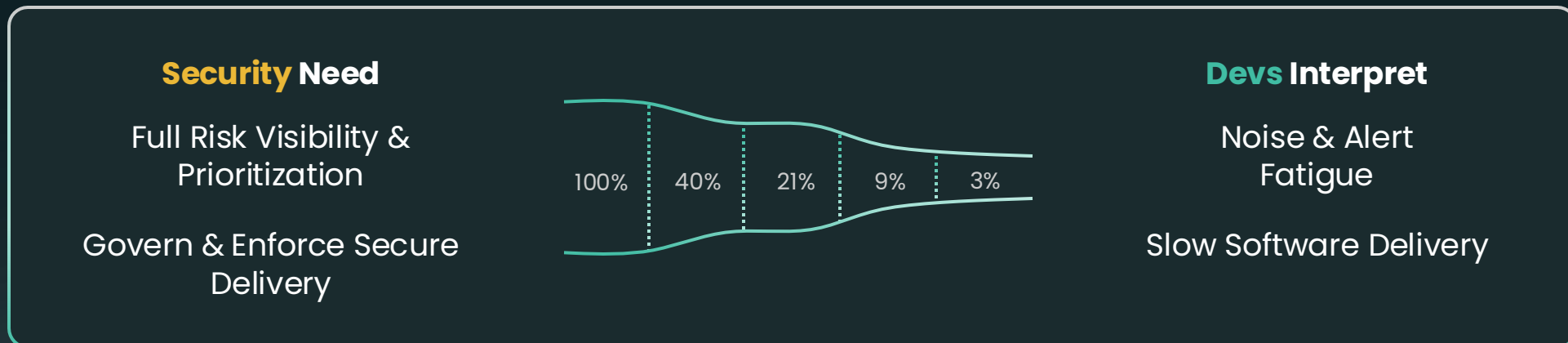
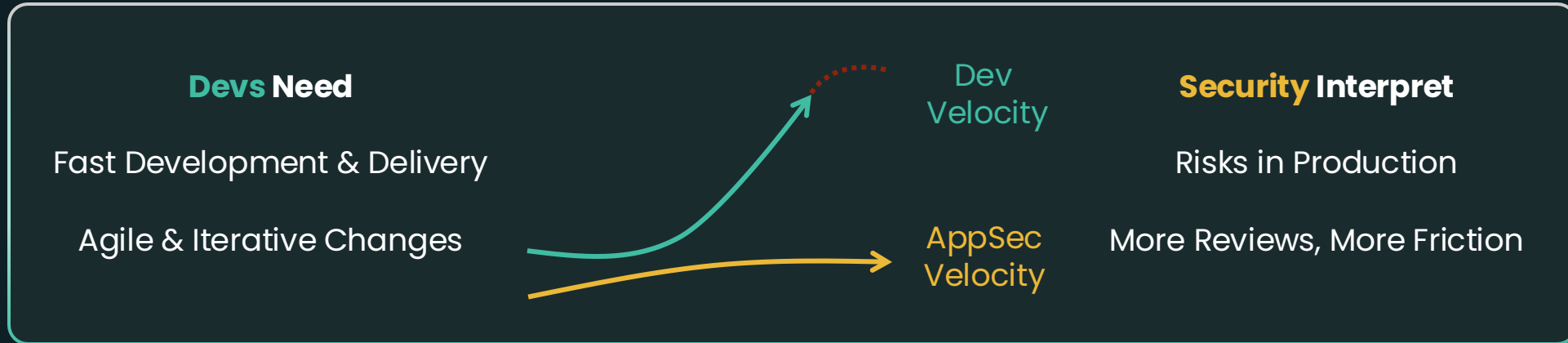
# **The Carrot vs. The Stick: Making a Positive Impact on the Security + Developer Relationship**

---

Nir Valtman  
Co-Founder & CEO



# Same World, Different Perceptions



# 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

# Private, Blameless & Shameless Feedback via IM

## Trigger

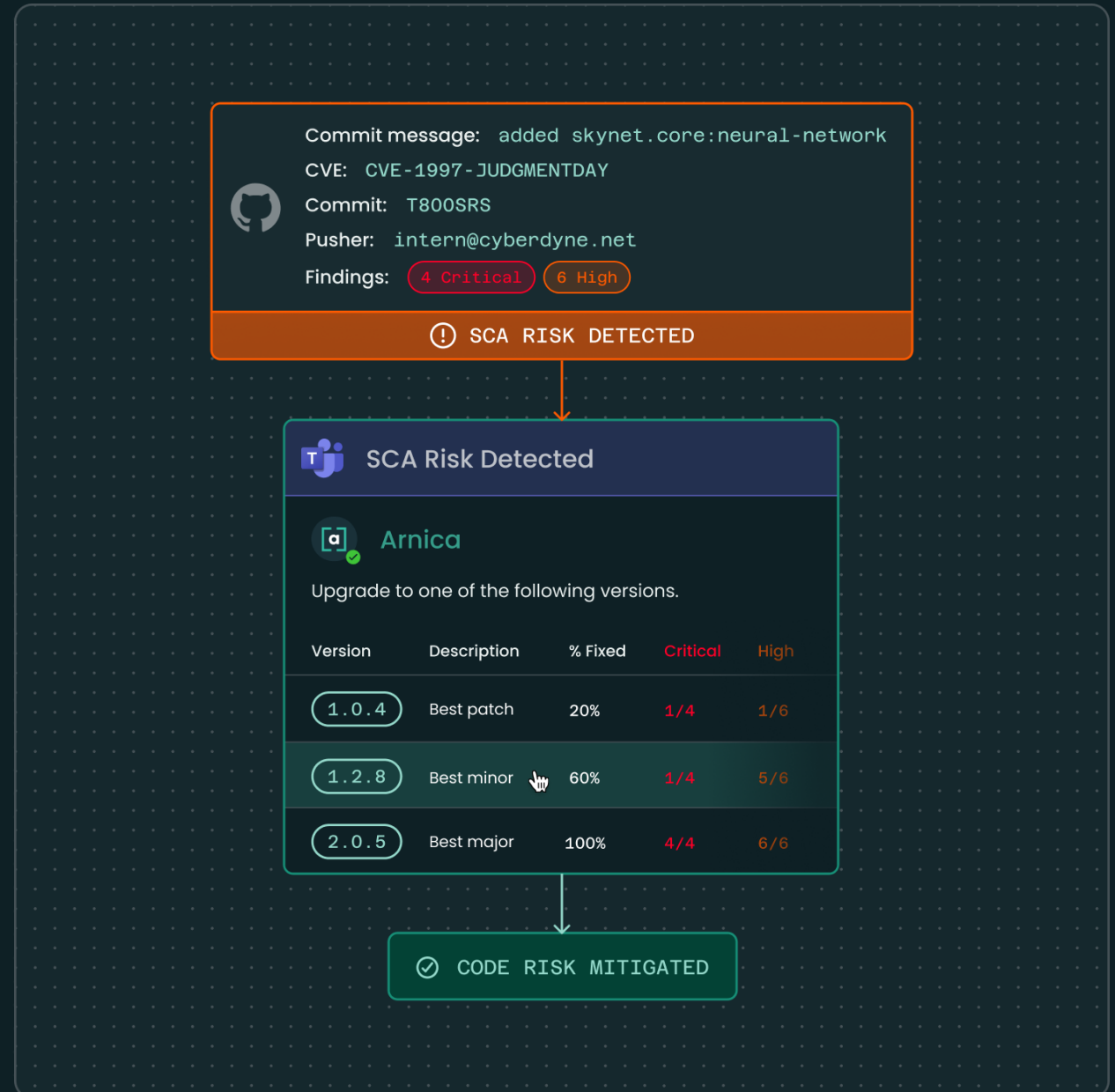
Notify developer when a code risk is detected on `git push`, finding changes, or SLA

## Condition

Business importance, severity, fixability, exploitability, etc.

## Action

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



# Dismiss Risks Before Pull Requests, In Feature Branches

The image illustrates a workflow for handling dependency risks in a development environment using Arnica. It is divided into three main sections: Developer, Developer, and Security.

**Developer (Left):** A chat window for 'arnica' shows a 'Dependency Risk: @babel/core@7.1.0 has 3 transitive vulnerabilities'. The risk is located at 'Oregano/...nch-sca-072320255829' in 'package-lock.json#24'. The pusher is Nir Valtman, and the severity is High. Mitigation options include recreating the package-lock.json file or upgrading to 7.1.6. A red button labeled 'Dismiss (pending review)' is highlighted with a green arrow.

**Developer (Middle):** A 'Dismiss Risk' dialog box is shown. The 'Dismissal Reason' is 'Risk is Tolerable'. The 'Additional Details' are 'Tolerable for me, hopefully for the company too... :-)'. A 'Cancel' button is visible at the bottom.

**Developer (Bottom):** A confirmation message from 'arnica' states: 'Your dismissal request has been Approved'. It repeats the risk details and mentions that the request was approved by '@Bill De Pipeline'.

**Security (Right):** A chat window for 'approvals-channel' shows a message from 'arnica' at 1:33 PM. The message is: 'Dependency Risk: @babel/core@7.1.0 has 3 transitive vulnerabilities : Dismissal Requested by nir'. It includes a 'More details' link, the location, and the file. There are 'Approve' and 'Reject' buttons. A yellow arrow points to the 'Approve' button. Below the buttons, the 'Dismissal Reason' is 'Risk Accepted' and the 'Additional Details' are 'Tolerable for me, hopefully for the company too... :-)'. The pusher is Nir Valtman, and the status is 'Dismissed (Pending Review)' with a yellow circle icon.



arnica-github-connector bot commented [last week](#)

# WOOt WOOt! 🕶️ - 1 code risk was fixed in this branch



👏 Kudos to: [@nir-valtman](#)

## SCA (Software Composition Analysis)

Severity	Status	Description
High	🟡 In Progress	<a href="#">@babel/core@7.1.0</a>

SOLVE OWNERSHIP

Celebrate  
Remediation

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

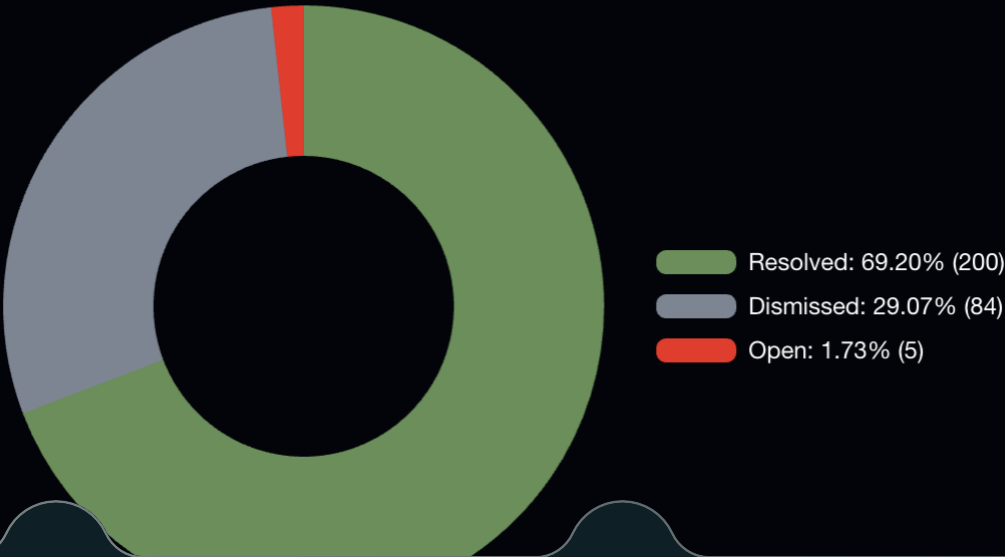


Lock conversation

# Measure Good Behavior

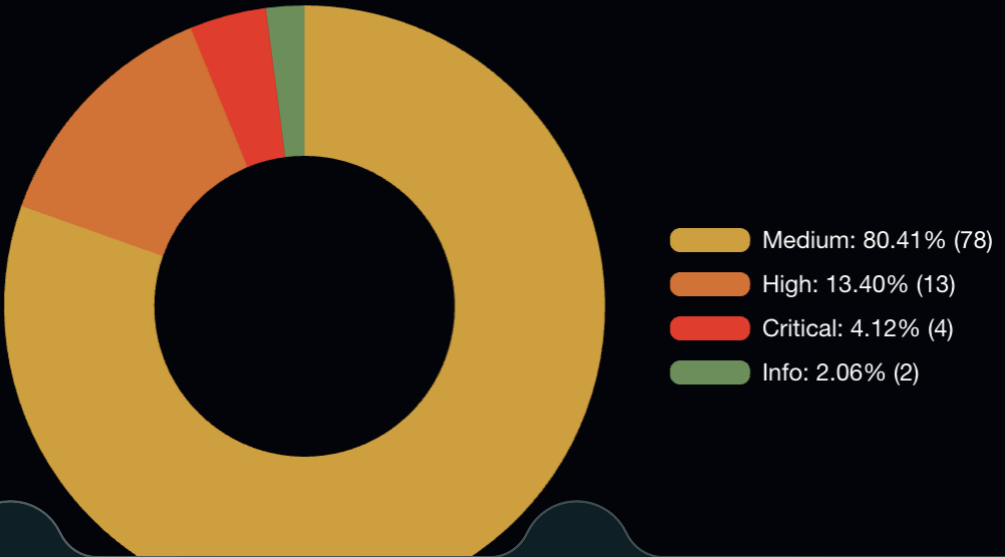
## Authored risks ⓘ

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

# Measure The Developer-Native Workflow Impact



78%

Resolved Before  
Pull/Merge Request



92%

Never Merged  
To Production



[arnica]



Thank You