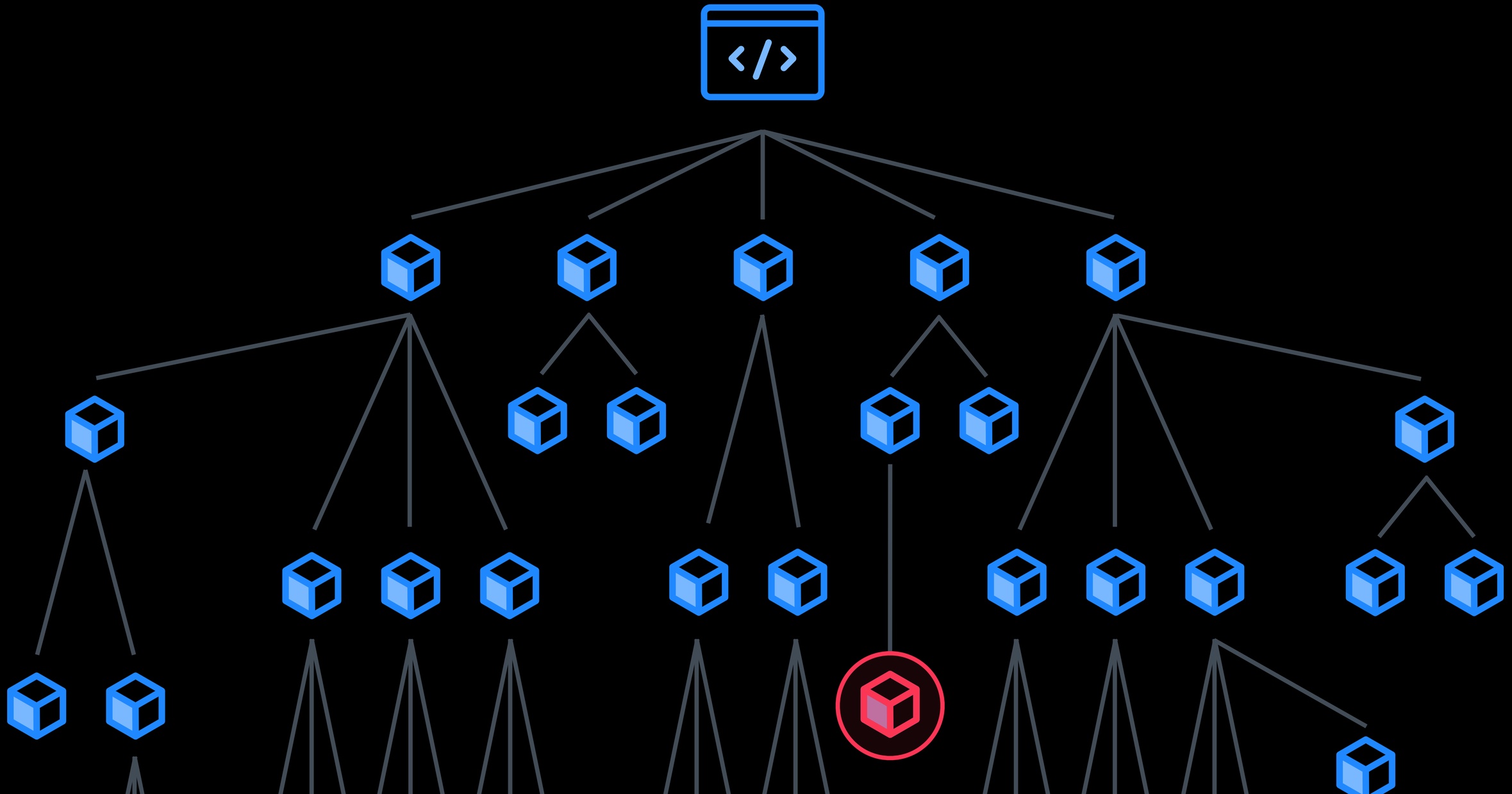
Securing Software from the Supply Side

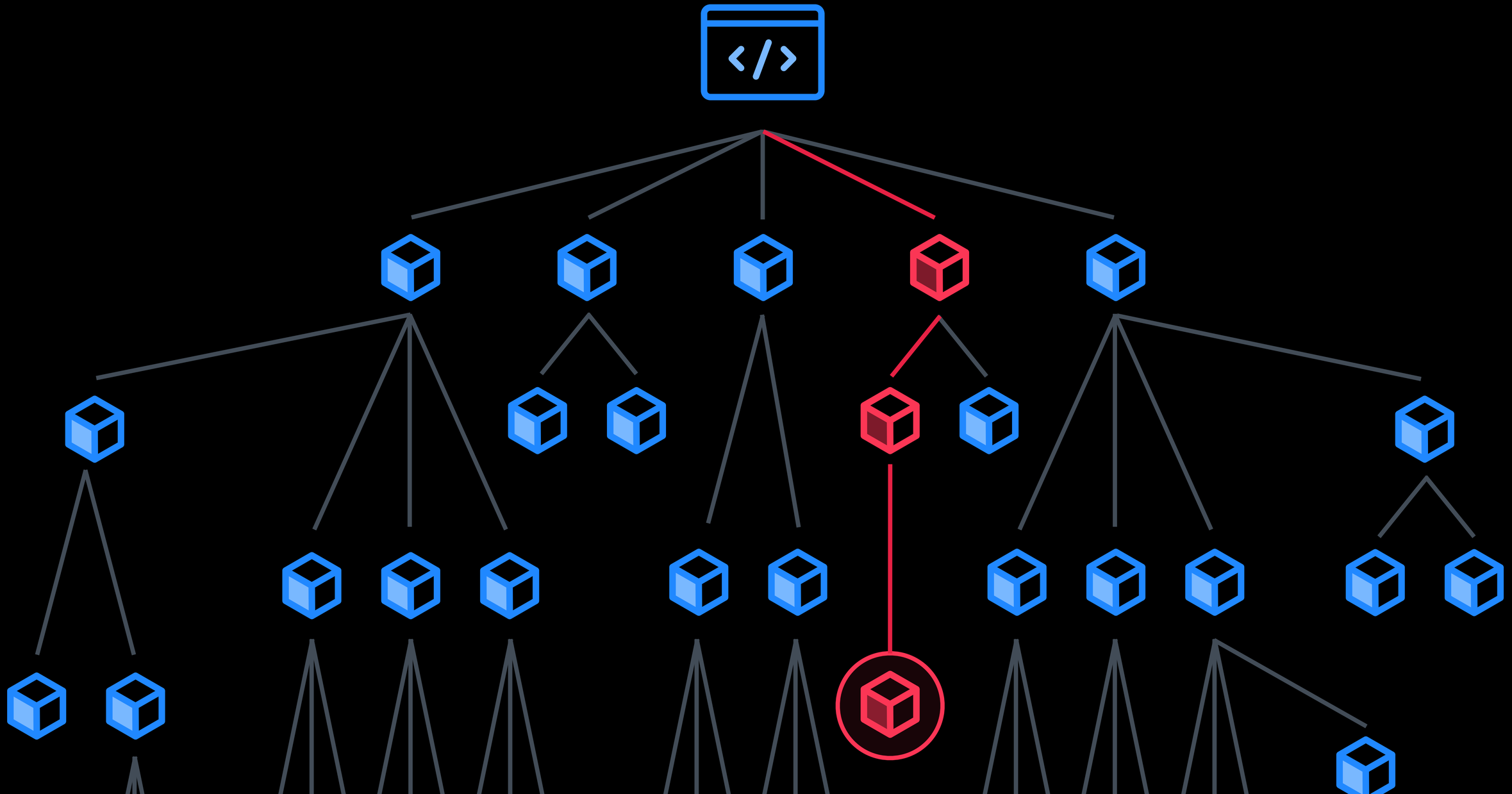
Nickolas Means
Senior Engineering Manager,
Security and Compliance
GitHub

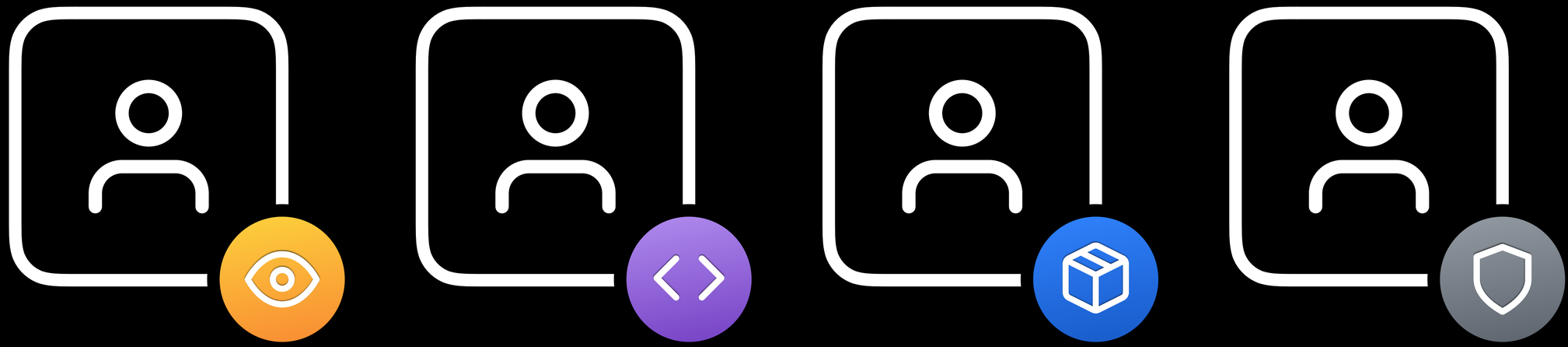
Open Source

99%

Of software projects use open source







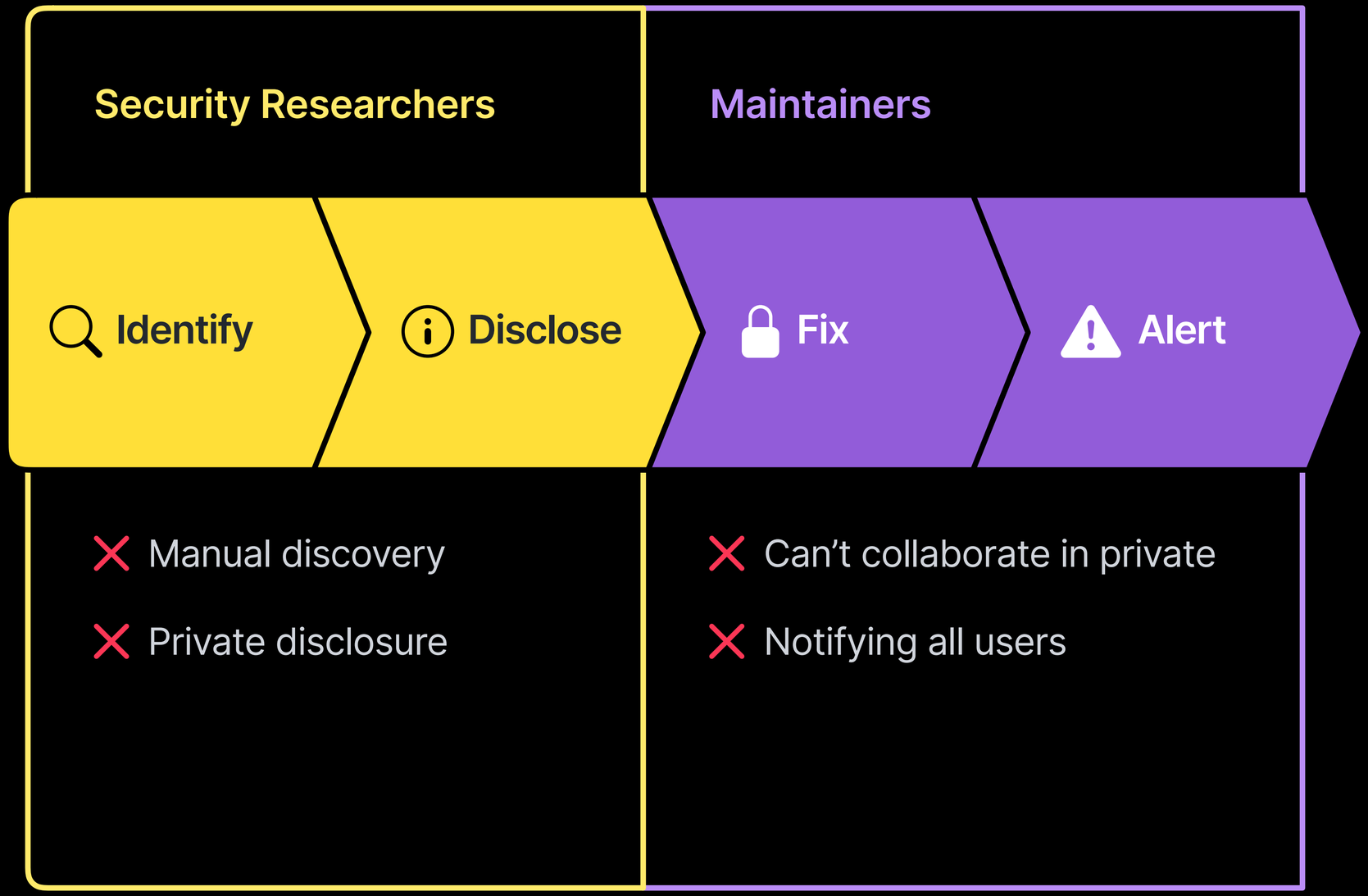
Security Researchers

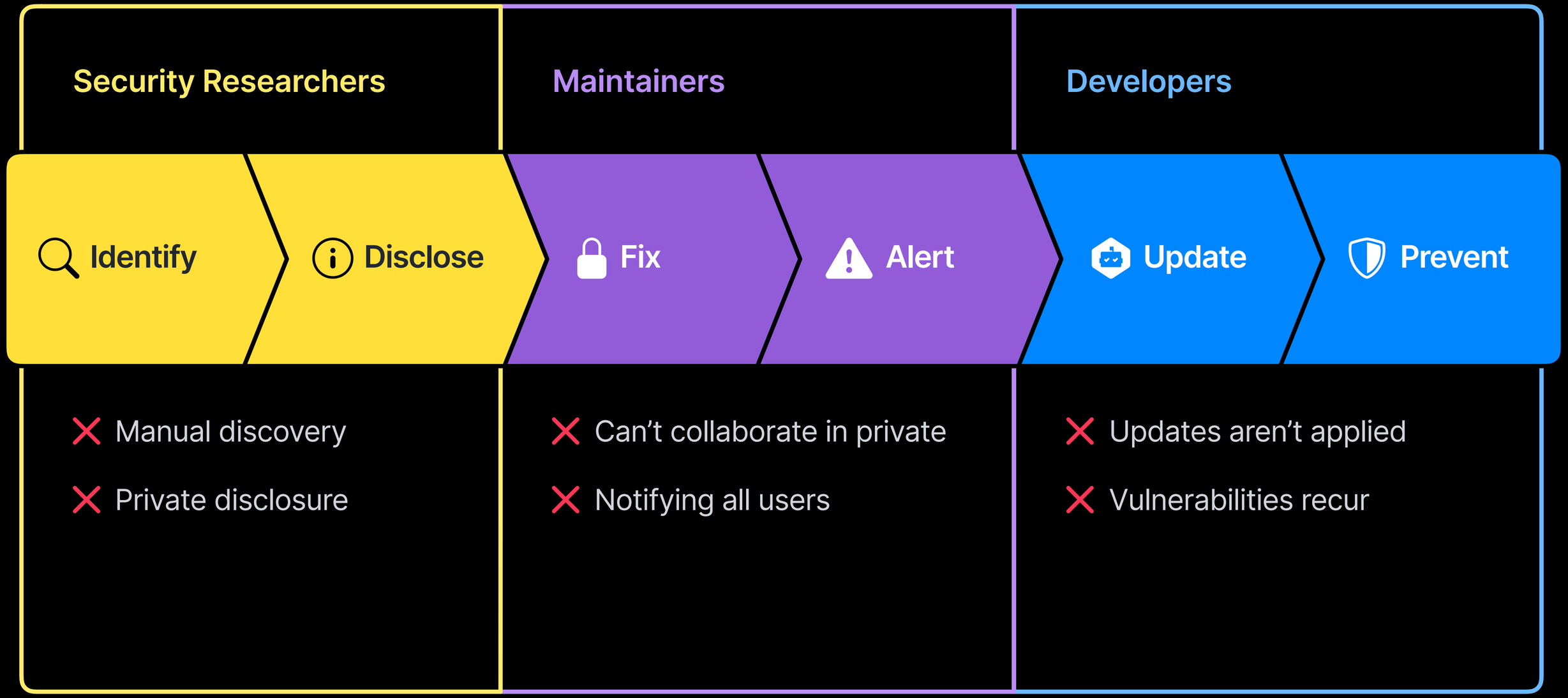
Maintainers

Developers

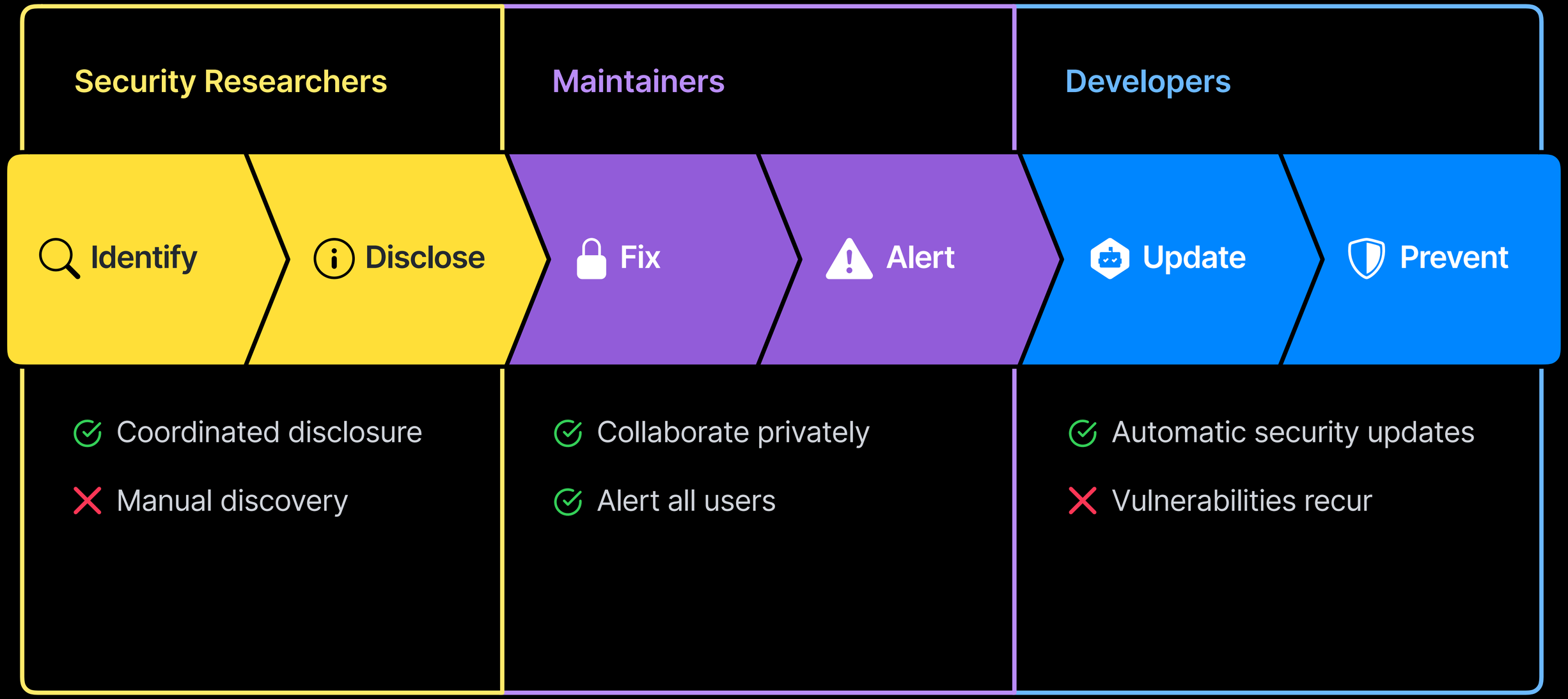
Security Teams

Security Researchers
Identify
Disclose
Manual discovery
Private disclosure


Security Researchers
Maintainers
Identify
Disclose
Fix
Alert
Manual discovery
Private disclosure
Can’t collaborate in private
Notifying all users


Security Researchers
Maintainers
Developers
Identify
Disclose
Fix
Alert
Update
Prevent
Manual discovery
Private disclosure
Can’t collaborate in private
Notifying all users
Updates aren’t applied
Vulnerabilities recur

Demo


Security Researchers
Maintainers
Developers
Identify
Disclose
Fix
Alert
Update
Prevent
Coordinated disclosure
Manual discovery
Collaborate privately
Alert all users
Automatic security updates
Vulnerabilities recur

+ Semmle

github.com/features/security

Securing Software from the Supply Side

Nickolas Means
Senior Engineering Manager,
Security and Compliance
GitHub