ARNICA, FOR SECURITY

Securing the development ecosystem by continuously managing permissions, ensuring least privilege, preventing secrets in code, and detecting anomalous developer behavior.

THE SECURITY CHALLENGE

Security teams at organizations of any size are now faced with addressing a growing security threat to their company's software supply chain – direct attacks on source code and CI/CD pipelines.

To make matters more challenging, they have to address supply chain risk without causing disruption to developers.

OUR APPROACH

Rapid security ROI. Upon integration, immediately identify and mitigate risks like excessive administration/code permissions, introducing new hardcoded secrets, account takeovers, spoofing, or insider developer threats.

We fix what we find. Leverage one-click or automated mitigation for every risk Arnica surfaces. Need a "single pane of glass"? This is free forever.

Security + developer delight. Security that impedes development is doomed. Arnica is built with developer delight in mind. While we aim to not slow developer velocity, we often accelerate it.

By automatically monitoring and managing permissions to least-privilege, Arnica solves an immediate problem that I have and one that I imagine most CISOs are dealing with: complying with audits of permissions in an ongoing and effective way.

Johnathan Jaffe
CISO @ Lemonade

ARNICA CORE PRODUCT VALUE

DEVELOPER ACCESS MANAGEMENT

Automate toward least privilege access, while empowering developers to control their own access.

ANOMALOUS BEHAVIOR DETECTION

Identify anomalous developer and code behavior in pushed commits. Add step up authentication to protect against account takeover.

SECRET DETECTION & MITIGATION

Identify and mitigate hardcoded secrets before they are accessed by anyone else.

SECURE DEVELOPMENT COMPLIANCE

Continuously monitor and report on the security and compliance of your development environment.

Get started!