Supply Chain Attacks on Open Source

What's Happening, What Can We Do Today, and What's Next

Zach Steindler
https://coffeehousecoders.org
USENIX Enigma 2026

Updated and Ongoing Supply Chain Attack Targets CrowdStrike npm Packages

Socket detected multiple compromised CrowdStrike npm packages, continuing the "Shai-Hulud" supply chain attack that has now impacted nearly 500 packages.

 Kush Pandya  Peter van der Zee  Olivia Brown

 Socket Research Team

September 16, 2025 / 9 min read



Research • May 20 • 9 min read

Mini Shai Hulud: Compro @antv npm packages ena CI/CD credential theft

By Microsoft Defender Security Research Team

Research • December 9, 2025 • 12 min read

Shai-Hulud 2.0: Guidance for detecting, investigating, and defending against the supply chain attack

By Microsoft Defender Security Research Team

Security

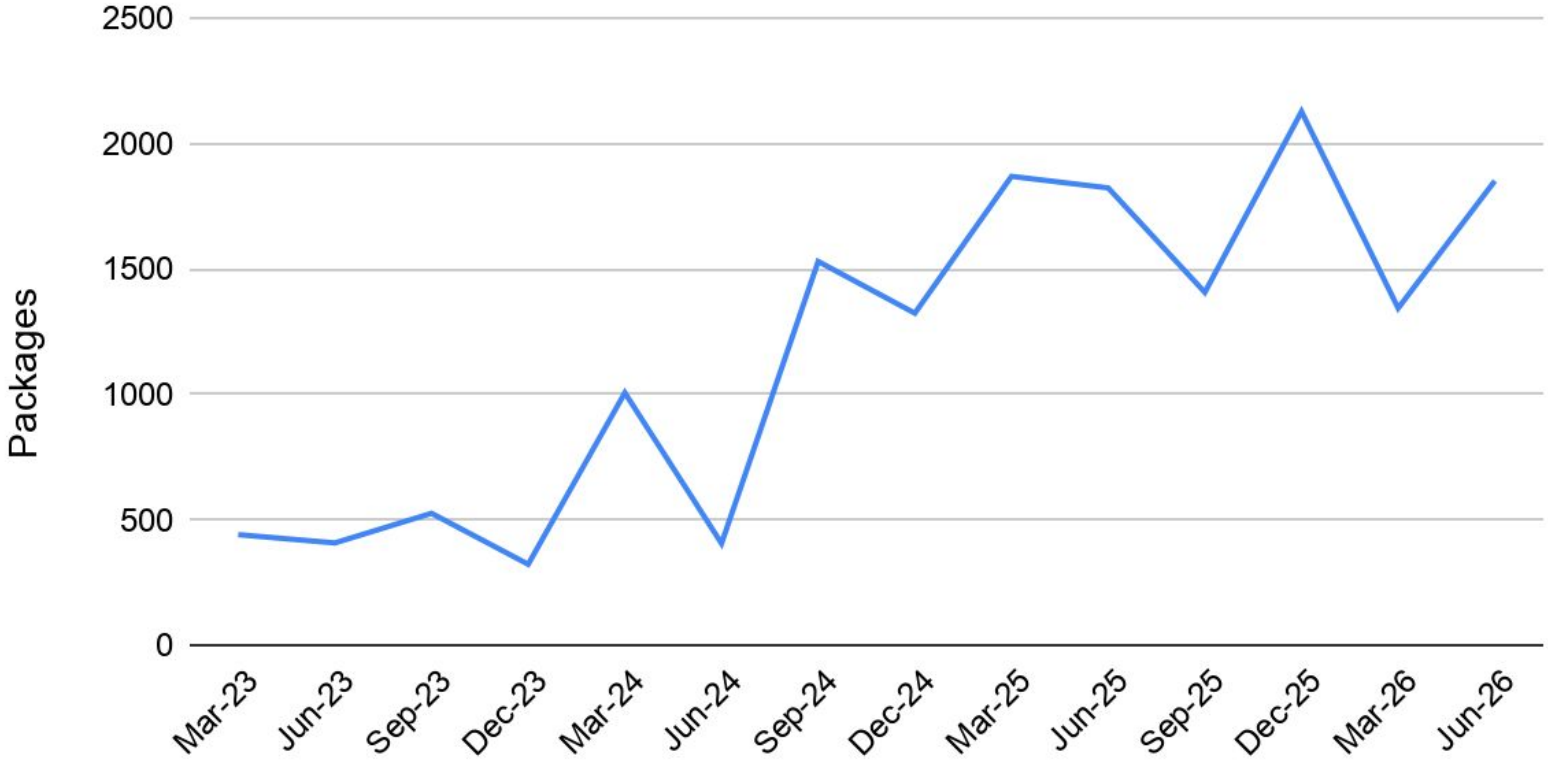
Strengthening supply chain security: Preparing for the next malware campaign

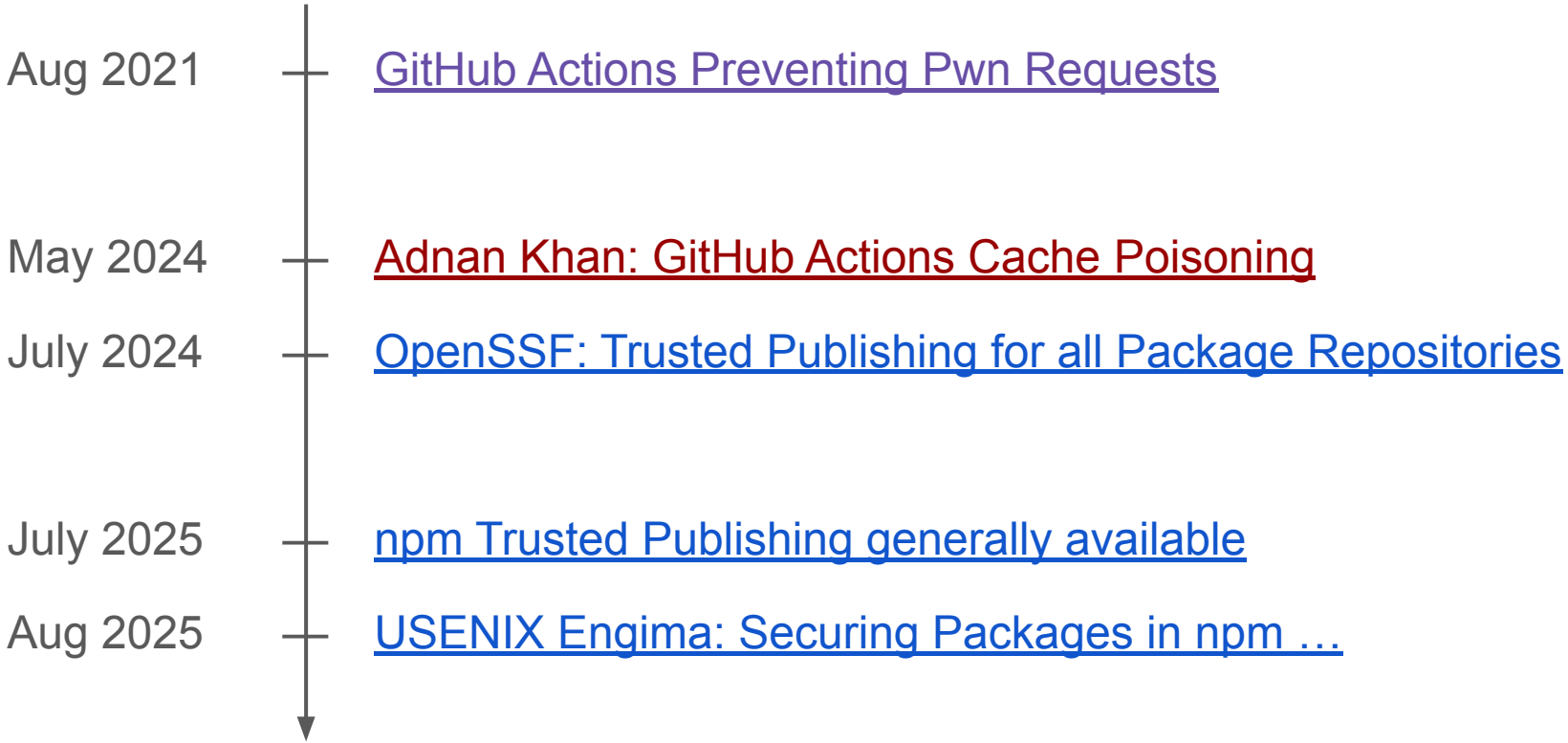
Security advice for users and maintainers to help reduce the impact of the next supply chain malware attack.

Madison Ficorilli · December 23, 2025

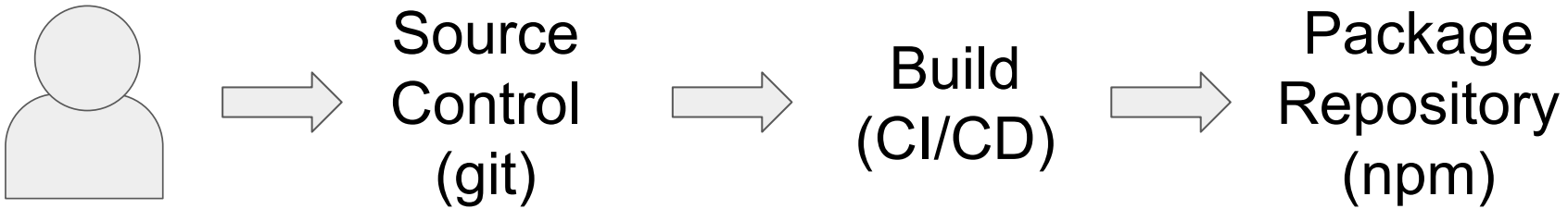
Credential Stealing Malware on npm

https://github.com/advisories

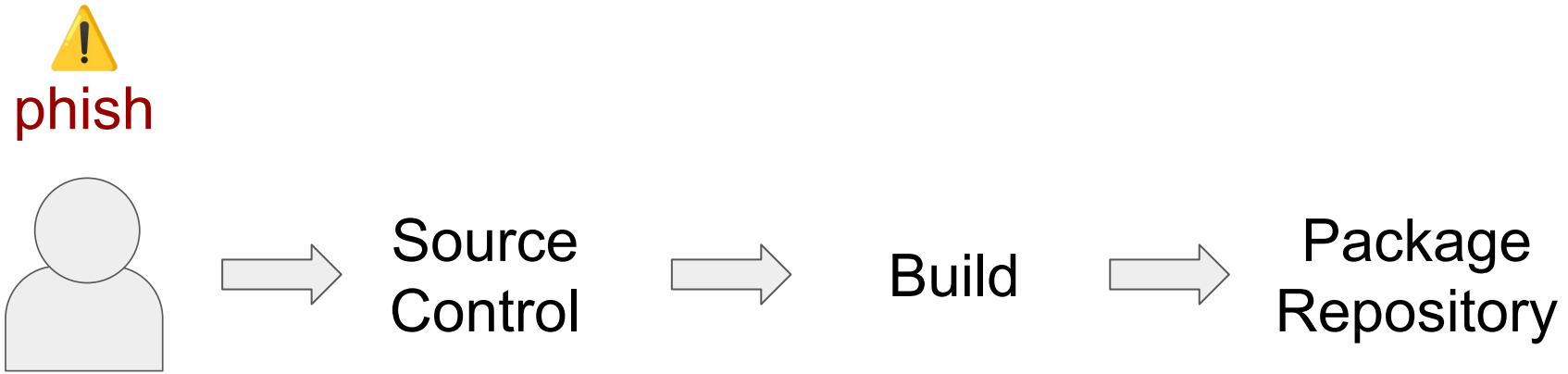



Aug 2021
GitHub Actions Preventing Pwn Requests
May 2024
Adnan Khan: GitHub Actions Cache Poisoning
July 2024
OpenSSF: Trusted Publishing for all Package Repositories
July 2025
npm Trusted Publishing generally available
Aug 2025
USENIX Engima: Securing Packages in npm …

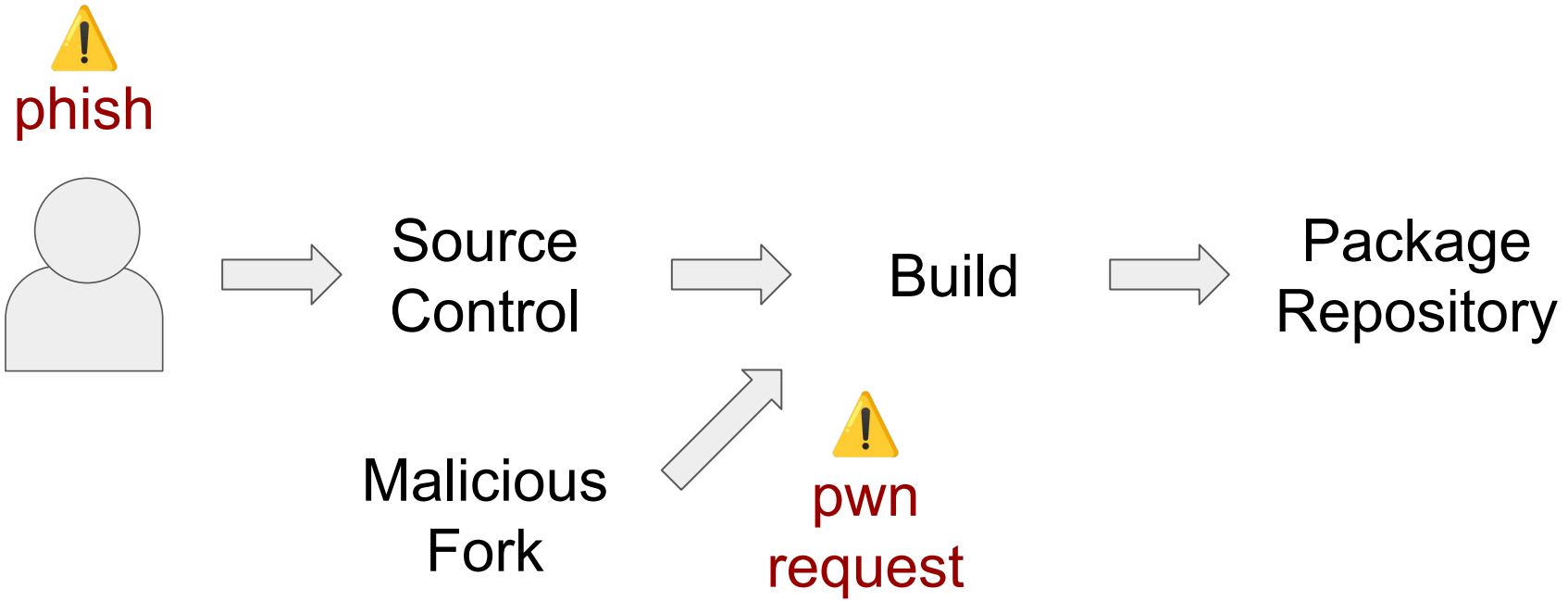
Software Supply Chain - https://slsa.dev



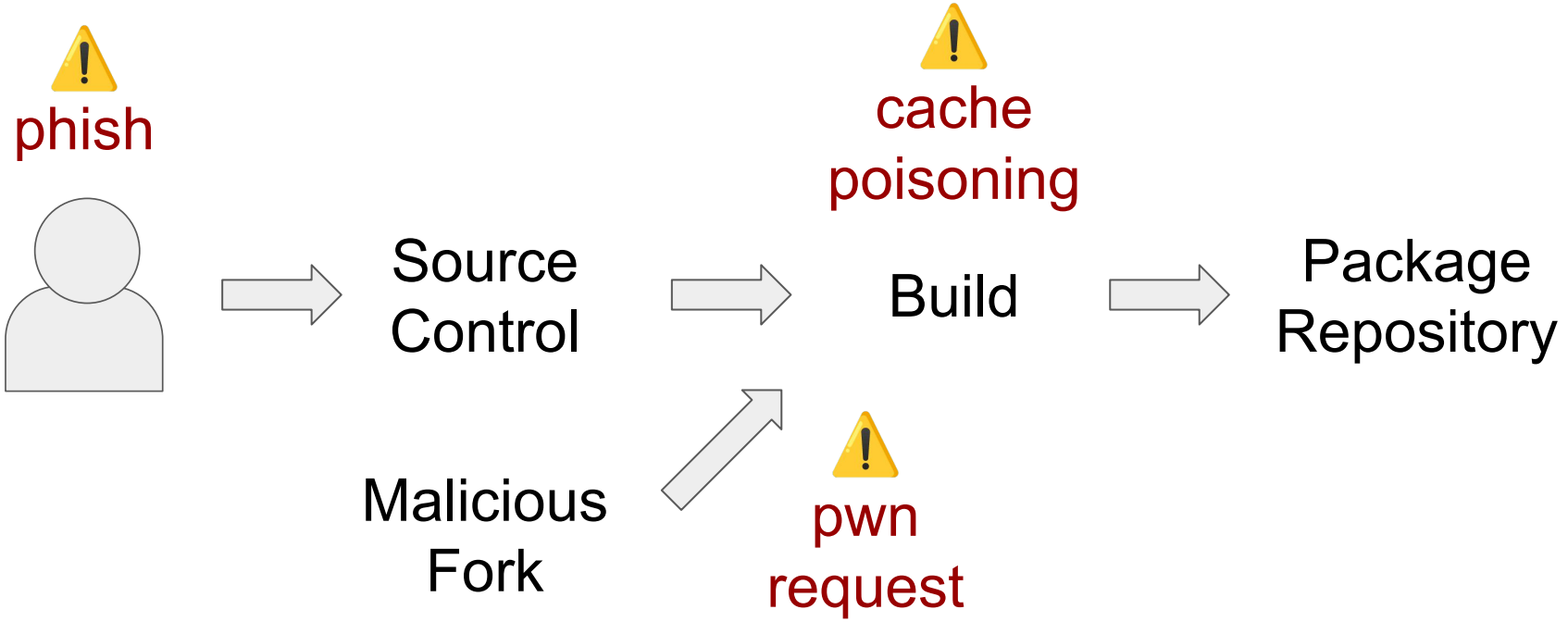
Do the Worm: 1) Compromise a Package



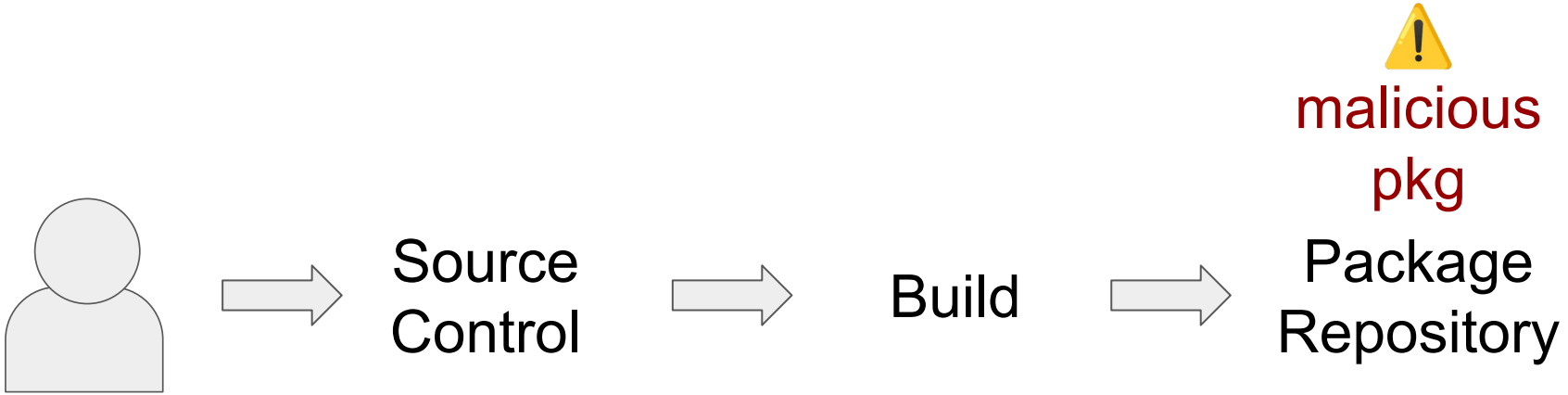
Do the Worm: 1) Compromise a Package



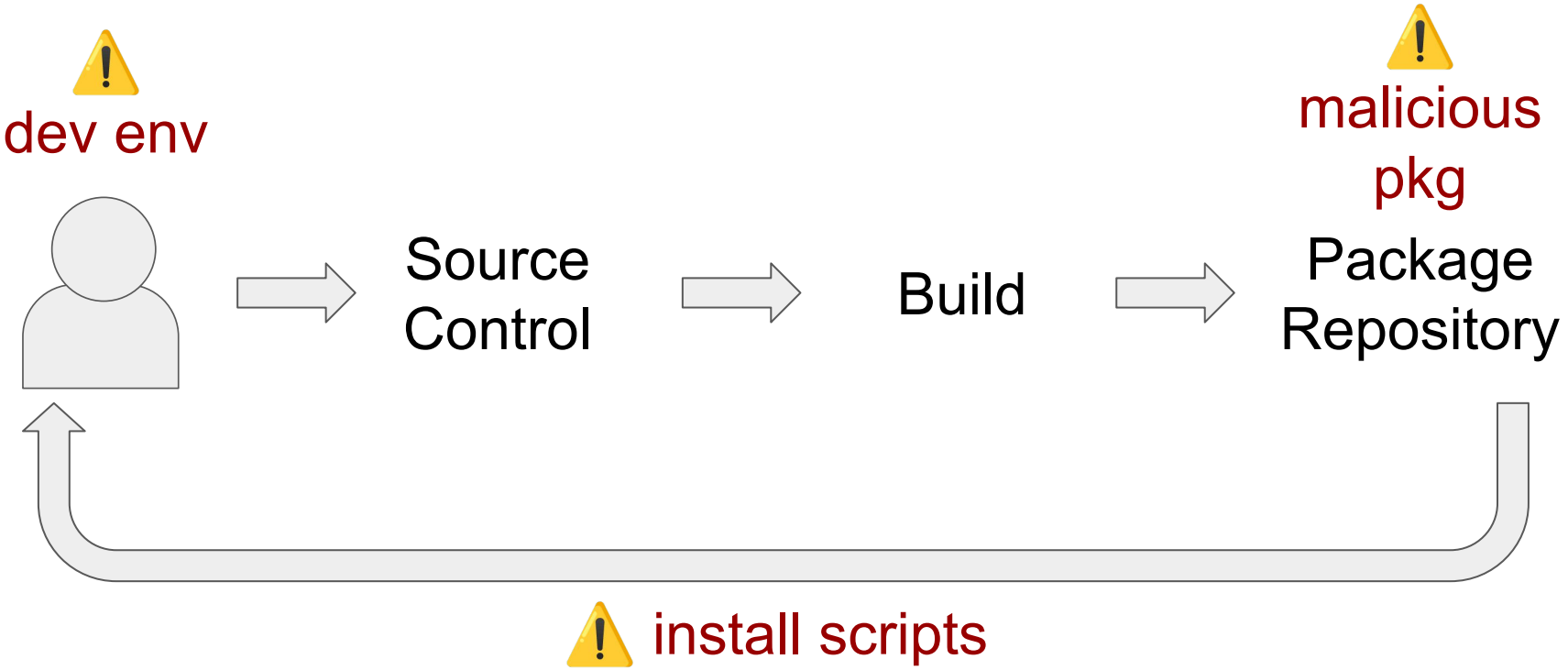
Do the Worm: 1) Compromise a Package



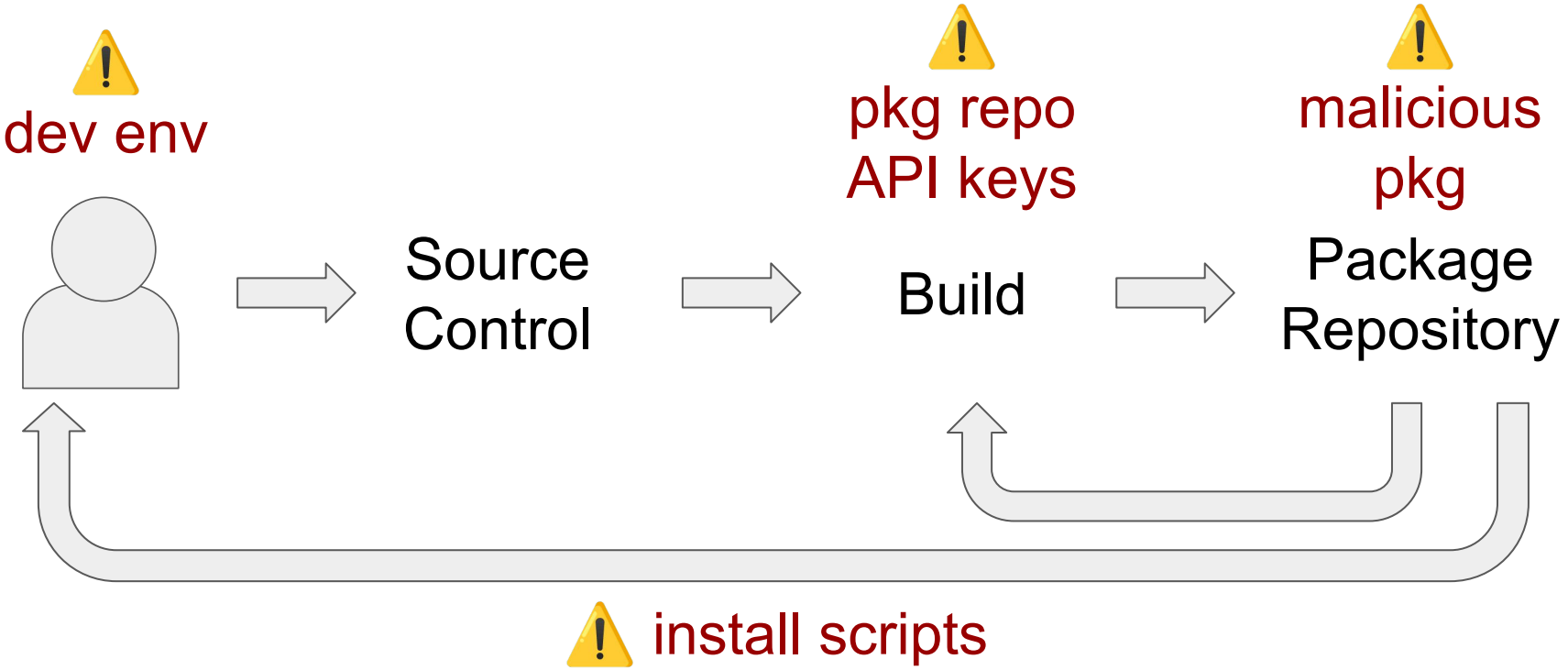
Do the Worm: 2) Exfil Credentials



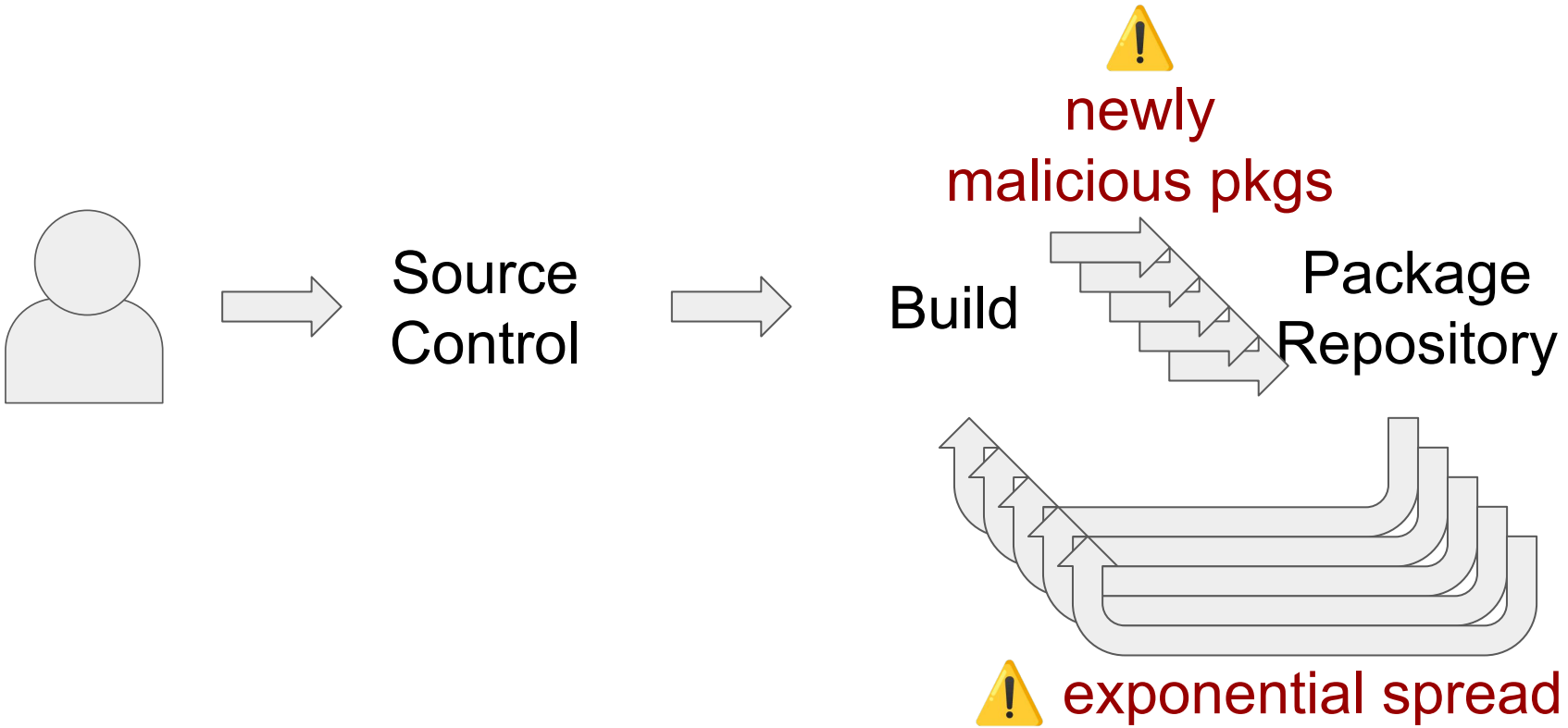
Do the Worm: 2) Exfil Credentials



Do the Worm: 2) Exfil Credentials

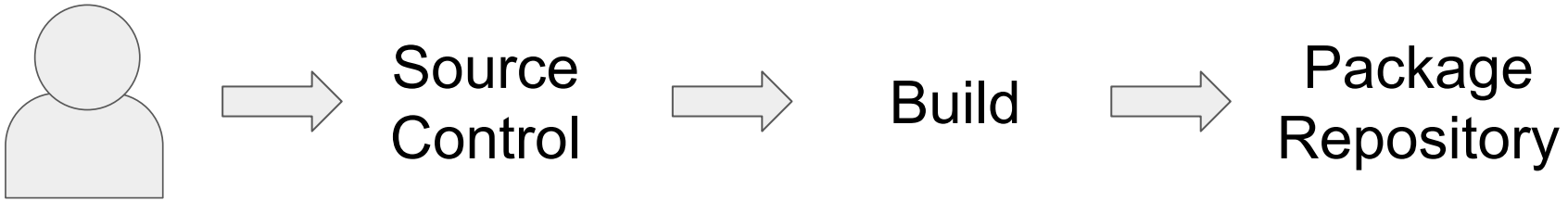


Do the Worm: 3) Propagate



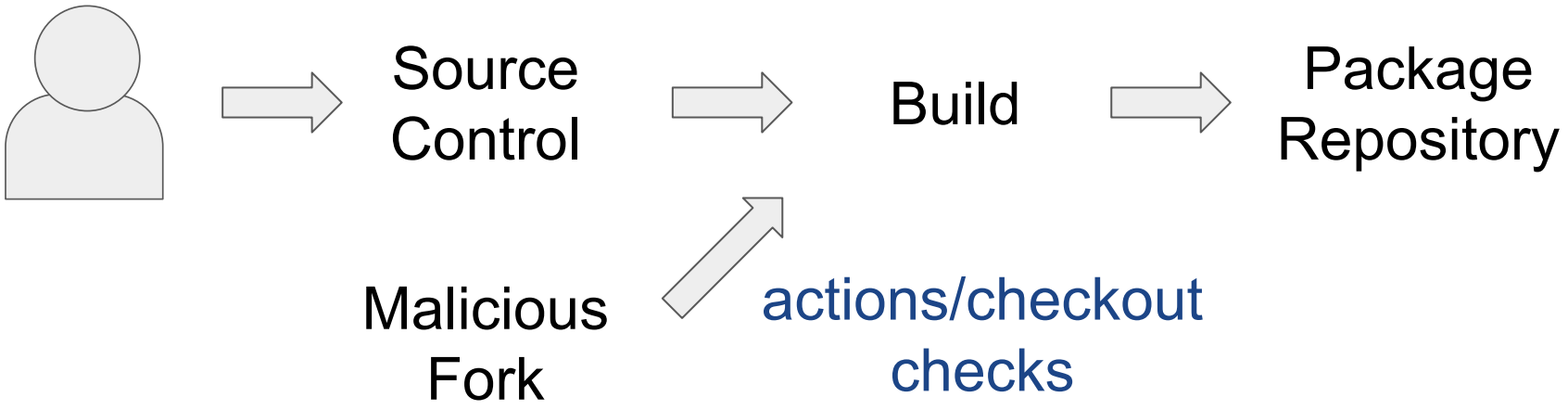
Defend: 1) Protect Packages

npm acct
read-only



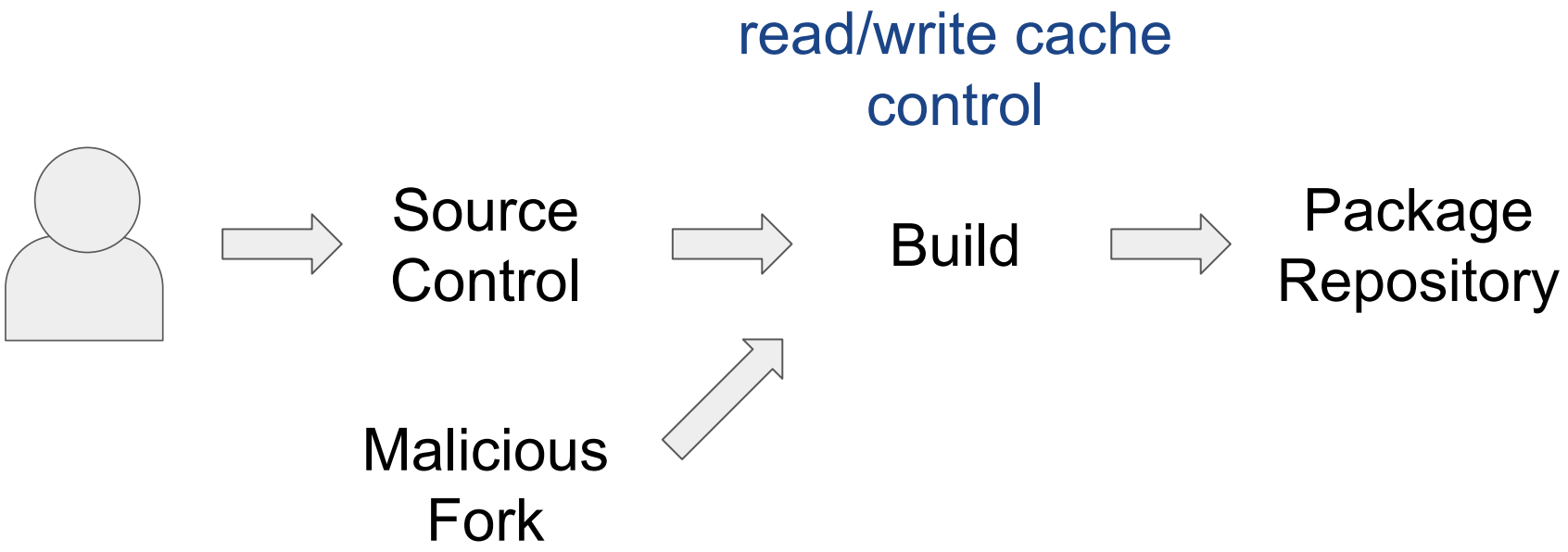
https://github.blog/changelog/2026-06-25-npm-adds-preventive-account-protection-for-high-impact-accounts/

Defend: 1) Protect Packages



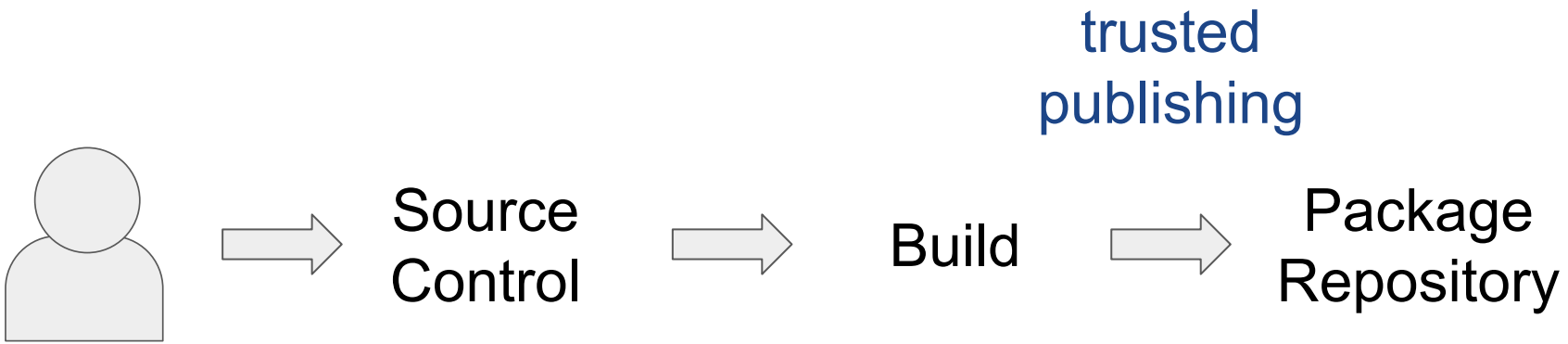
https://github.blog/changelog/2026-06-18-safer-pull_request_target-defaults-for-github-actions-checkout/

Defend: 1) Protect Packages



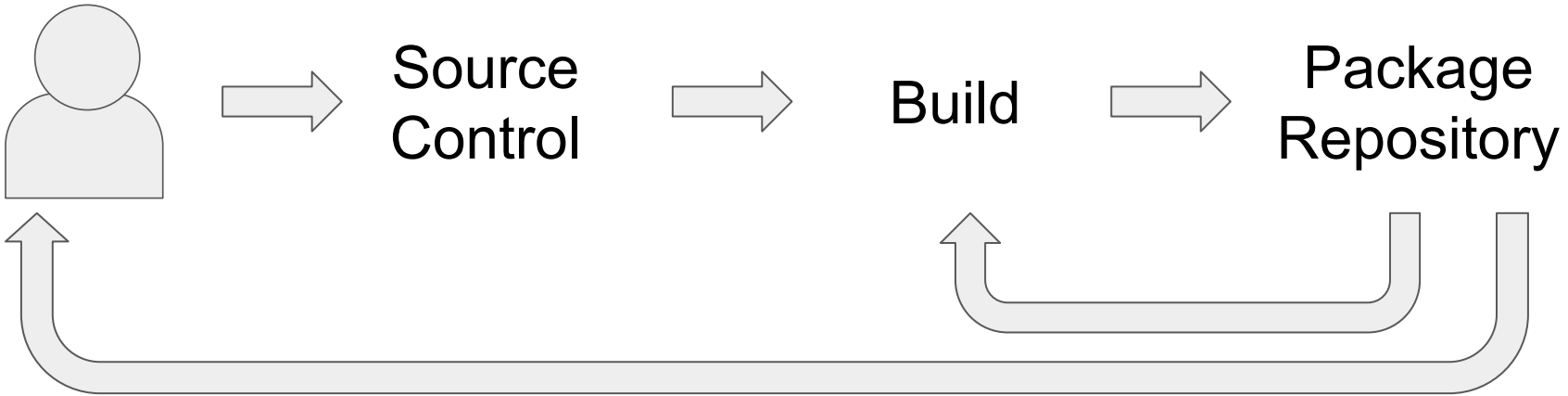
https://github.blog/changelog/2026-06-26-read-only-actions-cache-for-untrusted-triggers/

Defend: 2) Minimize Exfil



https://github.blog/changelog/2026-04-06-npm-trusted-publishing-now-supports-circleci/

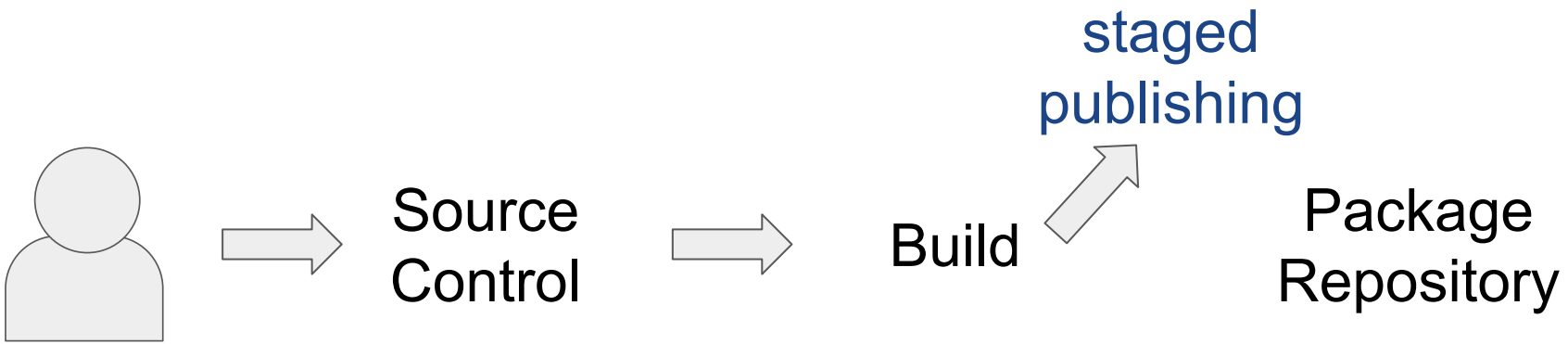
Defend: 2) Minimize Exfil



npm approve-scripts

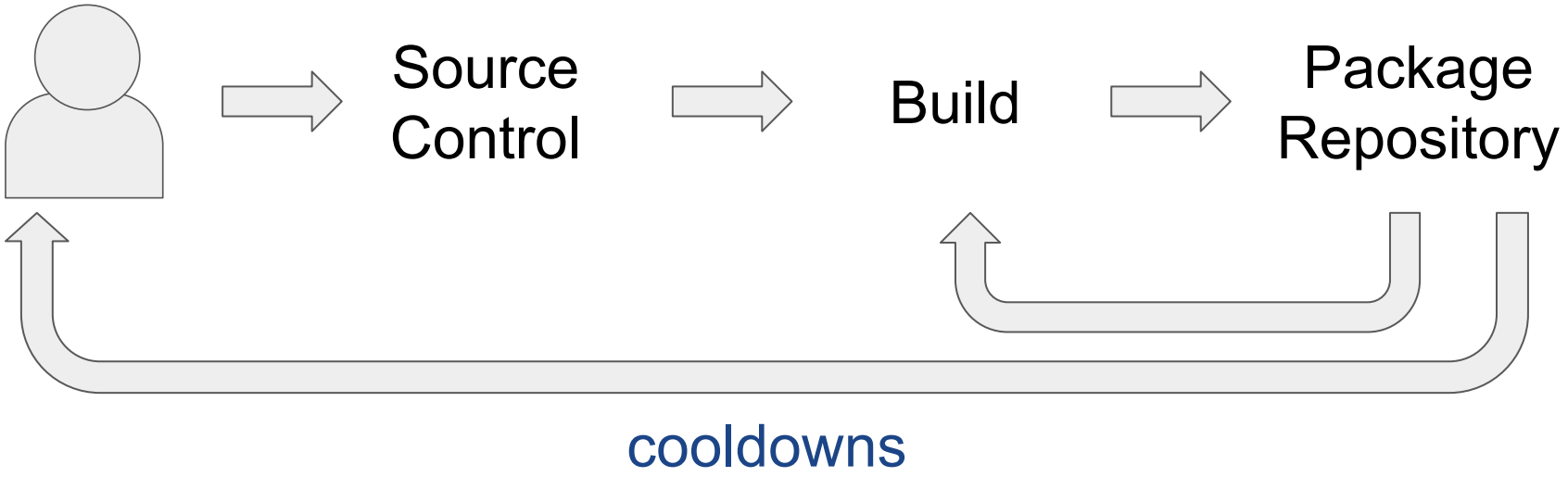
https://github.blog/changelog/2026-06-09-upcoming-breaking-changes-for-npm-v12/

Defend: 3) Minimize Propagation



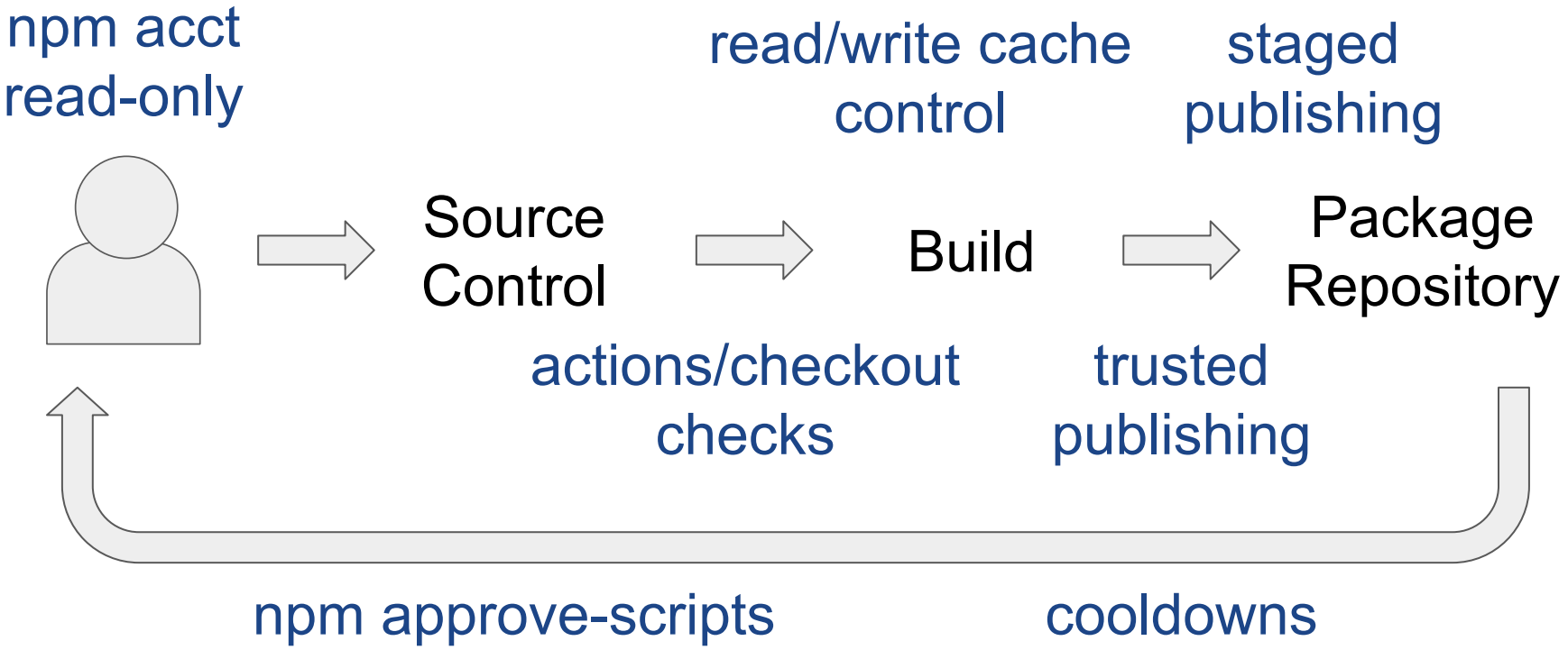
https://github.blog/changelog/2026-05-22-staged-publishing-and-new-install-time-controls-for-npm/

Defend: 3) Minimize Propagation



https://github.blog/changelog/2026-07-14-dependabot-version-updates-introduce-default-package-cooldown/

No Silver Bullets & Secure by Default



Research Questions

Cooldown duration & what they look like at scale

Lean in to open source as a strength

Anticipate future attack techniques

Thanks!

Zach Steindler

https://coffeehousecoders.org

USENIX Enigma 2026