mend.io

Mend.io Best Practice: Repository Scanning

The Challenge: Implementing Fixes In the Pipeline

Detecting vulnerable open source code in your applications only makes a difference when you can fix what's broken. When SCA scans are done only in the pipeline – when the vast majority of development work is already complete – fixes are often too complicated, and deadlines too close, for most vulnerabilities to be remediated.

The result is that organizations implementing only pipeline scanning may not be able to fix enough vulnerabilities to stop backlogs from forming and growing.

The Solution: Shift Left to Repository Scanning

By scanning in the repository, developers receive feedback in their native environment at the exact moment when they ask for information – before they have moved on to new coding tasks. By giving instant feedback when a pull request is made, developers can fix any security issues before they are merged, without the need to switch to a different UI.

This approach saves time and resources, reducing friction between developers and security teams. Mend.io research has shown that **customers who deploy Mend SCA scanning in the repository are able to fix over 3x more vulnerabilities, with a 74 percent reduction in mean time to remediation (MTTR).**

Using the instant feedback provided by repository scanning, organizations can implement and fine-tune policies to automate security processes. Mend.io also offers prioritization advice based on actual reachability (ensuring developers only fix what actually needs to be fixed). Developers can even automate the remediation process itself with automatic pull requests.

Benefits of Mend.io Repository Scanning

- **Shift left:** The repository represents the furthest left you can shift SCA scans while still enforcing policies and requiring all developers to scan their code.
- **Feedback on demand:** Developers receive feedback on their code right away, making it easier to remediate vulnerabilities and learn more secure coding practices.
- **No context switching:** Developers stay in the repository, with its familiar UI, making it easier to consume and act on scan results.
- **Differential results:** Developers are notified only when a pull request introduces new errors, reducing alert fatigue and making fixes available as soon as vulnerabilities are introduced.
- **Automated remediation:** Security vulnerabilities can be automatically remediated based on recommended fixes.