MEND

The Benefits of Application Scanning in the Repository

The goal of any software company is to ship reliable and secure code quickly. To develop securely at the speed of DevOps, where releases are delivered biweekly or more frequently, scanning for security defects after the build is too late. Scanning at later stages is costly. Returning to a problem from weeks earlier is inefficient and often causes friction between security teams and developers.

To address these concerns, security has been shifted left to earlier in the development process. Developers can now scan their code at all stages of development. Scanning without remediation, however, is not an effective strategy. Visibility does nothing to reduce risk.

Creating a Culture of Secure Coding

To reduce application security risk, organizations must focus on remediation, and any remediation efforts should automate as much of the security process as possible.

If developers are expected to own the security of their newly written code, security can not be a roadblock to development. Security needs to be integrated so that it is invisible to the developer experience. To achieve this, the best place to arm developers to take on security tasks is where they live and breathe – in the repository.

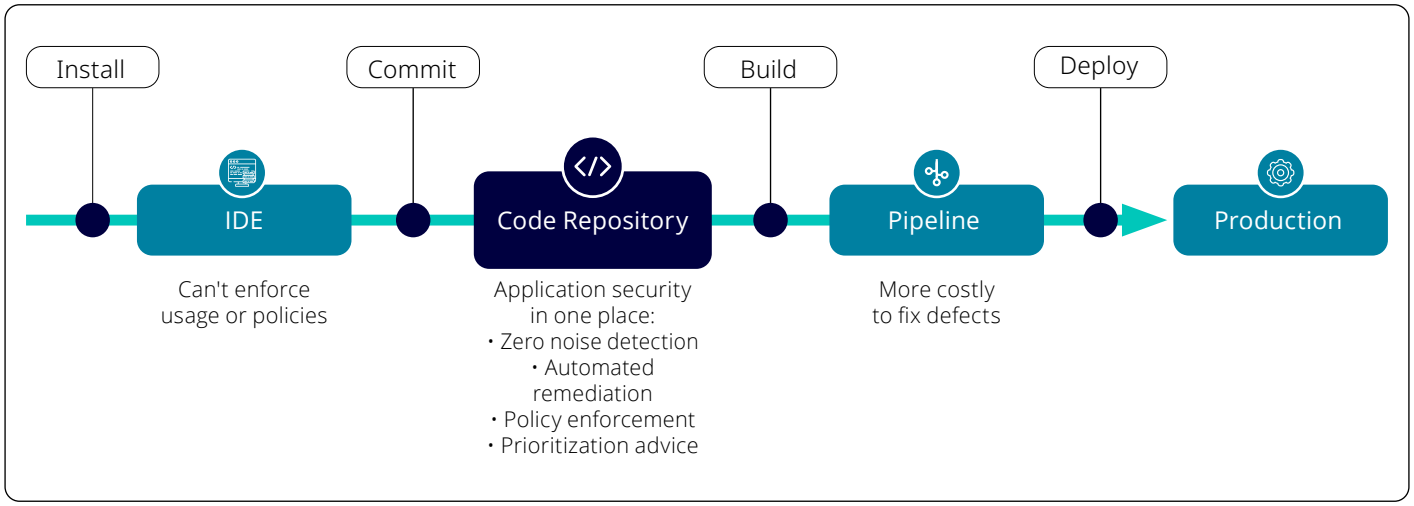
Scanning at the Repository Level

By scanning in the repository, developers receive feedback in their native development environment at the exact moment they are asking for information and before they have moved on to new coding tasks. By giving instant feedback when a pull request is made, developers are given the ability to fix any security issues before they are merged. Furthermore, by giving results within the repository, you avoid the context switching of moving to a different UI, which saves time and resources and reduces the friction between developers and security teams.

By scanning and providing instant feedback in the repository, organizations are able to implement and fine-tune policies that help automate the security process. Detailed prioritization and remediation advice at this point in development also helps lessen the burden placed on developers.

Benefits of Scanning in the Repository

- **Shift left** - Scanning at the repository is the furthest left you can shift while still enforcing policies and requiring all developers to scan their code.
- **Feedback on demand** – Developers receive feedback on their code when it is fresh in their minds, making it easier to remediate vulnerabilities.
- **No context switching** – Developers don't need to leave their native environment and don't have to learn a new UI, making it easier to consume and act upon scan results.
- **Differential results** – Developers are notified only if a pull request introduces new errors. Positive feedback is given to developers when a pull request resolves vulnerabilities. This differential view that focuses on feature branches – not mainline – prevents interruptions to workflows.
- **Automated remediation** – Security vulnerabilities can be automatically prioritized and remediated.



Weaknesses with Other SDLC Integrations

- **Browser integration** - While browser integrations help developers make informed decisions about the security of open source libraries, usage can not be enforced and is not being adopted consistently by every developer across an organization.
- **IDE integration** - IDEs are often not standardized across organizations, and there is no central way to enforce policies in IDEs.
- **CI/CD integration** - Scanning at this point in the SDLC occurs after code is already in the organization's repository, which means the cost of a fix is already higher. In addition, implementing an integration at this point is more challenging as organizations must deal with multiple, complex pipelines.

Developer-First Security

To create a culture of secure coding, security must focus on developers. A true developer-first security tool is fundamentally different and built with a different mindset from traditional security tooling. Organizations must meet developers in the environments in which they live and breathe every day to promote the consistent adoption of security best practices. Until then, it will be impossible to move security beyond just scanning to the remediation and prevention of security vulnerabilities.

About Mend

Mend helps organizations accelerate the development of secure software at scale. We provide automated tools that bridge the security knowledge gap, integrating easily into the software development life cycle and going beyond detection with a remediation-first approach. Mend is built on the most comprehensive vulnerability database in the industry, providing the widest coverage for threats and attack vectors. Our solution helps enterprises reduce risk and increase the productivity of their security and development teams. For more information, visit www.Mend.io

Related Resources

Learn more at www.mend.io