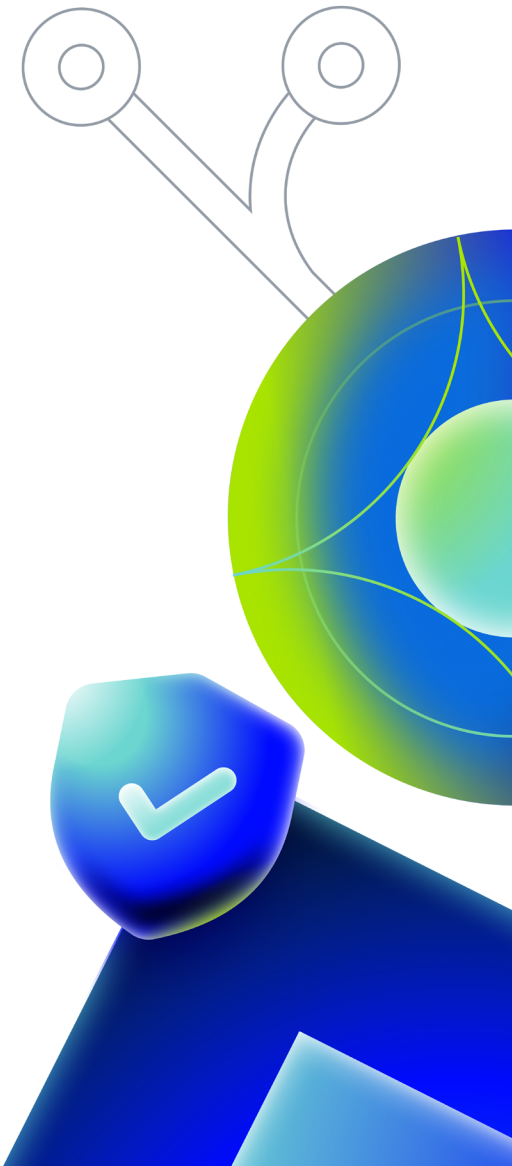
A checklist for AI-powered DevSecOps

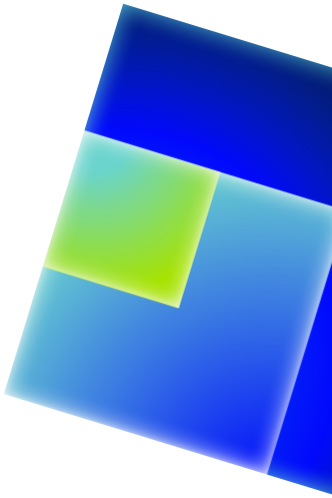


Could your software supply chain use a boost from AI?

Use this checklist to identify ways to safeguard your software supply chain and find opportunities for AI and automation integration.

Written by GitHub with ♥

Review and implement platform security fundamentals



Protect or safeguard accounts, and evaluate the security features of your tools and platforms.

- [ ] Only allow authorized personnel to access build environments. Use secure authentication and authorization measures.
- [x] Use secret scanning to scan identified and protected secrets against predefined partner patterns, as well as passwords, and other generic or unstructured secrets in code. AI
- [ ] When adopting an AI tool, ensure it meets security best practices, compliance requirements, and has solid security features like encryption and data masking.
- [x] Leverage AI to auto-generate custom patterns and protect secret types unique to your organization. AI
- [ ] Ensure your platform can compile and provide easy access to audit logs, so that your organization can meet compliance standards.

Protect your codebase

Monitor and protect the center of your supply chain.

- [ ] Create a software bill of materials (SBOM) that includes all software components (libraries, dependencies, etc.) of your product. The SBOM provides comprehensive details about the versions, origins, and dependencies of all software used in your products. This helps with vulnerability tracking and impact analysis.

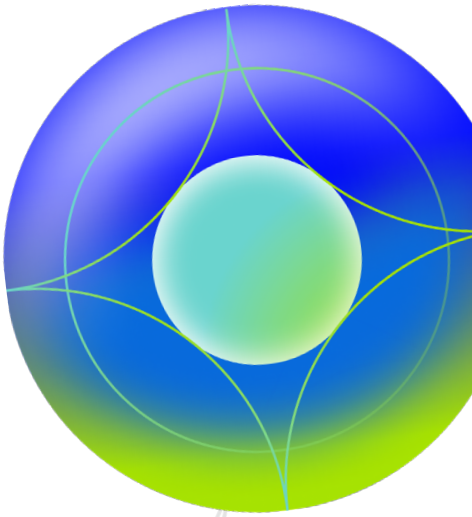
- [ ] Easily enable code scanning with default setup in your repository to automate monitoring of your codebase.

- [ ] Provide macro-level visibility into your environment so developers, team leaders, and security professionals can gauge the overall health and trends of your security posture, including tracking risk, remediation, and prevention.

- [x] Prioritize security alerts by customizing then automating triage rules with a tool like Dependabot. AI

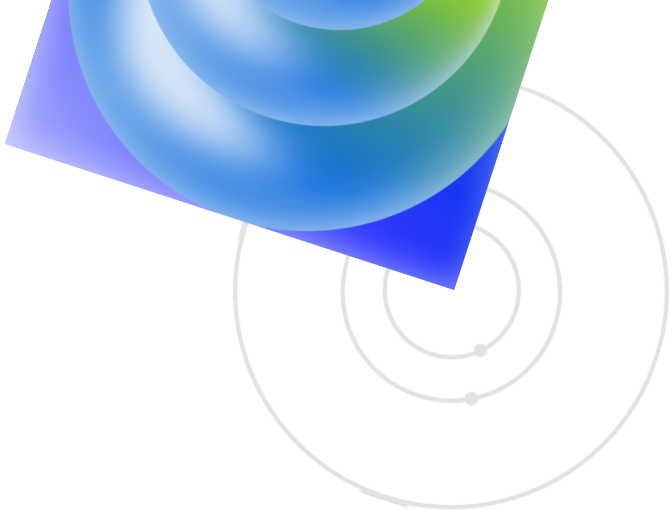
- [x] Automate remediation with code scanning autofix and provide developers, in a pull request, an AI-generated code fix with every vulnerability alert. AI

Safeguard your build system



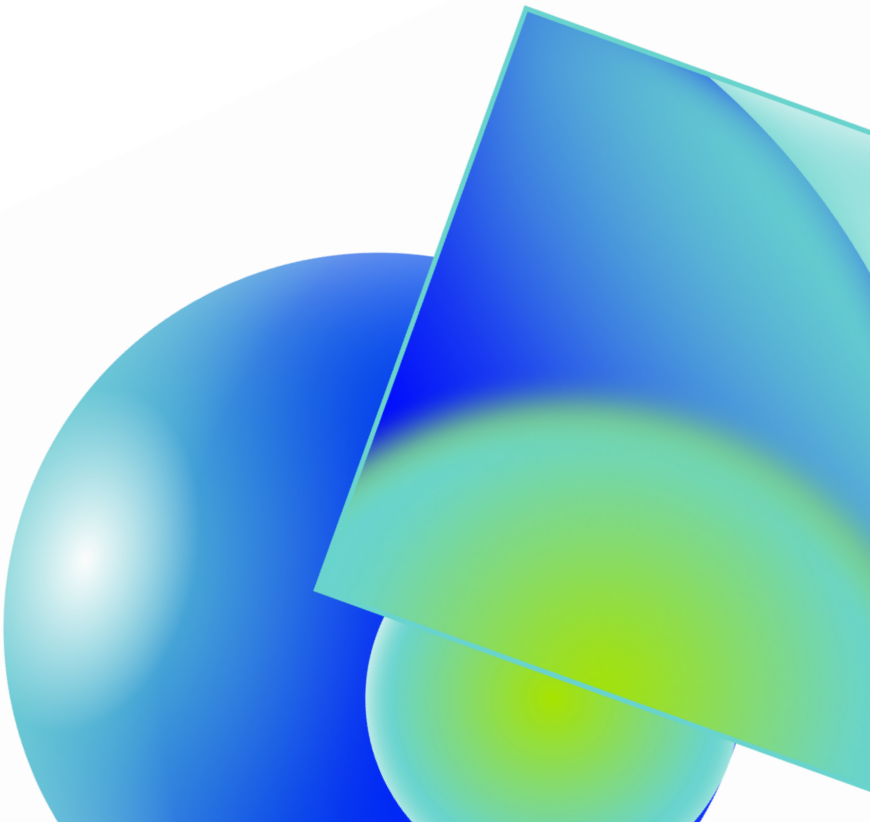
Protect the systems used to build and distribute artifacts.

- [ ] Isolate the environment where builds happen to prevent any outside interference or contamination of the build process.
- [ ] Use checksums or hash functions to conduct source code integrity checks and ensure the code is coming from a trusted source.
- [ ] Make the build process reproducible. This means that doing the build process in the same environment with the same source code should produce identical results.
- [ ] Sign the builds. Implement a system to sign the builds produced. This will certify that the build has not been tampered with since it was last signed.
- [x] Use an AI pair programmer to generate tailored workflows that you can automate with a CI/CD tool. AI
- [ ] Ensure developers use trusted workflows in their build environments by using secure automated workflows in the SDLC.



Learn more

Learn more about how new AI-powered features in GitHub Advanced Security can help you protect your software supply chain more efficiently than ever.



Written by GitHub with ♥