Phase 1: Align on your rollout strategy and goals

In this article

Before enabling code scanning and secret scanning, plan how GHAS should be rolled out across your enterprise.

This article is part of a series on adopting GitHub Advanced Security at scale. For the introduction to this series, see "Introduction to adopting GitHub Advanced Security at scale."

Set clear goals for your company’s rollout

To build a foundation for the direction of your company's rollout, outline goals for GHAS within your company, and communicate those goals to your team. Your goals can be simple or complex, as long as your team is aligned. If you need assistance with your goals, GitHub Professional Services can provide recommendations based on our experience with your company and other customers.

Here are some high-level examples of what your goals for rolling out GHAS might look like:

- Reducing the number of vulnerabilities: This may be in general, or because your company was recently impacted by a significant vulnerability that you believe could have been prevented by a tool like GHAS.
- Identifying high-risk repositories: Some companies simply want to target repositories that contain the most risk, enabling them to reduce risk by remediating vulnerabilities.
- Increasing remediation rates: To prevent the accumulation of security debt, you may wish to drive developer adoption of findings and ensure these vulnerabilities are remediated in a timely manner.
- Meeting compliance requirements: For example, many healthcare companies use GHAS to prevent the exposure of PHI (Personal Health Information).
- Preventing secrets leakage: Many companies want to prevent critical information from being leaked, such as software keys or financial data.

Lead your rollout with both your security and development groups

Companies that involve both their security and development teams in their GHAS rollouts tend to be more successful than companies who only involve their security group, waiting to include development teams once the pilot has concluded.

GHAS takes a developer-centered approach to software security by integrating seamlessly into the developer workflow. Having key representation from your development group early in the process decreases the risk of your rollout and encourages organizational buy-in.

Involving development groups earlier, ideally from the time of purchase, helps companies utilize GHAS to address security concerns earlier in the development process. When both groups work together, they achieve alignment early in the process, remove silos, build and strengthen their working relationships, and take more responsibility for the rollout.

Learn about GHAS

To set realistic expectations for the rollout, ensure that all stakeholders understand the following key facts about how GHAS works.

1. GHAS is a suite of security tools that require action to protect your code

GHAS is a suite of tools that increases with value when configured, maintained, used in daily workflows, and in combination with other tools.

2. GHAS will require adjustment out of the box

After GHAS is set up on your repositories, you'll need to configure GHAS to meet your company’s needs. Code scanning in particular requires further customization, such as evaluating initial results and making adjustments for future scans. Many customers find that initial scans return limited or irrelevant results until code scanning is adjusted based on the application's threat model.

3. GHAS tools are most effective when used together and integrated into your application security program

GHAS is most effective when all of the tools are used together. The effectiveness of your application security program is further improved by integrating GHAS with other tools and activities, such as penetration testing and dynamic scans. We recommend always utilizing multiple layers of protection.

4. Custom CodeQL queries are used by some companies to customize and target scan results

Code scanning is powered by CodeQL, the world’s most powerful code analysis engine. For many of our customers, the base query set and additional queries available in the community are more than sufficient. However, other companies may require custom CodeQL queries to target different results or reduce false positives.

If your company is interested in custom CodeQL queries, we recommend completing your rollout and implementation of GHAS first. Then, when your company is ready, GitHub Professional Services can help you navigate your requirements and ensure your company needs custom queries.

5. CodeQL scans the whole codebase, not just the changes made in a pull request

When code scanning is run from a pull request, the scan will include the full codebase and not just the changes made in the pull request. Scanning the entire codebase is an important step to ensure the change has been reviewed against all interactions in the

codebase.

For the next article in this series, see "Phase 2: Preparing to enable at scale."