Introduction to adopting GitHub Advanced Security at scale

In this article

You can adopt GitHub Advanced Security at scale in your company following industry and GitHub best practices.

About these articles

GitHub Advanced Security (GHAS) helps teams build more secure code faster using integrated tooling such as secret scanning and code scanning using CodeQL. To understand the security features available through GitHub Advanced Security, see "About GitHub Advanced Security."

GHAS is a suite of tools that requires active participation from developers across your enterprise. To realize the best return on your investment, you must learn how to use, apply, and maintain GHAS.

We've created a phased approach to GHAS rollouts developed from industry and GitHub best practices. We expect most customers will want to follow these phases, based on our experience helping customers with a successful deployment of GitHub Advanced Security, but you may need to modify this approach to meet the needs of your company.

Enabling GHAS across a large organization can be broken down into six core phases.

1. Align on your rollout strategy and goals: Think about what success will look like, and align on how GHAS will be implemented in your company. This phase may only take a few days or a week, but it lays a solid foundation for the rest of the rollout.
2. Preparing to enable at scale: Prepare developers, collect data about your repositories, and ensure you're ready for the next phase.
3. Pilot programs: Optionally, pilot an initial rollout to a few high-impact projects and teams. This will allow an initial group within your company to get familiar with GHAS before you roll out to the remainder of your company.
4. Create internal documentation: Create and communicate internal documentation for the consumers of GHAS. Without proper documentation provided to developers, security engineers, and others who will be using GHAS, the value will get lost in the rollout.
5. Rollout and scale code scanning: Leveraging the available APIs, automatically rollout code scanning by team and by language across your enterprise, using the repository data you collected earlier.
6. Rollout and scale secret scanning: Roll out secret scanning, which involves less configuration and is therefore simpler to adopt than code scanning. Still, it's critical

to have a strategy for handling new and old results.

GitHub Support and Professional Services

If you encounter any issues or have any questions during your implementation, you can search our documentation for solutions or engage with GitHub Support. For more information, see "About GitHub Support."

If you prefer to have guidance throughout the rollout process, GitHub Professional Services can partner with you for a successful rollout and implementation of GitHub Advanced Security. We offer a variety of options for guidance and support. We also have training and bootcamps available to help your company to optimize the value of GitHub Advanced Security.

Speak with your sales representative for more information about all the Professional Services options available. For more information, contact GitHub's Sales team.

> For the first article in this series, see "Phase 1: Align on your rollout strategy and goals."