

Viewing metrics for secret scanning push protection in your organization

In this article

About metrics for secret scanning push protection

Viewing metrics for secret scanning push protection

You can use security overview to see how secret scanning push protection is performing in repositories across your organization, and to identify repositories where you may need to take action.

Who can use this feature

Security overview for an organization is available to all members of the organization. The views and data displayed are determined by your role in the organization, and by your permissions for individual repositories within the organization. For more information, see "[About security overview](#)."

Security overview for an enterprise shows organization owners and security managers data for the organizations they have access to. Enterprise owners can only view data for organizations where they are added as an organization owner or security manager. For more information, see "[Managing your role in an organization owned by your enterprise](#)."

All enterprises and their organizations have a security overview. If you use GitHub Advanced Security features, which are free for public repositories, you will see additional information. For more information, see "[About GitHub Advanced Security](#)."

Note: Secret scanning metrics for push protection is currently in beta and subject to change.

About metrics for secret scanning push protection

If you are an organization owner or security manager, the metrics overview for secret scanning push protection helps you to understand how well you are preventing security leaks in your organization. You can use the metrics to assess how push protection is performing, and to easily identify the repositories where you may need to take action in order to prevent leaks of sensitive information.

The overview shows you a summary of how many pushes containing secrets have been successfully blocked across your organization by push protection, as well as how many times push protection was bypassed.

You can also find more granular metrics, such as:

- the secret types that have been blocked or bypassed the most
- the repositories that have had the most pushes blocked
- the repositories that are bypassing push protection the most
- the percentage distribution of reasons that users give when they bypass the protection

The metrics are based on activity from the last 30 days.

Secret scanning

Activity from the last 30 days

Push protection

Total secrets blocked

14

Total secrets blocked by push protection in this organization

Successfully blocked secrets

10

Secrets removed before pushing and not exposed in the repository

Bypassed secrets

4

Secrets bypassed after they were blocked by push protection

Blocks

All secrets pushed, including secrets bypassed and secrets fixed on block. Only secrets bypassed create alerts.

Most blocked secret types

octo-token-1 (custom pattern)	9
Clojars Deploy Token	4
Discord Bot Token	1

Repositories with most pushes blocked

octocat-repo	11
monalisa-repo	3

Bypasses

Secrets pushed and bypassed. A user allowed this secret to be pushed and the secret was exposed in a repository.

Most bypassed secret types

Clojars Deploy Token	2
octo-token-1 (custom pattern)	2

Repositories with most secrets bypassed

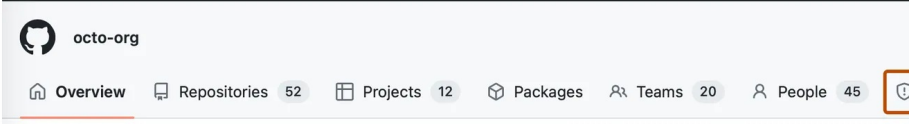
octocat-repo	4
------------------------------	---

Viewing metrics for secret scanning push protection



- 1

On GitHub.com, navigate to the main page of the organization.
- 2

Under your organization name, click **Security**.
- 
- 3

In the sidebar, under "Metrics", click **Secret scanning**.
- 4

Click on an individual secret type or repository to see the associated secret scanning alerts for your organization.

Legal