

Notification Decision Matrix for Monitoring Secret Scanning Alerts

This document summarizes *who* is notified, and *under what conditions*, when GitHub secret scanning generates alerts. It distinguishes between notifications from incremental scans (new secrets as they are committed) and historical scans (retrospective scans of existing content).

Decision Matrix by Role and Event

Table 1: Notification decision matrix for secret scanning alerts

Role	Incremental scan: new secret detected	Historical scan completed (secrets may or may not be found)	Historical scan detects at least one secret
Repository administrator	Notified according to their notification preferences when a new secret is detected in the repository.	No notification when a historical scan completes with <i>no</i> secrets detected.	Notified when a historical scan detects one or more secrets, subject to notification preferences.
Security manager	Notified according to notification preferences when a new secret is detected.	Notified whenever a historical scan completes for the organization or enterprise, even if no secrets are found.	Notified when a historical scan detects secrets, subject to notification preferences (in addition to the “scan completed” notification).
User with custom role (read/write access to the repository)	Notified according to notification preferences when a new secret is detected.	Not notified solely for completion events with no secrets (unless they also hold another role such as security manager).	Notified when a historical scan detects secrets in repositories where their custom role grants access, subject to notification preferences.
Organization owner (who is an administrator of the affected repository)	Notified according to notification preferences when a new secret is detected in a repository they administer.	Notified whenever a historical scan completes for the organization, even if no secrets are found.	No additional detection-specific notification is described beyond the “scan completed” notification.
Enterprise owner (who is an administrator of the affected repository)	Notified according to notification preferences when a new secret is detected in a repository they administer.	Notified whenever a historical scan completes for the enterprise, even if no secrets are found.	No additional detection-specific notification is described beyond the “scan completed” notification.
Commit author (for the commit that introduced the secret)	Always notified when they accidentally commit a secret, <i>regardless</i> of their notification preferences.	Not notified when a historical scan completes.	Not notified when a historical scan detects secrets.

Email Delivery Conditions for Preference-Based Notifications

For all cases in Table 1 that state “notified according to notification preferences,” an email notification is sent only when *all* of the following are true:

- The user is **watching** the repository.
- For that repository, the user has enabled either:
 - “All activity”, or
 - A custom configuration that includes “Security alerts”.
- In the personal notification settings, under “Subscriptions” and then “Watching”, the user has selected **Email** as a notification channel.

Assignment notifications. In addition to the matrix above, *any* user who can be assigned to a secret scanning alert will receive a notification when an alert is assigned to them, independent of whether they are watching the repository. The exact delivery channel (email, web, mobile, and so on) follows their general GitHub notification settings.

Auditing. Actions taken on secret scanning alerts (including resolution and assignment) can be audited using GitHub’s security auditing features, but this auditing does not change the notification behaviour summarized in the decision matrix.