0

GitHub Advanced Security implementation guide

What's inside

- 3 Introduction
- 4 Enabling GitHub Advanced Security
- 7 Configuring code scanning
- 10 Setting up secret scanning
- 12 Security overview
- 13 GitHub Advanced Security licensing model

Introduction

GitHub Advanced Security enables you to better secure your supply chain and simplify the remediation process for code in progress. The following guide has been created to help you enable and configure GitHub Advanced Security, and this guide contains direct links to all the resources and documents you might need during your implementation.

Prerequisites:

Your GitHub account manager has notified you that GitHub Advanced Security has been enabled for your enterprise or organization.

You must be the administrator or owner of your organization to enable and configure GitHub Advanced Security. If you are not the org admin/owner, you will need to request your GitHub org admin/owner to enable GitHub Advanced Security.

More resources:



Enabling GitHub Advanced Security

GitHub Advanced Security – organizational level

When you enable GitHub Advanced Security at the organizational level, you can secure the code in your organization's private repositories. The following steps address how to configure security features to meet your organization's specific requirements:

1. First access your organization as the administrator or owner, and then click on **Settings**.

2 General Code security and analysis 2 Features Security and analysis features help keep your repositories secure and updated. By enabling these features, you're granting us permission to permission to permission or your organization's repositories. 2 Bining and plans Dependency graph Disable all Enable all 2 Honber privileges Team discussions Dependabot Disable all Enable all 3 Monther privileges Dependabot alerts Dependabot Disable all Enable all 4 Monther privileges Dependabot alerts Dependabot alerts Dependabot 6 Adderation Dependabot alerts Dependabot alerts Disable all Enable all 8 Repository Sociespaces Dependabot alerts Disable all Enable all 9 Repository Sociespaces Disable all alerable for new repositories Disable all Enable all 9 Repository Sociespaces Disable all alerables or new repositories Disable all Enable all 9 Repository Sociespaces Disable all alerable for new private and Internal repositories. Learn more about Other Advanced Security Disable all Enable all 9 Repository Sociespaces Disable all Enable all E	Organization account	2 Switch to another account +	Go to your org	anization profile
E Fedures Security and analysis features help keep your repositories secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your organization's repositories. B Bling and plans Dependency graph Disable all Enable all Construction Dependency graph Disable all Enable all I Member privileges Dependency graph Disable all Enable all Paren discussions Dependabot Dependabot I memort/Export Dependabot alerts Dependabot alerts Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot puill requests to resolve these vulnerabilities. Configure alert notifications. Disable all Enable all I Repository Automatically enable for new provates Disable all Enable all I Repository Automatically enable for new provates automatically to resolve Dependabot alerts. Disable all Enable all I Repository Automatically enable for new provates automatically to resolve Dependabot alerts. Disable all Enable all I Receive alerts for vulnerabilities. Configure alert notifications. Disable all Enable all I Receive alerts for vulnerabilities that affect your dependencies accurity enable and internal repositories. Disable all Enab	General	Code security and analysis		
cess perform read-only analysis on your organization's repositories. 9 Billing and plans Dependency graph Understand your dependencies. Disable all • Member privileges I Automatically enable for new private repositories • Team discussions Dependabot • Recey our dependencies secure and up-to-date. Learn more about Dependabot. Disable all • Dependabot Recey our dependencies secure and up-to-date. Learn more about Dependabot. • Dependabot alerts Receive alerts for vulnerabilities. Configure alert notifications. • Receive alerts Dependabot alerts • Codespaces Dependabot security updates • Automatically enable for new repositories Disable all • Automatically enable for new repositories Disable all • Papedages CitHub Advanced Security updates Disable all • Projects CitHub Advanced Security features are billed per active committer in private and internal repositories. • Automatically enable for new repositories CitHub Advanced Security. • Projects CitHub Advanced Security features are billed per active committer in private and internal repositories. • Automatically enable for new problex learn more about GitHub Advanced Security. Disable all • Automatically enable for new public and Advanced Security. CitHub Advanced Security repositories • Automatically enable for	Features	Security and analysis features help keep your repositories secure and updated. By enabling these feature	s, you're granting us p	ermission to
Billing and plans Bependency graph Understand your dependencies.	cess	perform read-only analysis on your organization's repositories.		
a Repository roles Understand your dependencies. b Member privileges 7 Fam discussions i mort/Skport 3 Moderation 4 Repository <	Billing and plans	Dependency graph	Disable all	Enable all
A Member privileges A member privileg	Repository roles	Understand your dependencies.		Endere di
Team discussions Dependabot Import/Export Ree your dependabotics secure and up-to-date. Learn more about Dependabot. Dependabot alerts Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. Configure alert notifications. Disable all Enable all Receive alerts for vulnerabilities configure alert notifications. Disable all Enable all Receive alerts for vulnerabilities. Configure alert notifications. Disable all Receive alerts for vulnerabilities. Configure alert notifications. Disable all Receive alerts for vulnerabilities. Configure alert notifications. Disable all Receive alerts for vulnerabilities that affect your dependabot security updates Disable all Nethooks Automatically enable for new repositories Disable all Pages GitHub Advanced Security Disable all Enable all Projects GitHub Advanced Security Disable all Enable all Receive alerts for detected secrets, keys, or other tokens. Disable all Enable all Receive alerts for detected secrets, keys, or other tokens. Disable all Enable all Receive alerts for detected secrets, keys, or other tokens. Disable all Enable all Secrets	Member privileges	Automatically enable for new private repositories		
Import/Export Dependabot Moderation Very dependencies secure and up-to-date. Learn more about Dependabot. Moderation Dependabot alerts Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. Configure alert notifications. Disable all Enable all Repository Import/Export Dependabot security updates Disable all Enable all Actions Dependabot to open pull requests automatically to resolve Dependabot alerts. Disable all Enable all Neckages GitHub Advanced Security Automatically enable for new repositories Disable all Enable all Pages GitHub Advanced Security GitHub Advanced Security Disable all Enable all Projects GitHub Advanced Security GitHub Advanced Security Disable all Enable all Code security Secret scanning Receive alerts for detected secrets, keys, or other tokens. Disable all Enable all Verified and approved domains Secret scanning Disable of new public repositories added to secret scanning Disable all Enable all Outh application policy Outh application security and analysis Push protection Disable all Ena	Team discussions			
Moderation Codespaces Moderation Dependabot alerts Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull Receive alerts for vulnerabilities. Configure alert notifications. Godespaces Actions Vebbooks Actions Vebbooks Dependabot security updates Allow Dependabot to open pull requests automatically to resolve Dependabot alerts. Disable all Enable all Actions Vebbooks Discussions Receive alerts for vulnerabilities. Configure alert notifications. Disable all Enable all Automatically enable for new repositories Disable all Enable all Automatically enable for new repositories Packages GitHub Advanced Security Projects curity Automatically enable for new private and Internal repositories Code security and analysis Verified and approved domains Secret scanning Block commits that contain secrets, keys, or other tokens. Codespace Push protection Block commits that contain secrets, Learn more about push protection. Independation policy Okutomatically enable for repositories added to secret scanning	Import/Export	Dependabot		
de, planning, and automation Dependabot alerts Disable all Repository Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull Disable all Repository Codespaces Dependabot security updates Disable all Actions Dependabot to open pull requests a utomatically to resolve Dependabot alerts. Disable all Vebbooks Automatically enable for new repositories Disable all Packages GitHub Advanced Security Disable of reav repositories Packages GitHub Advanced Security Disable of reav repositories. Projects GitHub Advanced Security in their update and Internal repositories. The features are for onew repositories. Learn more about GitHub Advanced Security. Disable all Codes security and analysis Secret scanning Disable of reav public repositories. Verified and approved domains Secret scanning Disable of repositories alert scanning Secrets Push protection Disable of repositories alert scanning Idvitub Apps Automatically enable for new public and Advanced Security repositories Verified and approved domains Push protection Biock commits that contain secrets, keys, or other tokens. Disable all Idvitub Apps Automatically enable for repositories added to secret scanning Idvitub Apps Add aresource link in the CLI and web UI when a commit is blocked	Moderation	Reep your dependencies secure and up-to-date. Learn more about Dependabot.		
de, panning, and advination Repository Codespaces Actions Dependabot security updates Actions Dependabot to open pull requests automatically to resolve Dependabot alerts. Disable all Codespaces Webhoks Discussions Discussions Discussions Packages GitHub Advanced Security GitHub Advanced Security GitHub Advanced Security Disable all Enable all Code security Code security Secrets Push protection Biox commits the contain secrets, Learn more about push protection. Okable all Enable all Indumatically enable for new public and Advanced Security repositories Projects Code security Secret scanning Receive alerts for detected secrets, keys, or other tokens. Image: Secret scanning Receive alerts for detected secrets, keys, or other tokens. Image: Secret scanning Receive alerts for detected secrets, keys, or other tokens. Image: Secret scanning Receive alerts for detected secrets, keys, or other tokens. Image: Secret scanning Receive alerts for detected secrets, keys, or other tokens. Image: Secret scanning Receive alerts for detected secrets, keys, or other tokens. Image: Secret scanning Receive alerts for detected secrets, keys, or other tokens. Image: Secret scanni		Dependabot alerts Becally alerts for unless hitches that affect your dependencies and manually concerns Dependables of	Disable all	Enable all
Nepository Codespaces Codespaces Dependabot security updates Actions Dependabot to open pull requests automatically to resolve Dependabot alerts. Discussions Automatically enable for new repositories Packages GitHub Advanced Security GitHub Advanced Security Brojects Pages GitHub Advanced Security GitHub Advanced Security to stable of new private and Internal repositories. The features are free of charge in public repositories. Learn more about GitHub Advanced Security. Curity Secret scanning Receive alerts for detected secrets, keys, or other tokens. Verified and approved domains Push protection Block commits that contain secrets, Learn more about push protection. Secrets Push protection Block commits that contain secrets, Learn more about push protection. Olisable all Enable all	de, planning, and automation	requests to resolve these vulnerabilities. Configure alert notifications.		
	Repository	Automatically enable for new repositories		
Actions Dependabot security updates Disable all Enable all Actions Automatically enable for new repositories Image: Control of the contr	Codespaces			
a Webhooks Allow Dependabot to open pull requests automatically to resolve Dependabot alerts. b Biscussions Automatically enable for new repositories c Projects GitHub Advanced Security g Projects GitHub Advanced Security enable for new private and Internal repositories. The features are free of charge in public repositories. Learn more about GitHub Advanced Security. Disable all g Projects GitHub Advanced Security enable for new private and Internal repositories. Disable all courity Secret scanning Disable all Enable all Receive alerts for detected secrets, keys, or other tokens. Disable all Enable all eCourts Secret scanning Disable all Enable all Receive alerts for detected secrets, keys, or other tokens. Push protection Disable all Enable all B Overfield and approved domains Secrets Push protection Disable all Enable all B Overfield and approved domains Secrets Disable for repositories added to secret scanning Disable all Enable all edithub Apps Automatically enable for repositories added to secret scanning Disable all Enable all g Guthub Apps Add aresource link in the CLI and web UI when a commit is blocked Disable all) Actions	Dependabot security updates	Disable all	Enable all
Discussions Automatically enable for new repositories Disable all Disable al	Webhooks	Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.		
Operackages GitHub Advanced Security Disable all Enable all Projects GitHub Advanced Security features are billed per active committer in private and internal repositories. The features are free of charge in public repositories. Learn more about GitHub Advanced Security. Disable all Enable all corrity Authentication security Secret scanning Disable all Enable all Q code security and analysis Secret scanning Disable all Enable all Q code security and analysis Secret scanning Disable all Enable all Q code security and analysis Secret scanning Disable all Enable all Q code security and analysis Push protection Disable all Enable all B code security and proved domains Push protection Disable all Enable all B code security and security enable for repositories added to secret scanning Automatically enable for repositories added to secret scanning Disable all Enable all B code bases Quithub Advanced Security repositories Disable all Enable all Enable all GitHub Advanced Security enable for repositories added to secret scanning Add aresource link in the CLI and web UI when a commit is blocked Disable all Enable all	Discussions	Automatically enable for new repositories		
g Pages GitHub Advanced Security Disable all Enable all g Projects GitHub Advanced Security features are billed per active committer in private and internal repositories. The features are free of charge in public repositories. Learn more about GitHub Advanced Security. Disable all Enable all ecurity Automatically enable for new private and internal repositories Disable all Enable all g Code security and analysis Secret scanning Disable all Enable all g Code security and analysis Secret scanning Disable all Enable all g Parfed and approved domains Secrets Push protection Disable all Enable all B Ock commits that contain secrets, Learn more about push protection. Disable all Enable all Enable all B Ock party Access Isck contain secrets, Learn more about push protection. Disable all Enable all B Ock to party Access Automatically enable for repositories added to secret scanning Add aresource link in the CLI and web UI when a commit is blocked Disable all Enable all Disable all Add aresource link in the CLI and web UI when a commit is blocked Disable all Enable all) Packages			
Projects Foreidets] Pages	GitHub Advanced Security GitHub Advanced Security features are billed per active committer in private and internal reportionies. Th	Disable all	Enable all
ecurity Lutomatically enable for new private and Internal repositories Authentication security Code security and analysis Code s	Projects	features are free of charge in public repositories. Learn more about GitHub Advanced Security.		
Authentication security Authentication security Code security and analysis Code security analysis Code security analysis Code security analysis Code security	Murity	Automatically enable for new private and internal repositories		
	Authentication security	Secret scenning	Disable of	Fachin ell
O Verified and approved domains Automatically enable for new public and Advanced Security repositories O Verified and approved domains Push protection Push protection Push protection Nird-party Access Push contain secrets. Learn more about push protection. Disable all Enable all 8 OAuth application policy Add a resource link in the CLI and web UI when a commit is blocked Push protection Enable all <td>Code security and analysis</td> <td>Receive alerts for detected secrets, keys, or other tokens.</td> <td>L/Isable all</td> <td>Enable all</td>	Code security and analysis	Receive alerts for detected secrets, keys, or other tokens.	L/Isable all	Enable all
Secrets Push protection Disable all Enable all Mrd-party Access Block commits that contain secrets. Learn more about push protection. Disable all Enable all & OAuth application policy Indumnatically enable for repositories added to secret scanning Add a resource link in the CLI and web UI when a commit is blocked Enable all	Verified and approved doma	Automatically enable for new public and Advanced Security repositories		
Push protection Disable all Enable all Block commits that contain secrets. Learn more about push protection. Disable all Enable all North Application policy Automatically enable for repositories added to secret scanning Enable all Enable all OltHub Apps Add a resource link in the CLI and web UI when a commit is blocked Disable all Enable all	Secrets			
hird-party Access Block commits that contain secrets. Learn more about push protection. 8 OALth application policy Automatically enable for repositories added to secret scanning 9 Qithub Apps Add a resource link in the CLI and web UI when a commit is blocked Despond acress tokens Add a resource link in the CLI and web UI when a commit is blocked	5 000100	Push protection	Disable all	Enable all
OAuth application policy Automatically enable for repositories added to secret scanning Of GitHub Apps Add a resource link in the CLI and web UI when a commit is blocked	hird-party Access	Block commits that contain secrets. Learn more about push protection.		
GRHub Apps Add a resource link in the CLI and web UI when a commit is blocked	8 OAuth application policy	Automatically enable for repositories added to secret scanning		
Derennal access trikens	GitHub Apps	Add a resource link in the CLI and web UI when a commit is blocked		
Custom patterns	Personal access tokens	Custom patterns		New pattern

2. In **Settings**, click on **Code security and analysis** located under **Security** in the left-side menu panel.

3. Proceed to enable the following:

- <u>Dependency graph</u> (also enable: **Automatically** enable for new private repositories).
- <u>Dependabot alerts</u> (also enable: **Automatically** enable for new private repositories).
- <u>GitHub Advanced Security</u> (also enable: Automatically enable for new private and internal repositories).
- <u>Secret scanning</u> (also enable: Automatically enable for new public and Advanced Security repositories).

Please note: It's not recommended that you enable any of the following during the start of your implementation:

- 4. Dependabot security updates. Enabling this setting will allow Dependabot to open pull requests automatically to resolve Dependabot alerts. This is one of Dependabot's great features, but right now, if Dependabot finds 100 vulnerable dependencies, it will automatically open 100 pull requests. This is not the case if Dependabot alerts are enabled while Dependabot security updates are disabled.
- 5. <u>Push protection.</u> This feature will block commits that contain secrets. For the start of your implementation, we advise not to enable it as this could disrupt your developers by preventing them from pushing their changes into GitHub if a secret is identified within their push to GitHub.

GitHub Advanced Security – repository level

When you enable GitHub Advanced Security at the repository level, you can secure the code in your public repositories. Note that dependency graph and secret

scanning are permanently enabled. The following steps address configuring and managing security features to meet your repo's specific requirements.

- 1. Within the organization where you have enabled GitHub Advanced Security access any of the repositories you selected for this implementation.
- 2. Within the repository, click on **Settings** from the navigation bar.
- 3. Within the repository's **Settings**, click on **Code security and analysis** located under **Security** in the left-side menu panel.
- 4. Validate that only the following settings are enabled:
 - Dependency graph
 - Dependabot alerts
 - <u>GitHub Advanced Security</u>
 - <u>Code scanning</u> (you will see the option to set it up, which will be covered in this guide)
 - <u>Secret scanning</u>



Configuring code scanning

Setting up <u>CodeQL</u> – compiled and interpreted languages

- 1. Within your repository, proceed on accessing the **Security** tab.
- 2. In the **Security** tab, access **Code scanning** and click on **Configure scanning tool**.

To help get started with CodeQL, we've created this walkthrough

video for reference.

③ Overview			
Reporting Policy O Advisories	O Automatically detect vulnerabilities in your code.		
Vulnerability alerts 라 Dependabot	Configure consultatione account code scanning to keep the quality of your code under control, cearn more accounting.		
Ode scanning Ode scanning			
Secret scanning			
Detadama Secola D			

- 3. Once completed, you will be redirected to edit CodeQL YAML's configuration file. Within that file, you will have the ability to:
 - Change its trigger by changing lines 14 to 21.
 - Add or remove languages on the repository to be scanned by updating line 35.
 - Enable CodeQL's extended security query packs by uncommenting line 53.
 - Customize any setting needed. For details please refer to the following: <u>Configuring code scanning -</u> <u>GitHub Docs</u>

Note: For one of your repositories, we recommend uncommenting line 53 and committing the file to initialize CodeQL on your repository. 4. After reviewing, updating, or changing CodeQL's YAML configuration file, you can proceed with committing the file by clicking on **Start commit** on the top-right corner of your screen.



- 5. Once you have committed CodeQL's YAML file, proceed to access the **Actions** tab.
- 6. Within the Actions tab, you will see a job being executed. This is CodeQL starting to scan your repository for vulnerabilities. Once completed, it will upload the results. The results are located under the Security tab > Code scanning. Keep in mind that CodeQL must execute its job before it can upload any results.

Example: The screenshot below is an example of how vulnerabilities will be displayed in code scanning under the **Security** tab if your repo contains any vulnerability that has been identified by CodeQL.



Note: If you do not see any results after configuring CodeQL and allowing it to complete its scan, contact your GitHub account manager so that we can provide you with further assistance during your implementation.

- 7. In the scenario that you are using a repository where the majority of code is made up of a compiled language, please proceed with configuring code scanning following the steps above. If there is an error or a failure due to CodeQL's auto-builder being unable to build your applilcation, you will need to proceed with the following:
 - Create a bash or PowerShell script file to build your application and upload it to your repository.
 - Once done, you will need to modify CodeQL's YAML file. Comment out lines 58-59 and uncomment lines 67-69. In line 69, you will need to specify the location wihtin the repository of your build script so your application can be successfully built and scanned.
 - After you have completed all the changes needed, proceed with committing the file to initiate CodeQL's execution.

Secret scanning

Understanding secret scanning

GitHub Advanced Security's secret scanning is a targeted search based on a regular expression. Any strings that match patterns provided by secret scanning partners, by other service providers, or defined by your organization, are reported as alerts in the **Security** tab of repositories. To view the list of our partners to know which secrets we can identify natively, please review the following: <u>Secret</u> <u>scanning patterns – GitHub Docs</u>

In the scenario that your secrets are created in-house or you are generating secrets using a vendor that is not natively supported, you can add support for it by adding a custom pattern so that secret scanning can detect it. <u>Defining custom patterns for secret scanning – GitHub</u> <u>Enterprise Cloud Docs</u>

Secret scanning can either be enabled at the <u>organizational level</u> (recommended) or at the <u>repository</u> <u>level</u>. At this point in the guide, you have already enabled secret scanning at the organizational level by following the steps detailed on <u>Page 4</u>. Secret scanning requires no additional configuration, and it will automatically surface any secrets it identifies.

Secrets found can be seen either in specific repositories or at the organizational level.

Organizational level: Access the Organization> Security> Secret scanning

(i) Risk (Beta)		Secret scanning alerts Give us feedback	
Coverage (Beta)		Q is:open	
Vulnerability alerts			
👜 Dependabot	5,000+	① 1,247 Open 🗸 402 Closed	Repository - Secret type - Provider - Sort -
O Code scanning	5,000+		0 000 0-0
Secret scanning	1,247	Stripe API Key sk_live_abcdefghijklmnopqr_ Opened 3 hours ago - Detected secret in .gitignore:25	A OX2-Den
		③ Google API Key AIzaSyAQfxPJiounkh0j0DE057	A OX2-Dem
		Opened 3 hours ago - Detected secret in src//service/BookServiceTest.java:18	
		Ostripe API Key sk_live_abcdefghijklmnopqr_ Opened 3 hours ago • Detected secret in .gitignore:25	A OX2-Dem
		Amazon AWS Secret Access Key lscdYBApxrLWL0HKuVqVXWv3ou_ Opened 4 hours ago • Detected secret in homeassistant//cloud/const.py:12	♀ home-assistant-co
		Amazon AWS Access Key ID AKIAJGRK7MILPRJTT2ZQ Opened 4 hours ago • Detected secret in homeassistant//cloud/const.py:11	😵 home-assistant-co
		mcantu pattern my_secret_pattern_123 Onened vesterday. Detected custom pattern in secrets vml/1	€ dependency-review-testin

Repository level:

Access any repository within your **Organization**> **Security**> **Secret scanning**

③ Overview	Secret scanning alerts	
Reporting	Q is:open	
 Advisories 	□ ③ 3 Open ✓ 2 Closed	Secret type - Provider - Sort -
ulnerability alerts ت Dependabot 63	 Google API Key AIzaSyAxbaV6EvWYzKts=FRJf7_ #10 opened last month • Detected secret in Dockerfile:35 	
බු Code scanning 400	□ ① find jdbc.passwords jdbc.password	

Security overview

<u>Understanding the security</u> <u>overview – organizational level.</u>

Organization owners and security managers can access the security overview for organizations and view their organization's repositories via the enterprise-level security overview. Enterprise owners can use the enterprise-level security overview to view all repositories in their enterprise's organizations. Members of a team can see the security overview for repositories that the team has admin privileges for.

You can use the security overview for a high-level view of the security status of your organization or identify problematic repositories that require intervention. You can view aggregate or repository-specific security information in the security overview. You can also use the security overview to see which security features are enabled for your repositories and to configure any available security features that are not currently in use.

Example: The screenshot below will provide an example of the information you can see from the security overview.

Security		Security risk			Give feedback (Bet	
① Risk	Beta	Alert counts for security features in repositories act	ross the organization			
@ Coverage	Beta	Q Search	Q Search			
Alerts Dependabot O Code scanning Secret scanning	5,000+ 5,000+ 1,307	Dependabot 42% of repositories affected Repositories 726 affected 961 unaffected Open alerts	Code scanning 27% of repositories affected Repositories 461 affected 1,246 Open alerts	sunaffected 443 0	ret scanning % of repositories affected sitories affected 1,264 unaffected allerts	
		2,413 low Mean Time To Resolve (days) 50	1,413 low 61,973 in	formational Mean	n Time To Resolve (days) 67 Sort -	
		mixpix3Is-ketchup-clinic (Private) Updated 6 minutes ago	Dependabot 7	Code scanning	Secret scanning	
		colinbeales-ghas-demo (Private) Updated 13 minutes ago	Dependabot	Code scanning	Secret scanning	
		J18-Demo2 (Private) Updated 1 hour ago	Dependabot	Code scanning 65	Secret scanning	
		chef-clone Internal	Dependabot	Code scanning	Secret scanning	

GitHub Advanced Security licensing model

Licenses for GitHub Advanced Security are based on an active committer model. A committer is considered active if one of their commits has been pushed to a private or internal repository within the last 90 days, regardless of when it was originally authored

How does it work?



Code is committed or pushed to GitHub

Usage is measured across the whole enterprise account to ensure that each member uses one seat regardless of how many repositories or organizations the user contributes to.



Any user who makes a commit or push to a private or internal repository where GitHub Advanced Security is enabled will consume a license based on a 90-day period.



When you remove a user from your enterprise account, the user's license is freed within 24 hours.



Learn more at <u>github.com/learn/security</u> or contact our <u>Sales Team</u>

WRITTEN BY GITHUB WITH