Question #1 *Topic 1*

A secret scanning alert should be closed as “used in tests” when a secret is:

A. in a test file.

B. solely used for tests.

C. in the readme.md file.

D. not a secret in the production environment.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

What happens when you enable secret scanning on a private repository?

A. Repository administrators can view Dependabot alerts.

B. Dependency review, secret scanning, and code scanning are enabled.

C. Your team is subscribed to security alerts.

D. GitHub performs a read-only analysis on the repository.

Suggested Answer: *D*

Community vote distribution

D (100%)

tdkc 2 months, 2 weeks ago

Selected Answer: D

A is Incorrect. Enabling secret scanning does not automatically enable Dependabot alerts (a separate feature for vulnerable dependencies). When you enable secret scanning on a private repository (which requires GitHub Advanced Security), several actions occur, one of them is an Immediate Historical Scan: GitHub immediately initiates a scan of the entire Git history across all branches in the repository for known secret patterns.

Answer should be D. GitHub performs a read-only analysis on the repository.

upvoted 3 times

Question #3 *Topic 1*

Which of the following statements best describes secret scanning push protection?

A. Buttons for sensitive actions in the GitHub UI are disabled.

B. Commits that contain secrets are blocked before code is added to the repository.

C. Users need to reply to a 2FA challenge before any push events.

D. Secret scanning alerts must be closed before a branch can be merged into the repository.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

What is a security policy?

A. a security alert issued to a community in response to a vulnerability

B. a file in a GitHub repository that provides instructions to users about how to report a security vulnerability

C. an alert about dependencies that are known to contain security vulnerabilities

D. an automatic detection of security vulnerabilities and coding errors in new or modified code

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Which of the following information can be found in a repository's Security tab?

A. number of alerts per GHAS feature

B. GHAS settings

C. access management

D. two-factor authentication (2FA) options

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Which of the following benefits do code scanning, secret scanning, and dependency review provide?

A. Automatically raise pull requests, which reduces your exposure to older versions of dependencies.

B. View alerts about dependencies that are known to contain security vulnerabilities.

C. Search for potential security vulnerabilities, detect secrets, and show the full impact of changes to dependencies.

D. Confidentially report security vulnerabilities and privately discuss and fix security vulnerabilities in your repository's code.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Which alerts do you see in the repository's Security tab? Each answer presents part of the solution. (Choose three.)

A. secret scanning alerts

B. Dependabot alerts

C. code scanning alerts

D. security status alerts

E. repository permissions

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

A dependency has a known vulnerability. What does the warning message include?

A. an easily understandable visualization of dependency change

B. a brief description of the vulnerability

C. how many projects use these components

D. the security impact of these changes

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Which features require GitHub Advanced Security to be enabled for internal and private repositories in an organization? Each correct answer presents part of the solution. (Choose two.)

A. security policy

B. secret scanning

C. packages

D. dependency review

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which of the following is the best way to dispose of a compromised secret?

A. Create a new secret.

B. Revoke the secret.

C. Update any services that use the secret.

D. Remove the secret from the code base.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Assuming that no custom patterns are configured, what type of secret is detected by secret scanning?

A. usernames

B. sealed boxes

C. Personal Identifiable Information (PII)

D. private keys

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

What is the best method to ensure all new code is scanned for vulnerabilities?

A. Add the extended suite.

B. Configure code scanning.

C. Set up a security policy.

D. Configure code owners.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 2*

What is the first step you should take to fix an alert in secret scanning?

A. Remove the secret in a commit to the main branch.

B. Archive the repository.

C. Update your dependencies.

D. Revoke the alert if the secret is still valid.

Suggested Answer: *D*

Community vote distribution

A (100%)

ziggy1117 2 months ago

Selected Answer: A

A. Remove the secret in a commit to the main branch.

We first need to ensure the secret is no longer in the main branch.

D is incorrect because we need to revoke the secret NOT revoke the alert

upvoted 1 times

Question #2 *Topic 2*

Where in the repository can you give additional users access to secret scanning alerts?

A. Secrets

B. Insights

C. Settings

D. Security

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 2*

What filter or sort settings can be used to prioritize the secret scanning alerts that present the most risk?

A. Sort to display the oldest first.

B. Filter to display active secrets.

C. Select only the custom patterns.

D. Sort to display the newest first.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 2*

Which of the following secret scanning features can verify whether a secret is still active?

A. branch protection

B. validity checks

C. push protection

D. custom patterns

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 2*

What is a prerequisite to define a custom pattern for a repository?

A. Change the repository visibility to Internal.

B. Enable secret scanning.

C. Close other secret scanning alerts.

D. Specify additional match criteria.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 2*

Assuming security and analysis features are not configured at the repository, organization, or enterprise level, secret scanning is enabled on:

A. private repositories.

B. all new repositories within your organization.

C. public repositories.

D. user-owned private repositories.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 2*

Which patterns are secret scanning validity checks available to?

A. high entropy strings

B. custom patterns

C. push protection patterns

D. partner patterns

Suggested Answer: *B*

Community vote distribution

D (100%)

neophantom 4 months ago

Selected Answer: D

D should be correct answer

upvoted 3 times

Question #8 *Topic 2*

What role is required to change a repository's code scanning severity threshold that fails a pull request status check?

A. Maintain

B. Write

C. Admin

D. Triage

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 2*

What YAML syntax do you use to exclude certain files from secret scanning?

A. paths-ignore:

B. secret_scanning.yml

C. branches-ignore:

D. decrypt_secret.sh

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 2*

Secret scanning will scan:

A. a continuous integration system.

B. the GitHub repository.

C. any Git repository.

D. external services.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 2*

Which of the following features helps to prioritize secret scanning alerts that present an immediate risk?

A. non-provider patterns

B. push protection

C. secret validation

D. custom pattern dry runs

Suggested Answer: *C*

Community vote distribution

C (100%)

0a9a335 2 months ago

Selected Answer: C

Secret validation helps prioritize secret scanning alerts by checking whether a detected secret is still active (i.e., valid and in use). This allows teams to focus on alerts that present an immediate risk, as only active secrets can be exploited.

upvoted 1 times

tdkc 2 months, 2 weeks ago

Selected Answer: C

C Secret Validation. Validity checks help you prioritize alerts by automatically indicating if a detected secret is still active or inactive (invalidated) by communicating with the issuing service provider (for supported partner patterns). The reason validity checks are the correct feature to help prioritize existing secret scanning alerts (those already exposed in the history or present in the codebase) over push protection is based purely on their intended function.

upvoted 2 times

Question #12 *Topic 2*

What do you need to do before you can define a custom pattern for a repository?

A. Add a secret scanning custom pattern.

B. Provide match requirements for the secret format.

C. Enable secret scanning on the repository.

D. Provide a regular expression for the format of your secret pattern

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 2*

Which of the following statements most accurately describes push protection for secret scanning custom patterns?

A. Push protection is enabled by default for new custom patterns.

B. Push protection must be enabled for all, or none, of a repository's custom patterns.

C. Push protection is not available for custom patterns.

D. Push protection is an opt-in experience for each custom pattern.

Suggested Answer: *D*

Community vote distribution

D (100%)

tdkc 2 months, 2 weeks ago

Selected Answer: D

It cannot be B because it says ..., or none, ...

The most accurate is D. To enable push protection for secret scanning custom patterns in GitHub Advanced Security (GHAS), you must first ensure that generic secret scanning and push protection are generally enabled for the repository, organization, or enterprise. Once the base features are enabled, push protection is an opt-in experience for each custom pattern.

upvoted 3 times

Question #14 *Topic 2*

Which details do you have to provide to create a custom pattern for secret scanning? Each answer presents part of the solution. (Choose two.)

A. the secret format

B. a list of repositories to scan

C. the name of the pattern

D. additional match requirements for the secret format

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 2*

After defining a secret scanning custom pattern, what is the final step before publishing the pattern?

A. defining a custom pattern

B. adding additional match requirements

C. enabling push protection

D. performing a dry run

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 2*

Secret scanning will ignore a secret_scanning.yml file that

A. contains 1,000 or more entries.

B. has 1,000 or more directories

C. is 1 MB or larger

D. is 100 KB or larger.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 2*

By default, what is the minimum role needed to bypass push protection in a repository?

A. Maintain

B. Admin

C. Triage

D. Write

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 2*

By default, who will receive an e-mail when a secret has been detected in a repository? Each answer presents a complete solution. (Choose two.)

A. users with the Maintain repository role

B. user who committed the secret

C. users with the Write repository role

D. users with the Admin repository role

E. security analyst

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 2*

Which of the following is the most proactive and practical way to prevent new secret scanning alerts?

A. Scan for non-provider patterns

B. Use feature branches

C. Configure a secret scanning Actions workflow.

D. Enable push protection.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 2*

By default, where will secret scanning look in a repository in order to execute its job? Each correct answer presents part of the solution. (Choose three.)

A. all files in the repository

B. dependencies

C. selected files in the repository

D. full commit history

E. all branches

Suggested Answer: *CDE*

Community vote distribution

ADE (100%)

ziggy1117 2 months ago

Selected Answer: ADE

A. all files in the repository

D. full commit history

E. all branches

By default it will look at all files. You can specify which files or directories secret scanning should ignore (i.e., not scan) by creating a .github/secret_scanning.yml file in your repository with a paths-ignore setting. But its not the default way

upvoted 1 times

Question #21 *Topic 2*

Which of the following would raise secret scanning alerts?

A. GitHub personal access token

B. server-side request forgery

C. cross site scripting (XSS)

D. structured query language (SQL) injection

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 2*

What is the purpose of push protection?

A. to scan and block the code that contains vulnerabilities before it reaches the repository

B. to validate the push by the code owner

C. to define license requirements for the repository

D. to scan and block the code that contains secrets before it reaches the repository

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 2*

Which of the following pre-defined roles is required to manage code scanning alerts in a repository?

A. Maintain

B. View

C. Read

D. Triage

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 2*

Where is secret scanning enabled on a private repository?

A. within a secret.yml file in the repository

B. in the code scanning default set up settings

C. within a repository ruleset

D. in the code security settings

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 3*

Which of the following is the most complete method for Dependabot to find vulnerabilities in third-party dependencies?

A. CodeQL analyzes the code and raises vulnerabilities in third-party dependencies.

B. Dependabot reviews manifest files in the repository.

C. The build tool finds the vulnerable dependencies and calls the Dependabot API.

D. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory database.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 3*

In a private repository, what minimum requirements does GitHub need to generate a dependency graph? (Each answer presents part of the solution. Choose two.)

A. read-only access to all the repository's files

B. dependency graph enabled at the organization level for all new private repositories

C. write access to the dependency manifest and lock files for an enterprise

D. read-only access to the dependency manifest and lock files for a repository

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 3*

You have enabled security updates for a repository. When does GitHub mark a Dependabot alert as resolved for that repository?

A. when you merge a pull request that contains a security update

B. when Dependabot creates a pull request to update dependencies

C. when you dismiss the Dependabot alert

D. when the pull request checks are successful

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 3*

Assuming that notification settings and Dependabot alert recipients have not been customized, which user account setting should you use to get an alert when a vulnerability is detected in one of your repositories?

A. enable all in existing repositories

B. enable all for Dependabot alerts

C. enable all for Dependency graph

D. enable by default for new public repositories

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 3*

What are Dependabot security updates?

A. compatibility scores to let you know whether updating a dependency could cause breaking changes to your project

B. automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities

C. automated pull requests to update the manifest to the latest version of the dependency

D. automated pull requests that help you update dependencies that have known vulnerabilities

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 3*

Which of the following Watch settings could you use to get Dependabot alert notifications? Each answer presents part of the solution. (Choose two.)

A. the Participating and @mentions setting

B. the Custom setting

C. the Ignore setting

D. the All Activity setting

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 3*

If default code security settings have not been changed at the repository, organization, or enterprise level, which repositories receive Dependabot alerts?

A. private repositories

B. none

C. repositories owned by an organization

D. repositories owned by an enterprise account

Suggested Answer: *B*

Community vote distribution

C (100%)

0a9a335 1 month, 4 weeks ago

Selected Answer: C

By default, if no changes have been made to the code security settings, Dependabot alerts are enabled for repositories owned by an organization. Private repositories and enterprise accounts do not receive Dependabot alerts by default unless explicitly configured.

upvoted 1 times

Question #8 *Topic 3*

Who can fix a code scanning alert on a private repository?

A. users who have the security manager role within the repository

B. users who have Write access to the repository

C. users who have the Triage role within the repository

D. users who have Read permissions within the repository

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 3*

Assuming that no custom Dependabot behavior is configured, who has the ability to merge a pull request created via Dependabot security updates?

A. a repository member of an enterprise organization

B. an enterprise administrator

C. a user who has read access to the repository

D. a user who has write access to the repository

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 3*

Which key is required in the update settings of the Dependabot configuration file?

A. commit-message

B. package-ecosystem

C. assignees

D. rebase-strategy

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 3*

Where can you find a deleted line of code that contained a secret value?

A. Issues

B. Dependency graph

C. Commits

D. Insights

Suggested Answer: *B*

Community vote distribution

C (100%)

ivantsanev 2 months, 1 week ago

Selected Answer: C

I this should be C. Finding files changes can be easily seen in Commits tab.

upvoted 2 times

Question #12 *Topic 3*

Which security feature shows a vulnerable dependency in a pull request?

A. dependency review

B. dependency graph

C. Dependabot alert

D. the repository's Security tab

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 3*

What should you do after receiving an alert about a dependency added in a pull request?

A. Disable Dependabot alerts for all repositories owned by your organization.

B. Fork the branch and deploy the new fork.

C. Deploy the code to your default branch.

D. Update the vulnerable dependencies before the branch is merged.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 3*

Assuming that notification and alert recipients are not customized, what does GitHub do when it identifies a vulnerable dependency in a repository where Dependabot alerts are enabled? (Each answer presents part of the solution. Choose two.)

A. It generates a Dependabot alert and displays it on the Security tab for the repository.

B. It consults with a security service and conducts a thorough vulnerability review.

C. It generates Dependabot alerts by default for all private repositories.

D. It notifies the repository administrators about the new alert.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

0a9a335 1 month, 4 weeks ago

Selected Answer: AD

When GitHub identifies a vulnerable dependency in a repository where Dependabot alerts are enabled, it:

Generates a Dependabot alert and displays it on the Security tab of the repository.
Sends a notification to repository administrators about the new alert.

upvoted 1 times

Question #15 *Topic 3*

Which of the following workflow events would trigger a dependency review? (Each answer presents a complete solution. Choose two.)

A. commit

B. trigger

C. workflow_dispatch

D. pull_request

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 3*

A repository's dependency graph includes:

A. annotated code scanning alerts from your repository's dependencies.

B. dependencies from all your repositories.

C. a summary of the dependencies used in your organization's repositories.

D. dependencies parsed from a repository's manifest and lock files.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 3*

Assuming there is no custom Dependabot behavior configured, where possible, what does Dependabot do after sending an alert about a vulnerable dependency in a repository?

A. scans repositories for vulnerable dependencies on a schedule and adds those files to a manifest

B. scans any push to all branches and generates an alert for each vulnerable repository

C. creates a pull request to upgrade the vulnerable dependency to the minimum possible secure version

D. constructs a graph of all the repository's dependencies and public dependents for the default branch

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 3*

How many alerts are created when two instances of the same secret value are in the same repository?

A. 4

B. 2

C. 3

D. 1

Suggested Answer: *D*

Community vote distribution

B (100%)

guhancse 2 weeks ago

Selected Answer: B

It should be Option B. 2 alerts.

upvoted 1 times

Question #19 *Topic 3*

In the pull request, how can developers avoid adding new dependencies with known vulnerabilities?

A. Enable Dependabot security updates.

B. Add Dependabot rules.

C. Enable Dependabot alerts.

D. Add a workflow with the dependency review action.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 3*

If notification and alert recipients are not customized, which users receive notifications about new Dependabot alerts in an affected repository?

A. users with Maintain privileges to the repository

B. users with Read permissions to the repository

C. users with Write permissions to the repository

D. users with Admin privileges to the repository

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!