Vendor: Microsoft

Exam Code: GH-500

Exam Name: GitHub Actions

Version: DEMO

QUESTION 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.

Answer: B
Explanation:
If a secret is intentionally used in a test environment and poses no real-world security risk, you may close the alert with the reason"used in tests". This helps reduce noise and clarify that the alert was reviewed and accepted as non-critical.

Just being in a test file isn't enough unless itspurpose is purely for testing.

If a secret is intentionally used in a test environment and poses no real-world security risk, you may close the alert with the reason"used in tests". This helps reduce noise and clarify that the alert was reviewed and accepted as non-critical.

Just being in a test file isn't enough unless itspurpose is purely for testing.

QUESTION 2
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.

Answer: A
Explanation:
GitHub secret scanning detects and alerts on sensitive data exposure, such as API keys and credentials, in your code repositories. Use it to protect your secrets, ensure secure and compliant development practices, and reduce the risk of data breaches and unauthorized access.

GitHub has scanned public repositories for secrets (like API keys and tokens) for several years. Secret scanning protects our partners and our customers from unauthorized use of the services protected by those secrets. Just this month, 8% of active GitHub repositories committed a secret that was caught by secret scanning.

At GitHub Satellite, we announced secret scanning for private repositories, part of GitHub Advanced Security. We’re bringing the same lightning-fast scanning engine and broad set of 24 partners (including all the major cloud providers and many common SaaS providers) to your private repository, so you can catch secrets as soon as they’re checked in. Repository admins will be notified about any commit that contains a secret, and can quickly view all detected secrets in the repo’s Security tab.

QUESTION 3
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.

Answer: B
Explanation:
Secret scanning push protection is a security feature that prevents sensitive information like API keys or tokens from being pushed to a repository in the first place. It works by proactively scanning code during the push process and blocking any attempts to commit secrets. This differs from regular secret scanning, which only detects secrets after they have been committed.

QUESTION 4
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

Answer: B
Explanation:
Adding a security policy to your repository
You can give instructions for how to report a security vulnerability in your project by adding a security policy to your repository.

About security policies
To give people instructions for reporting security vulnerabilities in your project, you can add a SECURITY.md file to your repository's root, docs, or .github folder. Adding this file to this part(s) of your repository automatically creates a row with a description where people can review it. When someone creates an issue in your repository, they will see a link to your project's security policy.

QUESTION 5
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

Answer: A
Explanation:
You can find security alerts from Dependabot, Secret scanning, and Code scanning under your repository's Security tab. Security alerts for a repository are visible to people with write, maintain, or admin access to the repository and, when the repository is owned by an organization, organization owners.

QUESTION 6
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.

Answer: C

QUESTION 7
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

Answer: ABC
Explanation:
You can find security alerts from Dependabot, Secret scanning, and Code scanning under your repository's Security tab.

QUESTION 8
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

Answer: B
Explanation:
Where a dependency has a known vulnerability, the warning message includes:
A brief description of the vulnerability.

A Common Vulnerabilities and Exposures (CVE) or GitHub Security Advisories (GHSA) identification number. You can click this ID to find out more about the vulnerability.

The severity of the vulnerability.

The version of the dependency in which the vulnerability was fixed. If you are reviewing a pull request for someone, you might ask the contributor to update the dependency to the patched version, or a later release.

QUESTION 9
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

Answer: BD
Explanation:
About GitHub Advanced Security products
GitHub has many features that help you improve and maintain the quality of your code. Some of these are included in all plans, such as dependency graph and Dependabot alerts.

Other security features require you to purchase one of GitHub's Advanced Security products:

GitHub Secret Protection, which includes features that help you detect and prevent secret leaks, such as secret scanning [B] and push protection.

GitHub Code Security, which includes features that help you find and fix vulnerabilities, like code scanning, premium Dependabot features, and dependency review [D].

QUESTION 10
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.

Answer: B
Explanation:
Remediating a leaked secret in your repository

Revoke the secret
It is not sufficient to simply remove the secret from your codebase. The most important remediation step is revoking the secret with the secret's provider. By revoking the secret, you drastically reduce the potential for the secret to be exploited.

Note:
You should consider any leaked secret to be immediately compromised and it is essential that you undertake proper remediation steps, such as revoking the secret. Simply removing the secret from the codebase, pushing a new commit, or deleting and recreating the repository do not prevent the secret from being exploited.

QUESTION 11
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

Answer: D
Explanation:
GitHub secret scanning detects and alerts on sensitive data exposure, such as API keys and credentials, in your code repositories.

QUESTION 12
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.

Answer: B
Explanation:
Configuring automated code scanning integrated into a CI/CD pipeline is the best method to ensure new code is scanned for vulnerabilities because it identifies weaknesses early in the development lifecycle, preventing them from reaching production. This approach provides continuous, hands-off scanning as code is committed or merged, offering immediate feedback to developers and reducing the cost of fixing issues.

QUESTION 13
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.

Answer: D
Explanation:
Resolving alerts from secret scanning
After reviewing the details of a secret scanning alert, you should fix and then close the alert.

Fixing alerts
Once a secret has been committed to a repository, you should consider the secret compromised. GitHub recommends the following actions for compromised secrets:

Verify that the secret committed to GitHub is valid.
Review and update any services that use the old token. For GitHub personal access tokens, delete the compromised token and create a new token.
Depending on the secret provider, check your security logs for any unauthorized activity.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**