SANS OnDemand

SEC540: Cloud Security & DevSecOps Automation (H01_07_CM_8750)

Ask a Question | Notifications (1)

You passed the quiz!
You needed 80% (16 correct answers)
You scored

80%

Question 1 of 20 Correct

When running static analysis scans in a continuous delivery pipeline, what should be done for noisy, low-confidence checks?

Keep them in the pipeline for consistency.

Disable them completely and contact vendor support.

Improve the checks to get rid of negative results.

✔ **Run them separately and review them manually.**

Explanation

Developers will tune out results if you do not tune out false positives. Run them separately and review/qualify them manually. Feed real positive findings back to the development team's backlog.

Question 2 of 20 Correct

In which DevOps workflow phase are container security controls implemented?

Acceptance phase

✔ **Commit phase**

Container security controls are out of the scope of DevOps workflow.

Pre-commit phase

Explanation

The Commit/Continuous Integration stage, where the code is built and initial checks are done, is the best place to implement security checks such as static analysis testing (SAST) in CI, checking open-source/third-party software dependencies/libraries for vulnerabilities, and unit testing. Container security controls are implemented in this phase.

Question 3 of 20 Incorrect

With regards to secrets management, what is a security consideration when comparing GitLab CI/CD with GitHub Actions?

GitLab CI/CD has no native secrets management and relies on third-party secrets management, such as HashiCorp Vault.

✗ **GitLab CI/CD uses libsodium sealed boxes called environment secrets, while GitHub Actions has built in Azure Key Vault secrets manager.**

GitHub Actions has no native secrets management and relies on third-party secrets management, such as HashiCorp Vault.

Both GitLab CI/CD and GitHub Actions include a built-in AWS Secrets Manager to manage secrets.

Explanation

GitLab does not support secrets natively inside GitLab CI/CD. Instead, GitLab has an integration available for HashiCorp Vault. Each GitLab CI/CD job has a unique, signed JSON Web Token (JWT) that can be used to authenticate to a Vault instance.
GitHub Actions has built-in support for secrets scoped to the entire organization or an individual repository. Repository administrators can set one-to-many secret values, which are encrypted in libsodium sealed boxes until they are consumed by a workflow.

Question 4 of 20 Correct

What is an advantage of a distributed version control system (DVCS) over other version control systems?

DVCS eliminated merging conflicts.

DVCS introduced the notion of a repository-wide version identifier.

✔ **DVCS allows developers to share patches without a central intermediary.**

DVCS replaced reliance on .bak file.

Explanation

Distributed Version Control Systems (DVCS) shift version control from a client-server approach to a peer-to-peer approach. Rather than each client checking out a working copy from the server, in a DVCS environment, each client clones the entire repository to their local system. Because each developer has a full clone of the repository, it is possible to share patches that are based on a common point in the history directly between two developers, without needing to work through a central intermediary.

Question 5 of 20 Correct

Which of the following tools can be used to handle secrets in Chef configuration management tool?

Secrets Vault

Blackbox

✔ **Encrypted Data Bags**

Hiera-Eyaml

Explanation

Encrypted Data Bags are data stores for Chef. Chef Data Bag Items can be encrypted using the public keys of a list of Chef nodes. This allows only those chef nodes to decrypt the encrypted values.

Question 6 of 20 Incorrect

Which of the following is an example of a security code smell?

Hand-rolled crypto

Security libraries

✗ **Embedded product update URL**

Error handling

Explanation

Developers can be easily taught to watch out for security code smells—hardcoded secrets and backdoors, hand-rolled crypto, and suspect code, or code that is obfuscated or unnecessarily confusing.

Question 7 of 20 Correct

What action automatically triggers a pipeline in a Continuous Integration practice?

Random time intervals

Unit tests failing

✓ **Completing a commit on the main branch**

Deployment request

Explanation

Approving and completing a merge request creates a commit on the main branch and automatically triggers a pipeline. The pipeline ensures the changes integrate successfully with the rest of the code base. It also runs through automated unit and other tests to ensure the change does not break the build.

Question 8 of 20 Correct

How does Azure Key Vault handle user authentication?

- ✔ **Azure AD**
- API Keys
- Passwords
- Passphrases

Explanation

With Azure Key Vault, authentication and authorization are required to access the vault. Authentication is performed via Azure Active Directory and authorization is performed via role-based access control (RBAC) for management access or Key Vault access control policy for application access or key retrieval.

Question 9 of 20 Correct

What does the C stand for in the DevOps CAMS model?

Collaboration

✔ **Culture**

Cloud

Continuous

Explanation

The CAMS model acronym stands for the following:

• Culture: Start with people, build on Agile values, create an open working environment where people feel safe and want to solve problems together. Cultural diversity in development and operations is important in DevOps, especially gender equality, as these fields tend to become boys clubs.
• Automation: Automate repetitive work (like testing and deployment), and take advantage of open-source tools as much as possible.
• Measurement: You can't improve what you can't measure. Collect metrics on everything possible. Use this data to drive design and improvements.
• Sharing: Share ideas and information; share problems; share responsibility and accountability across development and operations (and InfoSec).

Question 10 of 20 Correct

Why is it important for security teams to understand the GitFlow option utilized by their organization?

- ✔ **To identify and understand potential weaknesses and secure them**
- To increase transparency in DevOps
- To minimize the need for security gates and rely on security guardrails only
- To satisfy the culture in CAMS/CALMS DevOps principles

Explanation

Understanding GitFlow is important for two reasons. First, security teams contributing to projects will need to learn how to use Git and follow this process. The second reason is equally important: security teams need to understand potential weaknesses attackers may try to exploit in the workflow.

Question 11 of 20 Correct

What is a benefit of an organization adopting a security champions or security mavens program?

Security champions help shield developers from taking responsibility for their own application's security.

Security champions do not require funding and support from upper management.

✔ **Security champions help bridge the gap between central security and the product development team.**

Security champions operate inside of the development teams ensuring they do not try to hide stuff from the central security team.

Explanation

Generally, the central security organization is greatly outnumbered by product development organizations building the applications that need to be secured. In order to scale security, these development teams must practice DevSecOps and take responsibility for their own application's security. Given the need to embed security expertise into the product development organizations, several companies have started security champions programs with the goal of always helping bridge the gap between product development and the central security organization.

Question 12 of 20 Correct

Which of the following GitLab branch protection options creates granular approval rules for individual files or directories in the repository?

- ✔ **Require approval from code owners**
- Allowed to merge
- Require approval from all users
- Allowed to receive

Explanation

CodeOwners creates granular approval rules for individual files or directories in the repository. This GitLab branch protection option requires code owner approval before changes can be merged. Unfortunately, this capability is only supported in the GitLab Premium edition or higher.

Question 13 of 20 Correct

What are the two Amazon AWS general-purpose secrets management solutions?

- Secrets Manager and Prime Parameter Store
- Prime and Secrets Manager
- Amazon EC2 and Key Management Store
- ✔ **Parameter Store and Secrets Manager**

Explanation

Amazon currently offers two mechanisms specifically designed for application secrets management: Secrets Manager and the Parameter Store feature of EC2 Simple Systems Manager. They are very similar, each providing the following: general-purpose application secrets management, secure storage, access control through AWS IAM, secret rotation, and audit trails.

Question 14 of 20 Incorrect

Which of the following HashiCorp Vault secrets engine could be used to temporarily store secrets namespaced to a user token?

Database

TOTP

Cubbyhole

✗ **kv**

Explanation

Cubbyhole secrets engine provides read/write arbitrary secrets, namespaced to a user token. When the token expires or is revoked, its associated cubbyhole is destroyed. Unlike kv, it is not possible to read into another token's cubbyhole, even as the root user.

Question 15 of 20 Incorrect

Which of the following is a common lean engineering workflow management technique that improves efficiency, reduces friction, and eliminates hand-offs and delays?

Waterfall

✗ **Value stream mapping**

Automation

Kanban

Explanation

Kanban is a technique that teams use to make their work visible, keep track of their work, and to pull from a just-in-time queue when needed. It allows a team to limit the amount of work they are working on since it is visible to the whole team.

Question 16 of 20 Correct

Which of the following tools can be used to prevent secrets from being committed to Git code repos?

- ✔ **Talisman**
- Git-all-secrets
- GitRob
- TruffleHog

Explanation

Talisman, from ThoughtWorks, is a tool used to validate code changes to be pushed out of a local Git repository on a developer's workstation. By hooking into the pre-push hook provided by Git, it validates the outgoing changeset for things that look suspicious—such as potential SSH keys, authorization tokens, private keys, etc.

Question 17 of 20 Correct

What should be in place to successfully integrate a static analysis scan into the CI/CD pipeline?

- Scan for high-risk flaws in a full scan only.
- ✔ **Run high-risk checks early in the pipeline.**
- Have Security team review findings first.
- Trigger a full scan prior to each deployment.

Explanation

In Continuous Integration and Continuous Delivery, the focus of Static Analysis Security Testing (SAST) is not about finding and reviewing all the potential security vulnerabilities existing in the application. Providing fast and clear feedback on a code commit and running high-risk checks early in the pipeline to fail fast, provides the opportunity to get feedback to developers as quickly as possible so that they can fix vulnerabilities right away.

Question 18 of 20 Correct

Which open-source SAST tool provides the ability to quickly write, test, and publish rules written in YAML with grep patterns to identify matches in the parsed AST files?

- Yara
- dnGrep
- Sigma
- ✔ **Semgrep**

Explanation

Semgrep is an open-source SAST tool with the ability to quickly write, test, and publish rules. The Semgrep engine reads rules written in YAML with grep patterns for identifying matches in the parsed AST files. Semgrep also maintains rulesets for the community to use in the Semgrep Registry.

Question 19 of 20 Correct

Which tool can be used for static code analysis that supports automation from the CLI, Docker image, and Github Actions, and supports multiple languages including Java?

- ✔ **Semgrep**
- CodeSniffer
- Brakeman
- ESLint

Explanation

Semgrep is a light-weight solution for static code analysis. It is supports multiple languages including Java, Go, Python, and generic markup. Sempgrep supports automation from the CLI, Docker image, and GitHub Actions. CodeSniffer supports code quality checks for PHP. ESLint is a rules-based code quality checker JavaScript. Brakeman is a security checker for Ruby projects.

Question 20 of 20 Correct

What CI/CD security hardening step can serve as a final step to identify a malicious code from entering a production environment?

- Patch self-hosted CI/CD runners.
- ✔ **Restrict control flow into production using branch protections and gated approvals.**
- Limit service account permissions and long-lived credentials.
- Protect the supply chain with allow lists of trusted actions.

Explanation

Continuous Deployment systems (deploying to production without gates) can allow the most damaging attacks to succeed without human validation. Systems that have a manual step in the production release process, via a branch protection or gated approval process, have one final opportunity to identify a malicious step or piece of code about to enter the production environment.

← Return to Course

Retake