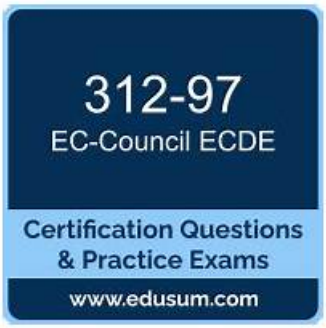
312-97 Prüfungsressourcen: EC-Council Certified DevSecOps Engineer (ECDE) & 312-97 Reale Fragen



2026 Die neuesten ZertPruefung 312-97 PDF-Versionen Prüfungsfragen und 312-97 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=1K5A9_K0oOqqXTOCwlCJyGSWfjVIG4b8T

100% Garantie für 312-97 Zertifizierung EC-Council Certified DevSecOps Engineer (ECDE) Prüfungserfolg. Wenn Sie ZertPruefung 312-97 Prüfung ECCouncil wählen, ist ZertPruefung Test Engine das perfekte Werkzeug, mit dem Sie sich besser auf die Zertifizierungsprüfung vorbereiten. Erfolg kommt einfach, wenn Sie mit Hilfe 312-97 Dumps (EC-Council Certified DevSecOps Engineer (ECDE)) von ZertPruefung nutzen. Falls Sie in der Prüfung durchfallen, geben wir Ihnen eine volle Rückerstattung Ihres Einkaufs.

ECCouncil 312-97 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• DevSecOps Pipeline - Operate and Monitor Stage: This module focuses on securing operational environments and implementing continuous monitoring for security incidents. It covers logging, monitoring, incident response, and SIEM tools for maintaining security visibility and threat identification.
Thema 2	• Introduction to DevSecOps: This module covers foundational DevSecOps concepts, focusing on integrating security into the DevOps lifecycle through automated, collaborative approaches. It introduces key components, tools, and practices while discussing adoption benefits, implementation challenges, and strategies for establishing a security-first culture.
Thema 3	• DevSecOps Pipeline - Release and Deploy Stage: This module explains maintaining security during release and deployment through secure techniques and infrastructure as code security. It covers container security tools, release management, and secure configuration practices for production transitions.

>> 312-97 German <<

312-97 Probesfragen, 312-97 Prüfungsmaterialien

Wir ZertPruefung sind der beste Lieferant von ECCouncil 312-97 Zertifizierungsprüfungen und bieten Ihnen auch echte Prüfungsfragen und Antworten. Die IT-Eliten von ZertPruefung bieten Ihnen Hilfen, damit Sie 312-97 Zertifizierungsprüfung bestehen. Und wir ZertPruefung beinhalten echte Fragen und Antworten in PDF-Versionen. Nach dem Kauf unserer 312-97 Schulungsunterlagen können Sie eine kostlose Aktualisierung bekommen.

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) 312-97 Prüfungsfragen mit Lösungen (Q86-Q91):

86. Frage
(Brett Ryan has been working as a senior DevSecOps engineer in an IT company in Charleston, South Carolina. He is using git-mutimail tool to send email notification for every push to git repository. By default, the tool will send one output email providing details about the reference change and one output email for every new commit due to a reference change. How can Brett ensure that git-multimail is set up appropriately?)

- A. Running the environmental variable GIT_MULTIMAIL_CHECK_SETUP by setting it to non-empty string.
- B. Running the environmental variable GITHUB_MULTIMAIL_CHECK_SETUP by setting it to non- empty string.
- C. Running the environmental variable GITHUB_MULTIMAIL_CHECK_SETUP by setting it to empty string.
- D. Running the environmental variable GIT_MULTIMAIL_CHECK_SETUP by setting it to empty string.

Antwort: A

Begründung:
The git-multimail tool provides a mechanism to verify whether it has been installed and configured correctly before being relied upon for production notifications. This verification is done using an environment variable namedGIT_MULTIMAIL_CHECK_SETUP. When this variable is set to anon-empty string, git-multimail performs a setup validation and outputs diagnostic information toconfirm that configuration values, hooks, and parameters are correctly defined. This helps prevent silent failures where commits occur but email notifications are not sent. Options that referenceGITHUB_MULTIMAIL_CHECK_SETUPare incorrect because git-multimail is not limited to GitHub and does not use that variable name. Additionally, setting the variable to an empty string does not trigger the setup check. Ensuring proper configuration during the Code stage is important because it supports auditability, traceability, and timely communication among development and security teams. Therefore, Brett must run the environment variable GIT_MULTIMAIL_CHECK_SETUPwith a non-empty value to ensure the tool is set up appropriately.
==========

87. Frage
(Debra Aniston is a DevSecOps engineer in an IT company that develops software products and web applications. Her team has found various coding issues in the application code. Debra would like to fix coding issues before they exist. She recommended a DevSecOps tool to the software developer team that highlights bugs and security vulnerabilities with clear remediation guidance, which helps in fixing security issues before the code is committed. Based on the information given, which of the following tools has Debra recommended to the software development team?)

- A. Tenable.io.
- B. SonarLint.
- C. Arachni.
- D. OWASP ZAP.

Antwort: B

Begründung:
SonarLint is a static code analysis tool designed specifically to be used inside developers' IDEs, where it provides immediate feedback while code is being written. It highlights bugs, security vulnerabilities, and code smells and, importantly, providesclear remediation guidancethat explains why an issue exists and how it can be fixed. This aligns directly with Debra's requirement to fix issues "before they exist," meaning before code is committed to the repository. Arachni and OWASP ZAP are dynamic application security testing tools that require a running application and are typically used later in the pipeline. Tenable.io is a vulnerability management platform focused on infrastructure and application scanning rather than real-time developer feedback. By using SonarLint, developers receive continuous guidance during coding, supporting the shift-left security approach in DevSecOps and reducing the cost and effort of fixing vulnerabilities later in the lifecycle.
==========

88. Frage
(Evan Peters has been working as a DevSecOps engineer in an IT company located in Denver, Colorado. His organization has deployed various applications on Docker containers. Evan has been running SSH service inside the containers, and handling of SSH keys and access policies is a major security concern for him. What will be the solution for Evan security concern?)

- A. Run SSH on the client and utilize docker exec for interacting with the container.
- B. Run SSH on the registry and utilize docker exec for interacting with the container.
- C. Run SSH on the docker build and utilize docker exec for interacting with the container.
- D. Run SSH on the host and utilize docker exec for interacting with the container.

Antwort: D

Begründung:
Running an SSH service inside Docker containers is considered a security anti-pattern because it increases the attack surface and complicates key and access management. Containers are designed to run a single primary process and be managed externally rather than accessed via SSH. The recommended solution is torun SSH on the host systemand use docker exec to interact with containers when administrative access is required.
This approach eliminates the need to manage SSH keys inside containers, reduces exposure to brute-force attacks, and simplifies access control. The other options incorrectly suggest running SSH in inappropriate locations such as the registry, client, or build process, which do not address the core security concern. During the Operate and Monitor stage, minimizing unnecessary services within containers is critical to enforcing least privilege and maintaining a secure runtime environment.
==========

89. Frage
(Curtis Morgan is working as a DevSecOps engineer at Orchid Pvt. Ltd. His organization develops online teaching software. Beth McCarthy is working in a software development team, and she requested Curtis to help her in making pre-commit hooks executable on her local machine. Curtis went through the "repo.
git\hooks" directory and removed the ".sample" extension from "pre-commit.sample" file by using "chmod
+x filename" command and made the pre-commit hook executable on Beth's local machine. On the next day while developing the code for the software product, Beth accidentally committed the code with sensitive information. What will be the result of this commit?.)

- A. The script will exit with 3.
- B. The script will exit with 0.
- C. The script will exit with 2.
- D. The script will exit with 1.

Antwort: B

Begründung:
If a pre-commit hook script does not explicitly detect sensitive information or return a non-zero exit code, Git will treat the hook execution as successful. In this scenario, although the hook was made executable, Beth still managed to commit sensitive information. This implies that the hook either did not contain logic to detect such data or did not fail the commit upon detection. As a result, the script exited with0, allowing the commit to proceed. Exit code 0 always signals success to Git, while non-zero exit codes block commits. This highlights the importance of properly implementing security checks within hooks, not just enabling them.
Making a hook executable is necessary, but it must also include correct validation logic to enforce security policies during the Code stage.
==========

90. Frage
(Sandra Oliver joined SinClare Soft Pvt. Ltd. as a DevSecOps engineer in January of 2010. Her organization develops software and web applications related to the healthcare industry. Using IAST runtime security testing technology, she is detecting and diagnosing security issues in applications and APIs. The IAST solution used by Sandra encompasses a web scanner with an agent that works inside the server that hosts the application to provide additional analysis details such as the location of the vulnerability in the application code. Based on the given information, which of the following IAST solutions is Sandra using?)

- A. Passive IAST.

- B. Semi-active IAST.
- C. Active IAST.
- D. Semi-passive IAST.

Antwort: B

Begründung:
Interactive Application Security Testing (IAST) solutions are classified based on how they interact with the application and runtime environment. In this scenario, the solution uses aweb scannerto actively send requests to the application while also deploying anagent inside the application serverto observe runtime behavior and map vulnerabilities directly to source code locations. This combined approach is known assemi- active IAST. It is considered "semi-active" because it actively drives traffic through the application using a scanner, while the agent passively observes execution paths, data flows, and method calls. Passive IAST solutions rely only on observing existing traffic and do not use scanners, while active IAST solutions do not typically rely on deep runtime agents in the same manner. Semi-active IAST significantly reduces false positives and provides precise remediation details, making it highly effective during the Build and Test stage, where applications are actively exercised and security issues can be identified and fixed before release.
═══════

91. Frage
.....

Wie kann man Erfolge erlangen. Es gibt nur eine Ankürzung, nämlich: die Lernhilfe zur ECCouncil 312-97Zertifizierungsprüfung von ZertPruefung zu benutzen. Das ist unser Vorschlag für jeden Kandidaten. Wir hoffen, dass Sie Ihren Traum erfüllen können.