312-97 Online Praxisprüfung & 312-97 Online Test

Außerdem sind jetzt einige Teile dieser It-Pruefung 312-97 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=171kSz0xpq-k4N0Ooylg0XKEd_MLNU35v

Wir versprechen, dass alle Kandidaten, die Shunglungsunterlagen von It-Pruefung benutzt haben, Ihre ECCouncil 312-97 Prüfung 100% bestehen können, ohne Ausnahme. Wenn Sie heute It-Pruefung wählen, fangen Sie dann mit Ihrem Training an. Sie können die nächste ECCouncil 312-97 Zertifizierungsprüfung sicher bestehen und die besten Ressourcen mit der Marktkohärenz und zuverlässiger Garantie bekommen

Die Fragenkataloge zur ECCouncil 312-97 Zertifizierungsprüfung von It-Pruefung sind die besten. Wenn Sie ein ECCouncil -Fachmann sind, sind sie Ihnen ganz notwendig. Sie sind ganz zuverlässig. Wir bieten speziell den 312-97 -Kandidaten die Schulungsunterlagen, die Prüfungsfragen und Antworten zur 312-97 Zertifizierung enthalten. Viele 312-97 -Fachleute streben danach, die ECCouncil 312-97 Prüfung zu bestehen. Die Erfolgsquote von It-Pruefung ist unglaublich hoch. Unser It-Pruefung setzt sich dafür ein, Ihnen zu helfen, den Erfolg zu erlangen.

>> 312-97 Online Praxisprüfung <<

312-97 Pass4sure Dumps & 312-97 Sichere Praxis Dumps

Warum wählen viele Leute die Schulungsunterlagen zur ECCouncil 312-97 Zertifizierungsprüfung von It-Pruefung? Es gibt auch andere Websites, die Schulungsressourcen zur 312-97 Zertifizierungsprüfung bietet. Unser It-Pruefung stellt Ihnen die echten Prüfungsmaterialien zur Verfügung. Unser Eliteteam, Zertifizierungsexperten, Techniker und berühmte Linguisten bearbeiten die

neueste ECCouncil 312-97 Zertifizierungsprüfung. Deshalb klicken Sie It-Pruefung Website, wenn Sie die ECCouncil 312-97 Zertifizierungsprüfung bestehen wollen. Mit It-Pruefung können Sie Ihren Traum Schritt für Schritt verwirklichen.

ECCouncil 312-97 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• DevSecOps Pipeline - Build and Test Stage: This module explores integrating automated security testing into build and testing processes through CI pipelines. It covers SAST and DAST approaches to identify and address vulnerabilities early in development.
Thema 2	• DevSecOps Pipeline - Plan Stage: This module covers the planning phase, emphasizing security requirement identification and threat modeling. It highlights cross-functional collaboration between development, security, and operations teams to ensure alignment with security goals.
Thema 3	• 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 4	• 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.

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) 312-97 Prüfungsfragen mit Lösungen (Q28-Q33):

28. Frage
(Rockmond Dunbar is a senior DevSecOps engineer in a software development company. His organization develops customized software for retail industries. Rockmond would like to avoid setting mount propagation mode to share until it is required because when a volume is mounted in shared mode, it does not limit other containers to mount and modify that volume. If mounted volume is sensitive to changes, then it would be a serious security concern. Which of the following commands should Rockmond run to list out the propagation mode for mounted volumes?.)

- A. docker ps -quiet -all | xargs docker inspect -format ': Propagation='.
- B. docker ps --quiet --all | xargs docker inspect --format ': Propagation='.
- C. docker ps -quiet -all | xargs docker inspect -format ': Propagation'.
- D. docker ps --quiet --all | xargs docker inspect --format ': Propagation'.

Antwort: B

Begründung:
To inspect mount propagation modes for Docker containers, Rockmond needs to list all container IDs and then inspect their configuration. The docker ps --quiet --all command outputs container IDs only, which are then passed to docker inspect using xargs. The --format option allows extraction of specific fields, such as mount propagation settings. Option C correctly uses valid flags (--quiet --all) and proper formatting syntax.
Options A and D incorrectly use single hyphens, and option B omits the equals sign, which is required to display the propagation value. Inspecting mount propagation during the Operate and Monitor stage helps prevent unintended privilege escalation or data modification by other containers, aligning with container hardening best practices.
═══════

29. Frage
(Dustin Hoffman has been working as a DevSecOps engineer in an IT company located in San Diego, California. For detecting new security vulnerabilities at the beginning of the source code development, he would like to integrate Checkmarx SCA tool with GitLab. The Checkmarx template has all the jobs defined for pipeline. Where should Dustin incorporate the Checkmarx template file 'https://raw.githubusercontent.com
/checkmarx-ltd/cx-flow/develop/templates/gitlab/v3/Checkmarx.gitlab-ci.yml'?)

- A. gitlab-cd.yml root directory.
- B. gitlab-ci.yml root directory.
- C. gitlab.yml root directory.
- D. gitlab-ci/cd.yml root directory.

Antwort: B

Begründung:
GitLab CI/CD pipelines are defined using a configuration file namedgitlab-ci.yml, which must be placed in the root directory of the repository. This file controls pipeline stages, jobs, and template inclusions. To integrate Checkmarx SCA using a predefined template, the template reference must be included in the root- level gitlab-ci.yml file so GitLab can load and execute the defined jobs automatically. The other filenames listed in the options are not recognized by GitLab as valid pipeline configuration files. Integrating SCA at the Code stage allows early detection of vulnerable open-source dependencies, reducing remediation cost and preventing insecure components from progressing further in the DevSecOps pipeline.

30. Frage
(Michael Rady recently joined an IT company as a DevSecOps engineer. His organization develops software products and web applications related to online marketing. Michael deployed a web application on Apache server. He would like to safeguard the deployed application from diverse types of web attacks by deploying ModSecurity WAF on Apache server. Which of the following command should Michael run to install ModSecurity WAF?)

- A. sudo apt install libapache2-mod-security2 -x.
- B. sudo apt install libapache2-mod-security2 -y.
- C. sudo apt install libapache2-mod-security2 -w.
- D. sudo apt install libapache2-mod-security2 -z.

Antwort: B

Begründung:
On Debian- and Ubuntu-based systems, ModSecurity for Apache is installed using the package libapache2- mod-security2. The correct command to install this package is sudo apt install libapache2-mod-security2 -y, where the -y flag automatically confirms installation prompts. The other options include invalid flags that are not recognized by the package manager and would result in command failure. Installing ModSecurity during the Operate and Monitor stage provides an additional layer of defense by inspecting incoming HTTP requests and blocking malicious traffic such as SQL injection, cross-site scripting, and protocol violations. A Web Application Firewall helps protect deployed applications from common attack vectors and supports defense- in-depth strategies in production environments.

31. Frage
(Erica Mena has been working as a DevSecOps engineer in an IT company that provides customize software solutions to various clients across United States. To protect serverless and container applications with RASP, she would like to create an Azure container instance using Azure CLI in Microsoft PowerShell. She created the Azure container instance and loaded the container image to it. She then reviewed the deployment of the container instance. Which of the following commands should Erica run to get the logging information from the Azure container instance? (Assume the resource group name as ACI and container name as aci-test- closh.))

- A. az get container logs --resource-group ACI --name aci-test-closh.
- B. az container logs -resource-group ACI -name aci-test-closh.
- C. az container logs --resource-group ACI --name aci-test-closh.
- D. az get container logs -resource-group ACI --name aci-test-closh.

Antwort: C

Begründung:
Azure Container Instances provide built-in logging capabilities that can be accessed using the Azure CLI. To retrieve logs from a deployed container instance, the correct command isaz container logsfollowed by the resource group and container name. The proper syntax requires double-dash parameters:--resource-groupand
--name. In Erica's case, the correct command is az container logs --resource-group ACI --name aci-test-closh.
Options that use "az get container logs" are invalid because "get" is not a supported verb in this context.
Option C uses incorrect single-dash flags, which do not match Azure CLI standards. Accessing container logs during the Code stage

helps engineers validate application behavior, identify runtime errors, and ensure that security instrumentation such as RASP agents are functioning correctly before progressing further in the pipeline.
==========

32. Frage
(Trevor Noah has been working as a DevSecOps engineer in an IT company located in Detroit, Michigan. His team leader asked him to perform continuous threat modeling using ThreatSpec. To do so, Trevor installed and initialized ThreatSpec in the source code repository; he then started annotating the source code with security issues, actions, or concept. Trevor ran ThreatSpec against the application code and he wants to generate the threat model report. Which of the following command Trevor should use to generate the threat model report using ThreatSpec?.)

- A. $ ThreatSpec Report.
- B. $ ThreatSpec report.
- C. $ threatspec report.
- D. $ Threatspec Report.

Antwort: C

Begründung:
ThreatSpec is a command-line tool that follows standard Unix-style conventions, where commands are lowercase. To generate a threat model report after annotating source code, the correct command is threatspec report. Commands using incorrect casing or capitalization will fail because the CLI is case-sensitive. Options A, B, and C incorrectly capitalize either the command or the subcommand. Generating threat model reports during the Plan stage allows DevSecOps teams to continuously identify, document, and visualize security threats as the code evolves. This practice embeds threat modeling directly into the development lifecycle, enabling early risk identification and more secure system design decisions.
==========

33. Frage
.....

Warum wählen viele Leute die Schulungsunterlagen zur ECCouncil 312-97 Zertifizierungsprüfung von It-Pruefung? Es gibt auch andere Websites, die Schulungsressourcen zur 312-97 Zertifizierungsprüfung bietet. Unser It-Pruefung stellt Ihnen die echten Prüfungsmaterialien zur Verfügung. Unser Eliteteam, Zertifizierungsexperten, Techniker und berühmte Linguisten bearbeiten die neueste ECCouncil 312-97 Zertifizierungsprüfung. Deshalb klicken Sie It-Pruefung Website, wenn Sie die ECCouncil 312-97 Zertifizierungsprüfung bestehen wollen. Mit It-Pruefung können Sie Ihren Traum Schritt für Schritt verwirklichen.

312-97 Online Test: https://www.it-pruefung.com/312-97.html

- 312-97 Torrent Anleitung - 312-97 Studienführer - 312-97 wirkliche Prüfung □ Erhalten Sie den kostenlosen Download von □ 312-97 □ mühelos über □ de.fast2test.com □ □312-97 Testengine
- 100% Garantie 312-97 Prüfungserfolg □ Öffnen Sie ✔ www.itzert.com □✔□ geben Sie ▹ 312-97 ◃ ein und erhalten Sie den kostenlosen Download □312-97 Demotesten
- 312-97 Dumps Deutsch □ 312-97 Testfagen □ 312-97 Trainingsunterlagen □ Öffnen Sie die Website ⇛ www.zertpruefung.ch ⇚ Suchen Sie { 312-97 } Kostenloser Download □312-97 Deutsch Prüfung
- 312-97 Musterprüfungsfragen - 312-97Zertifizierung - 312-97Testfagen □ Öffnen Sie die Webseite ➥ www.itzert.com □ □ und suchen Sie nach kostenloser Download von ➡ 312-97 □□□ □312-97 Antworten
- 312-97 Übungstest: EC-Council Certified DevSecOps Engineer (ECDE) - 312-97 Braindumps Prüfung □ Öffnen Sie die Webseite □ www.pass4test.de □ und suchen Sie nach kostenloser Download von □ 312-97 □ □312-97 Deutsche
- 312-97 Torrent Anleitung - 312-97 Studienführer - 312-97 wirkliche Prüfung □ Öffnen Sie die Website ✔ www.itzert.com □✔□ Suchen Sie { 312-97 } Kostenloser Download □312-97 Deutsch
- 312-97 Dumps Deutsch □ 312-97 Simulationsfragen □ 312-97 Prüfungsfrage □ URL kopieren ⇛ www.pruefungfrage.de ⇚ Öffnen und suchen Sie 《 312-97 》 Kostenloser Download □312-97 Deutsch Prüfung
- 100% Garantie 312-97 Prüfungserfolg □ Öffnen Sie ➠ www.itzert.com □ geben Sie ➡ 312-97 □□□ ein und erhalten Sie den kostenlosen Download □312-97 Examengine
- 312-97 Pass Dumps - PassGuide 312-97 Prüfung - 312-97 Guide □ Suchen Sie jetzt auf ▸ www.zertpruefung.ch ◂ nach ➥ 312-97 □ und laden Sie es kostenlos herunter □312-97 Deutsch Prüfung
- 312-97 Antworten ☀ 312-97 Prüfungs □ 312-97 Deutsch Prüfung □ Suchen Sie jetzt auf ⇛ www.itzert.com ⇚ nach □ 312-97 □ um den kostenlosen Download zu erhalten □312-97 Demotesten
- 312-97 Deutsch Prüfung □ 312-97 Prüfungsübungen □ 312-97 Deutsch □ Suchen Sie auf ▹ www.zertpruefung.ch ◃

nach kostenlosem Download von ➡ 312-97 □□□ □312-97 Praxisprüfung