Question 312-97 Explanations | Valid 312-97 Test Dumps

Of course, when we review a qualifying exam, we can't be closed-door. We should pay attention to the new policies and information related to the test 312-97 certification. For the convenience of the users, the 312-97 test materials will be updated on the homepage and timely update the information related to the qualification examination. Annual qualification examination, although content broadly may be the same, but as the policy of each year, the corresponding examination pattern grading standards and hot spots will be changed, as a result, the 312-97 Test Prep can help users to spend the least time, you can know the test information directly what you care about on the learning platform that provided by us, let users save time and used their time in learning the new hot spot concerning about the knowledge content.

ECCouncil 312-97 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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.
Topic 3	• 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.
Topic 4	• 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.
Topic 5	• 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.
Topic 6	• Understanding DevOps Culture: This module introduces DevOps principles, covering cultural and technical foundations that emphasize collaboration between development and operations teams. It addresses automation, CI • CD practices, continuous improvement, and the essential communication patterns needed for faster, reliable software delivery.

Valid ECCouncil 312-97 Test Dumps - 312-97 Certification Exam Infor

The language which is easy to be understood and simple, 312-97 exam questions are suitable for any learners no matter he or she is a student or the person who have worked for many years with profound experiences. So it is convenient for the learners to master the 312-97 Guide Torrent and pass the exam in a short time. The amount of the examinee is large. For the office workers, they are both busy in their job and their family life; for the students, they possibly have to learn or do other things.

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) Sample Questions (Q35-Q40):

NEW QUESTION # 35
(Rachel Maddow has been working at RuizSoft Solution Pvt. Ltd. for the past 7 years as a senior DevSecOps engineer. To develop software products quickly and securely, her organization has been using AWS DevOps services. On January 1, 2022, the software development team of her organization developed a spring boot application with microservices and deployed it in AWS EC2 instance. Which of the following AWS services should Rachel use to scan the AWS workloads in EC2 instance for security issues and unintended network exposures?.)

- A. AWS Inspector.
- B. AWS Config.
- C. Amazon CloudWatch.
- D. AWS WAF.

Answer: A

Explanation:
AWS Inspector is a managed vulnerability assessment service designed specifically to scan workloads running on Amazon EC2 instances and container images for security vulnerabilities and unintended network exposures. It automatically evaluates instances against known vulnerabilities and security best practices, providing detailed findings and risk severity levels. AWS WAF protects web applications from common web exploits but does not perform host-based vulnerability scanning. AWS Config tracks configuration changes and compliance but does not actively scan workloads for vulnerabilities. Amazon CloudWatch focuses on monitoring logs, metrics, and alarms rather than security scanning. For a Spring Boot microservices application deployed on EC2, AWS Inspector is the correct choice to continuously assess security posture during the Build, Deploy, and Operate phases of the DevSecOps pipeline.
==========

NEW QUESTION # 36
(Peter Dinklage has been working as a senior DevSecOps engineer at SacramentSoft Solution Pvt. Ltd. He has deployed applications in docker containers. His team leader asked him to check the exposure of unnecessary ports. Which of the following commands should Peter use to check all the containers and the exposed ports?)

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

Answer: B

Explanation:
To inspect exposed ports for running Docker containers, the recommended approach is to first retrieve container IDs using docker ps --quiet and then pass them to docker inspect. The --format option allows selective output of container configuration details, including port mappings. The command docker ps --quiet | xargs docker inspect --format ': Ports=' correctly extracts port information for each container. Options that include the --all flag or incorrect formatting are not valid for this inspection use case. Checking exposed ports is an important activity in the Operate and Monitor stage because unnecessary open ports increase the attack surface and may violate container security best practices. Regular inspection helps ensure that only required ports are exposed, supporting secure runtime operations.
==========

NEW QUESTION # 37

(William McDougall has been working as a DevSecOps engineer in an IT company located in Sacramento, California. His organization has been using Microsoft Azure DevOps service to develop software products securely and quickly. To take proactive decisions related to security issues and to reduce the overall security risk, William would like to integrate ThreatModeler with Azure Pipelines. How can ThreatModeler be integrated with Azure Pipelines and made a part of William's organization DevSecOps pipeline?)

- A. By using a unidirectional API.
- B. By using a bidirectional UI.
- C. By using a unidirectional UI.
- D. By using a bidirectional API.

Answer: D

Explanation:
ThreatModeler integration with Azure Pipelines is achieved using abidirectional API, which allows automated and continuous interaction between the pipeline and the threat modeling platform. This bidirectional communication enables Azure Pipelines to trigger threat modeling activities while also receiving results, risk scores, and actionable insights back from ThreatModeler. Such feedback loops are critical for proactive security decision-making during the Plan stage of DevSecOps. Unidirectional APIs or UI-based integrations limit automation and do not support continuous feedback, making them unsuitable for pipeline- driven workflows. UI-based approaches also introduce manual steps, which conflict with DevSecOps principles of automation and consistency. By using a bidirectional API, William's organization can embed threat modeling into the planning process, identify architectural risks early, and ensure security considerations are continuously enforced as part of the pipeline.
==========

NEW QUESTION # 38
(Lara Grice has been working as a DevSecOps engineer in an IT company located in Denver, Colorado. Her team leader has told her to save all the container images in the centos repository to centos-all.tar. Which of the following is a STDOUT command that Lara can use to save all the container images in the centos repository to centos-all.tar?.)

- A. # docker save centos < centos all.tar.
- B. # docker save centos > centos all.tar.
- C. # docker save centos > centos-all.tar.
- D. # docker save centos < centos-all.tar.

Answer: C

Explanation:
The docker save command exports one or more Docker images to a tar archive by writing the image data to standard output (STDOUT). To redirect this output into a file, the > redirection operator is used. The correct syntax is docker save <image> > <filename>.tar. In this scenario, the image repository name is centos, and the desired archive file is centos-all.tar, making option B correct. Options C and D incorrectly use input redirection (<) instead of output redirection. Option A includes a space in the filename (centos all.tar), which would be interpreted as two separate arguments and cause an error unless quoted. Saving images to a tar archive is a common operational task used for backups, transfers between environments, or offline analysis during the Operate and Monitor stage.

NEW QUESTION # 39
(Gabriel Bateman has been working as a DevSecOps engineer in an IT company that develops virtual classroom software for online teaching. He would like to clone the BDD security framework on his local machine using the following URL,https://github.com/continuumsecurity/bdd-security.git. Which of the following command should Gabriel use to clone the BBD security framework?)

- A. git clonehttps://github.com/continumsecurity/bdd-security.git.
- B. github clonehttps://github.com/continuumsecurity/bdd-security.git.
- C. github clonehttps://github.com/continumsecurity/bdd-security.git.
- D. git clonehttps://github.com/continuumsecurity/bdd-security.git.

Answer: D

Explanation:

To clone a repository from GitHub, the correct command is git clone followed by the accurate repository URL. The organization name continuumsecurity and repository name bdd-security must be spelled correctly for the command to succeed. Options using github clone are invalid because github is not a standard Git command-line utility. Options with misspelled organization names will result in errors. Cloning security testing frameworks during the Code stage enables DevSecOps engineers to evaluate, customize, and integrate security automation tools into development workflows, supporting secure application development and testing practices.

NEW QUESTION # 40

.....

Our company has employed a lot of leading experts in the field to compile the 312-97 Exam Materials, in order to give candidate a chance to pass the 312-97 exam. So many candidates see our Prep4sures web page occasionally, and they are attracted by our high quality and valid dumps. They bought it without any hesitation. However, they passed the exam successfully. It turned out that their choice was extremely correct.