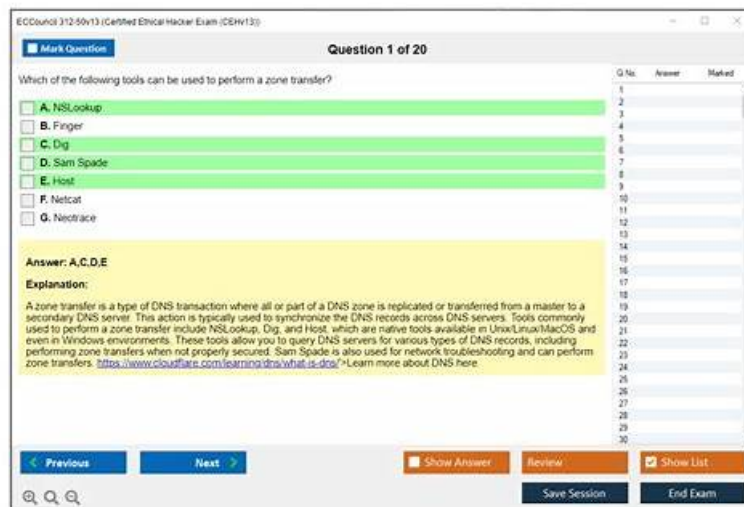# 100% Pass Quiz 2026 ECCouncil Authoritative 312-97 Reliable Exam Tips

Our worldwide after sale staff will be online for 24/7 and reassure your rows of doubts on our 312-97 exam questions as well as exclude the difficulties and anxiety with all the customers. Just let us know your puzzles and we will figure out together. You can contact with us at any time and we will give you the most professional and specific suggestions on the 312-97 Study Materials. What is more, you can free download the demos of the 312-97 learning guide on our website to check the quality and validity.

We can provide absolutely high quality guarantee for our 312-97 practice materials, for all of our 312-97 learning materials are finalized after being approved by industry experts. Without doubt, you will get what you expect to achieve, no matter your satisfied scores or according 312-97certification file. As long as you choose our 312-97 exam questions, you will get the most awarded.

>> 312-97 Reliable Exam Tips <<

100% Pass Quiz 2026 Useful ECCouncil 312-97 Reliable Exam Tips

Contemporarily, social competitions stimulate development of modern science, technology and business, which revolutionizes our society's recognition to 312-97 exam and affect the quality of people's life. According to a recent report, those who own more than one skill certificate are easier to be promoted by their boss. To be out of the ordinary and seek an ideal life, we must master an extra skill to get high scores and win the match in the workplace. Our 312-97 Exam Question can help make your dream come true. What's more, you can have a visit of our website that provides you more detailed information about the 312-97 guide torrent.

ECCouncil 312-97 Exam Syllabus Topics:

Topic	Details
Topic 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.
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	• 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 4	• 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 5	• DevSecOps Pipeline - Code Stage: This module discusses secure coding practices and security integration within the development process and IDE. Developers learn to write secure code using static code analysis tools and industry-standard secure coding guidelines.
Topic 6	• 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.

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) Sample Questions (Q36-Q41):

NEW QUESTION # 36
(Brady Coleman is a senior DevSecOps engineer at CloudVac Security Private Ltd. He has created a new container named "eccbrad" from the centos:7 image using the command docker run -i -t --name geeklab centos:7 /bin/bash. Now, Brady wants to install the httpd package inside the eccbrad container. Which of the following commands should Brady use to install the httpd package inside the container?)

- A. yum install-httpd.
- B. yum install httpd.
- C. sudo install httpd.
- D. sudo install-httpd.

Answer: B

Explanation:
The CentOS operating system uses theyumpackage manager to install software packages. Inside a CentOS- based Docker container, the correct way to install the Apache HTTP Server is by running yum install httpd.
Containers typically run as the root user by default, making the use of sudo unnecessary. Commands such as install-httpd are invalid because yum requires the install keyword followed by the package name separated by a space. Installing required packages inside containers should be done carefully to avoid bloating images and increasing the attack surface. During the Operate and Monitor stage, DevSecOps teams must balance functionality with container hardening best practices by installing only necessary components.
=========

NEW QUESTION # 37
(Frances Fisher joined TerraWolt Pvt. Ltd. as a DevSecOps engineer in 2020. On February 1, 2022, his organization became a victim of cyber security attack. The attacker targeted the network and application vulnerabilities and compromised some important functionality of the application. To secure the organization against similar types of attacks, Franches used a flexible, accurate, low maintenance vulnerability management and assessment solution that continuously scans the network and application vulnerabilities and provides daily updates and specialized testing methodologies to catch maximum detectable vulnerabilities.
Based on the above-mentioned information, which of the following tools is Frances using?)

- A. Shadow Daemon.
- B. Black Duck.
- C. SonarQube.
- D. BeSECURE.

Answer: D

Explanation:
BeSECURE is a vulnerability management and assessment solution designed for continuous scanning of both network and application vulnerabilities. It emphasizes flexibility, accuracy, low maintenance overhead, and frequent updates to vulnerability detection mechanisms. These characteristics align directly with the scenario described, where the organization requires continuous scanning, daily updates, and specialized testing methodologies to detect a wide range of vulnerabilities. SonarQube focuses on static code quality and security analysis during development, Black Duck is primarily used for open-source software composition analysis,

and Shadow Daemon is a web application firewall rather than a comprehensive vulnerability management solution. Using BeSECURE during the Operate and Monitor stage allows organizations to maintain ongoing visibility into their security posture, detect new vulnerabilities as they emerge, and reduce the likelihood of repeat attacks by addressing weaknesses proactively.
========

NEW QUESTION # 38

(Richard Branson has been working as a DevSecOps engineer in an IT company that develops apps for Android mobiles. To manage the secret information of an application in various phases of development lifecycle and to provide fine-grained access to each secret, he would like to integrate HashiCorp Vault with Jenkins. To access the vault from Jenkins, Richard installed hashicorp-vault-plugin and ran a vault instance; he then selected the AppRole authentication method, which allows apps to access vault with a predefined role.

Which of the following commands should Richard use to enable AppRole authentication?)

- A. enable auth vault approle.
- B. auth vault enable approle.
- C. vault auth enable approle.
- D. enable vault auth approle.

Answer: C

Explanation:
HashiCorp Vault enables authentication mechanisms using the vault auth enable command followed by the name of the authentication method. To enable AppRole authentication, the correct command is vault auth enable approle. AppRole is specifically designed for machine-to-machine authentication, making it ideal for CI/CD tools like Jenkins. It allows applications to authenticate securely using role IDs and secret IDs instead of static credentials. The other options do not follow Vault CLI syntax and would result in command errors.
Enabling AppRole during the Build and Test stage ensures that secrets are accessed securely and dynamically, supporting least-privilege access control and reducing the risk of credential leakage across the DevSecOps pipeline.

NEW QUESTION # 39

(Robert Wheeler has been working as a DevSecOps engineer in an IT company for the past 5 years. His organization develops software products and web applications related to AutoCAD. Rob would like to integrate Rapid7 tCell Next-Gen Cloud WAF and RASP Tool with AWS CloudFront to protect application by identifying suspicious actors, enforcing content security policies (CSPs), and securing against unvalidated HTTP redirections on web applications. How can Rob deploy the tCell agent as a CloudFormation stack into his organization AWS account?.)

- A. By plugging into CloudFormation through Lambda@Edge.
- B. By plugging into CloudFront through Lambda@Edge.
- C. By plugging into CloudFormation through Lambda Function.
- D. By plugging into CloudFront through Lambda Function.

Answer: B

Explanation:
When integrating security controls at the CDN edge with AWS CloudFront, the typical deployment model usesLambda@Edge, which allows code to execute at CloudFront edge locations on viewer request/response or origin request/response events. Deploying the tCell agent "as a CloudFormation stack" describes packaging the required AWS resources (IAM roles, functions, permissions, and CloudFront associations) into infrastructure-as-code, but the actual attachment point for CloudFront request/response processing is Lambda@Edge. Option C correctly reflects this: "plugging into CloudFront through Lambda@Edge." Standard Lambda functions run in regional AWS environments and cannot directly run at CloudFront edge locations in the same way; therefore, "CloudFront through Lambda Function" is not the best match for edge enforcement needs like CSP handling and redirect protections. Options that claim "plugging into CloudFormation" misunderstand CloudFormation's role: it deploys resources, but it is not the runtime integration point. Hence, CloudFront + Lambda@Edge is the correct deployment approach.

NEW QUESTION # 40

(Terry Diab has been working as a DevSecOps engineer in an IT company that develops software products and web applications for a call center. She would like to integrate Snyk with AWS CodeCommit to monitor and remediate vulnerabilities in the code

repository. Terry pushed code to AWS CodeCommit; this triggered Amazon EventBridge Rule, which then triggered AWS CodePipeline. AWS CodePipeline passed code to Snyk CLI run. Who among the following interacts with Snyk CLI and sends the results to Snyk UI?)

- A. AWS CodeBuild.
- B. AWS Pipeline.
- C. AWS CodeCommit.
- D. AWS CodeDeploy.

Answer: A

Explanation:
In an AWS CI/CD architecture, AWS CodePipeline acts as an orchestration service that coordinates different stages but does not execute build or scan commands itself. AWS CodeBuild is the service responsible for running commands such as compiling code, executing tests, and running third-party security tools like the Snyk CLI. In Terry's workflow, CodeCommit stores the source code, EventBridge triggers the pipeline, and CodePipeline passes the source to CodeBuild. CodeBuild then executes the Snyk CLI, performs vulnerability scanning, and sends the scan results to the Snyk UI using the configured authentication token. AWS CodeDeploy is focused on application deployment and does not interact with Snyk CLI. Therefore, AWS CodeBuild is the component that interacts with Snyk CLI and communicates results back to the Snyk platform. This integration ensures that dependency vulnerabilities are detected early in the Build and Test stage.
=========

NEW QUESTION # 41

......

Everyone is not willing to fall behind, but very few people take the initiative to change their situation. Take time to make a change and you will surely do it. Our 312-97 learning materials can give you some help. Our company aims to help ease the pressure on you to prepare for the exam and eventually get a certificate. Obtaining a certificate is equivalent to having a promising future and good professional development. Our 312-97 Learning Materials have a good reputation in the international community and their quality is guaranteed. Why don't you there have a brave attempt? You will certainly benefit from your wise choice.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes