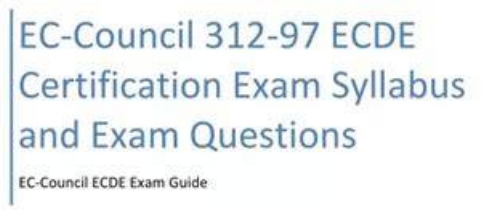
Get a Free Demo of ExamDiscuss ECCouncil Exam Questions and Start Your 312-97 Exam Preparation Now



BONUS!!! Download part of ExamDiscuss 312-97 dumps for free: https://drive.google.com/open?id=1PtmP6Ofa0tPncIvvrjU5BwCmaRjEIVmE

The EC-Council Certified DevSecOps Engineer (ECDE) (312-97) web-based practice test is compatible with these browsers: Chrome, Safari, Internet Explorer, MS Edge, Firefox, and Opera. This EC-Council Certified DevSecOps Engineer (ECDE) (312-97) practice exam does not require any software installation as it is web-based. It has similar specifications to the ECCouncil 312-97 desktop-based practice exam software, but it requires an internet connection.

ECCouncil 312-97 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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.
Topic 3	• 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 4	• 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 5	• 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.

312-97 Trustworthy Pdf, 312-97 Valid Exam Duration

Many job-hunters want to gain the competition advantages in the labor market and become the hottest people which the companies rush to get. But if they want to realize that they must boost some valuable 312-97 certificate. The 312-97 certificate enjoys a high reputation among the labor market circle and is widely recognized as the proof of excellent talents and if you are one of them and you want to pass the 312-97 test smoothly you can choose our 312-97 practice questions.

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) Sample Questions (Q82-Q87):

NEW QUESTION # 82
Ethan Roberts, a DevSecOps engineer at SecureSoft Technologies, is responsible for securing software products and web applications throughout the development lifecycle. To enhance security testing, he implements Interactive Application Security Testing (IAST), which allows him to analyze source code for vulnerabilities in real-time, monitor security issues dynamically as the application runs, utilize IAST across the development, QA, and production stages to identify vulnerabilities early, and reduce remediation costs by detecting issues before deployment. Ethan's team is particularly interested in how IAST integrates both SAST and DAST capabilities. They observe that IAST can analyze every line of code statically (SAST) and examine every request and response dynamically (DAST). How does IAST achieve this dual functionality?

- A. Because IAST has access to both the server and local machine.
- B. Because IAST has access to the source code and HTTP traffic.
- C. Because IAST has access to offline and runtime environments.
- D. Because IAST has access to both internal and external security agents.

Answer: B

Explanation:
IAST combines SAST and DAST because its instrumentation agent has access to the application's source code (and runtime internals) while also observing HTTP requests and responses as the application runs. This lets it statically analyze every line of code and dynamically examine every request/response, pinpointing vulnerabilities with context. The other options mischaracterize what IAST agents access.

NEW QUESTION # 83
(Steven Gerrard has been working as a DevSecOps engineer at an IT company that develops software products and applications related to the healthcare industry. His organization has been using Azure DevOps services to securely and quickly develop software products. To ensure that the deployed infrastructure is in accordance with the architecture and industrial standards and the security policies are appropriately implemented, she would like to integrate InSpec with Azure. Therefore, after installation and configuration of InSpec, she created InSpec profile file and upgraded it with personal metadata and Azure resource pack information; then she wrote the InSpec tests. Which of the following commands should Steven use to run InSpec tests to check the compliance of Azure infrastructure?)

- A. inspec exec inspec-tests/integration/ -it azure://.
- B. inspec exec inspec-tests/integration/ -t azure://.
- C. inspec exe inspec-tests/integration/ -it azure://.
- D. inspec exe inspec-tests/integration/ -t azure://.

Answer: B

Explanation:
Chef InSpec executes compliance tests using the inspec exec command. When testing Azure infrastructure, InSpec requires a target specification using the -t flag with the Azure transport identifier azure://. The correct command is inspec exec inspec-tests/integration/ -t azure://. Options using exe instead of exec are invalid due to incorrect command spelling. Options that use the -it flag misuse command-line parameters that are not intended for target selection. Running InSpec tests in this way allows DevSecOps teams to validate that Azure resources comply with architectural, security, and regulatory requirements. Integrating these checks into the Build and Test stage ensures continuous compliance and reduces the risk of insecure infrastructure reaching production environments.
==========

NEW QUESTION # 84
Daniel Ross, a DevSecOps engineer at TechNova Inc., is responsible for integrating Jira with Jenkins to streamline project management and automate issue tracking. His team needs to search for relevant Jira issues related to specific builds, filter tasks based on status, and track deployment progress within Jira. To achieve this, Daniel is looking for a way to query and retrieve specific Jira issues based on project requirements, such as filtering by issue type, status, or assigned developer. Which of the following should Daniel use to efficiently search and filter Jira issues?

- A. Jira Query Language (JQL).
- B. REST API Requests.
- C. Pipeline DSL in Jenkins.
- D. Groovy Scripting.

Answer: A

Explanation:
Jira Query Language (JQL) is Jira's native query language for searching and filtering issues by project, issue type, status, assignee, and more-exactly what Daniel needs to retrieve specific issues tied to builds. Groovy, Pipeline DSL, and raw REST calls are scripting/integration mechanisms, not Jira's issue search facility.

NEW QUESTION # 85
A DevSecOps team is responsible for automating infrastructure deployment using Ansible. During a routine security audit, they discover that sensitive information-such as database credentials and API keys-is stored in plain text within Ansible playbooks. This introduces a serious security risk, as exposing these playbooks could lead to unauthorized access to critical systems. To address this issue, the team must implement a secure approach that protects confidential data within Ansible playbooks, prevents unauthorized access to sensitive information, and ensures seamless automation without exposing secrets in plaintext. Which solution should the team implement?

- A. Use ansible-vault to encrypt sensitive data within the playbooks.
- B. Use ansible-galaxy to fetch encryption modules for securing playbooks.
- C. Use ansible-playbook to apply encryption to sensitive data directly within task definitions.
- D. Use ansible-console to encrypt sensitive information during runtime execution of tasks.

Answer: A

Explanation:
ansible-vault is Ansible's built-in feature for encrypting sensitive data (variables, files) within playbooks, so credentials and API keys are never stored in plaintext while automation still runs seamlessly with a vault password or key. ansible-playbook executes playbooks, ansible-console is an interactive shell, and ansible-galaxy manages roles/collections-none encrypt secrets.

NEW QUESTION # 86
(William O'Neil has been working as a senior DevSecOps engineer in an IT company that develops software products related to ecommerce. At this point in time, his team is working on securing a python-based application. Using GitGraber, William would like to detect sensitive information in real-time in his organizational GitHub repository. Therefore, he downloaded GitGraber and installed the dependencies. Which of the following commands should William use to find secrets using a keyword (assume the keyword is yahoo)?.)

- A. python3 gitGraber.py -k wordlist/keywordsfile.txt -q "\yahoo" -s.

- B. python3 gitGraber.py -w wordlist/keywordsfile.txt -q "\yahoo" -s.
- C. python3 gitGraber.py -g wordlist/keywordsfile.txt -q "\yahoo" -s.
- D. python3 gitGraber.py -p wordlist/keywordsfile.txt -q "\yahoo" -s.

Answer: A

Explanation:
GitGraber uses specific command-line flags to define how secret detection is performed. The -k flag is used to specify akeyword filethat contains search terms for identifying sensitive data in repositories. In this case, William wants to search for secrets using the keyword "yahoo," which is passed using the -q flag. Options -w,
-g, and -p are not valid flags for keyword-based scanning in GitGraber. By using -k, GitGraber scans repositories for matches against the defined keywords and reports potential secret exposures in real time. This capability is especially valuable during the Code stage, helping teams prevent credential leakage and maintain secure repositories.

NEW QUESTION # 87
.....

In order to meet the demands of all the customers, we can promise that we will provide all customers with three different versions of the 312-97 study materials: PDF version, Soft version and APP version. In addition, we can make sure that we are going to offer high quality 312-97 practice study materials with reasonable prices but various benefits for all customers. It is our sincere hope to help you pass 312-97 exam by the help of our 312-97 certification guide. Just come and buy our 312-97 learning prep!