312-97 Reliable Test Blueprint & 312-97 Test Free

BONUS!!! Download part of DumpsMaterials 312-97 dumps for free: https://drive.google.com/open?id=1dVOejB4as3g3zVOsP9apaOKYNWvwsBjB

You can also be a part of this wonderful community. To do this you just need to pass the ECCouncil 312-97 certification exam. Are you ready to accept this challenge? Looking for the proven and easiest way to crack the ECCouncil 312-97 Certification Exam? If your answer is yes then you do not need to go anywhere. Just download DumpsMaterials 312-97 exam practice questions and start EC-Council Certified DevSecOps Engineer (ECDE) (312-97) exam preparation without wasting further time.

As we all know, HR form many companies hold the view that candidates who own a 312-97 professional certification are preferred, because they are more likely to solve potential problems during work. And the 312-97 certification vividly demonstrates the fact that they are better learners. Concentrated all our energies on the study 312-97 learning guide we never change the goal of helping candidates pass the exam. Our 312-97 test questions' quality is guaranteed by our experts' hard work. So what are you waiting for? Just choose our 312-97 exam materials, and you won't be regret.

>> 312-97 Reliable Test Blueprint <<

312-97 Test Free | 312-97 Study Guides

The sources and content of our 312-97 practice dumps are all based on the real 312-97 exam. And they are the masterpieces of processional expertise these area with reasonable prices. Besides, they are high efficient for passing rate is between 98 to 100 percent, so they can help you save time and cut down additional time to focus on the 312-97 Actual Exam review only. We understand your drive of the certificate, so you have a focus already and that is a good start.

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 - 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 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 - 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	• 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.

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) Sample Questions (Q89-Q94):

NEW QUESTION # 89
(Matt LeBlanc has been working as a DevSecOps engineer in an IT company that develops software products and web applications for IoT devices. His team leader has asked him to use GitRob tool to find sensitive data in the organizational public GitHub repository. To install GitRob, Matt ensured that he has correctly configured Go >= 1.8 environment and that $GOPATH/bin is in his $PATH. The GitHub repository URL from which he is supposed to install the tool ishttps://github.com/michenriksen/gitrob. Which of the following command should Matt use to install GitRob?.)

- A. $ go git github.com/michenriksen/gitrob.
- B. $ go get gitrob github.com/michenriksen/gitrob.
- C. $ go get github.com/michenriksen/gitrob.
- D. $ go git gitrob github.com/michenriksen/gitrob.

Answer: C

Explanation:
In Go-based tool installation, the standard method to download, compile, and install a Go package is using the go get command followed by the repository import path. Since Matt has already ensured that Go version 1.8 or later is installed and that $GOPATH/bin is included in the system PATH, running go get github.com /michenriksen/gitrob will fetch the GitRob source code, build the binary, and place it in the appropriate bin directory. Options B, C, and D are invalid because go get does not accept multiple positional arguments in that manner, and go git is not a valid Go command. Installing GitRob during the Code stage enables DevSecOps teams to scan repositories for accidentally committed credentials, API keys, and other sensitive information, helping prevent data leakage from public repositories.
==========

NEW QUESTION # 90
(Curtis Morgan has been working as a software developer in an MNC company. His team has developed a NodeJS application. While doing peer review of the NodeJS application, he observed that there are insecure libraries in the application. Therefore, he approached, Teresa Lisbon, who is working as a DevSecOps engineer, to detect the insecure libraries in the NodeJS application. Teresa used a SCA tool to find known vulnerabilities in JavaScript libraries for Node.JS applications and detected all the insecure libraries in the application. Which of the following tools did Teresa use for detecting insecure libraries in the NodeJS application?)

- A. Bandit.
- B. Retire.js.
- C. Bundler-Audit.
- D. Tenable.io.

Answer: B

Explanation:
Retire.js is a Software Composition Analysis (SCA) tool designed specifically to identify known vulnerabilities in JavaScript libraries used in web and NodeJS applications. It scans dependencies and compares detected versions against a vulnerability database to identify insecure libraries. Bandit is a static analysis tool for Python, Bundler-Audit is used for Ruby dependencies, and Tenable.io focuses on infrastructure and vulnerability management rather than JavaScript libraries. Using Retire.js during the Code stage allows DevSecOps teams to identify insecure third-party dependencies early, reducing the likelihood of vulnerable libraries being deployed into production. This supports shift-left security and strengthens the application's overall security posture.
==========

NEW QUESTION # 91
(Timothy Dalton has been working as a senior DevSecOps engineer in an IT company located in Auburn, New York. He would like to use Jenkins for CI and Azure Pipelines for CD to deploy a Java-based app to an Azure Container Service (AKS) Kubernetes cluster. Before deploying Azure Kubernetes Service (AKS) Cluster, Timothy wants to create a Resource group named Jenkins in southindia location. Which of the following commands should Timothy run?.)

- A. azure group create --n Jenkins --loc southindia.
- B. az group create --name Jenkins --location southindia.
- C. azure group create --name Jenkins --location southindia.
- D. az grp create --n Jenkins --loc southindia.

Answer: B

Explanation:
Azure resource groups are created using the Azure CLI command az group create. The --name parameter specifies the resource group name, and --location defines the Azure region. Option A uses the correct CLI prefix (az), command group (group create), and valid parameters. Options B, C, and D are incorrect due to invalid command abbreviations or incorrect CLI prefixes (azure instead of az). Creating a resource group is a foundational step in the Release and Deploy stage, as it provides a logical container for AKS clusters, networking components, and related resources, enabling organized, secure, and manageable deployments.

NEW QUESTION # 92
(Patrick Fisher is a DevSecOps engineer in an IT company that develops software products and web applications. He is using IAST to analyze code for security vulnerabilities and to view real-time reports of the security issues. Patrick is using IAST in development, QA, and production stages to detect the vulnerabilities from the early stage of development, reduce the remediation cost, and keep the application secure. How can IAST perform SAST on every line of code and DAST on every request and response?.)

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

Answer: B

Explanation:
Interactive Application Security Testing (IAST) works by instrumenting the application at runtime, allowing it to observe both thesource code execution pathsand theHTTP requests and responsesflowing through the application. Because of this dual visibility, IAST can analyze every executed line of code (similar to SAST) while also monitoring real-time application behavior (similar to DAST). This unique capability enables highly accurate vulnerability detection with fewer false positives. The other options do not correctly explain how IAST achieves this hybrid analysis. Access to both code and HTTP traffic is what allows IAST to bridge static and dynamic testing techniques, making it highly effective across development, QA, and production environments.
==========

NEW QUESTION # 93
(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. Active IAST.
- B. Semi-active IAST.
- C. Semi-passive IAST.
- D. Passive IAST.

Answer: B

Explanation:
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.
═══════

NEW QUESTION # 94
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, schoolido.lu, myportal.utt.edu.tt, ngmetamorphosis.com, Disposable vapes

2026 Latest DumpsMaterials 312-97 PDF Dumps and 312-97 Exam Engine Free Share: https://drive.google.com/open?id=1dVOejB4as3g3zVOsP9apaOKYNWvwsBjB