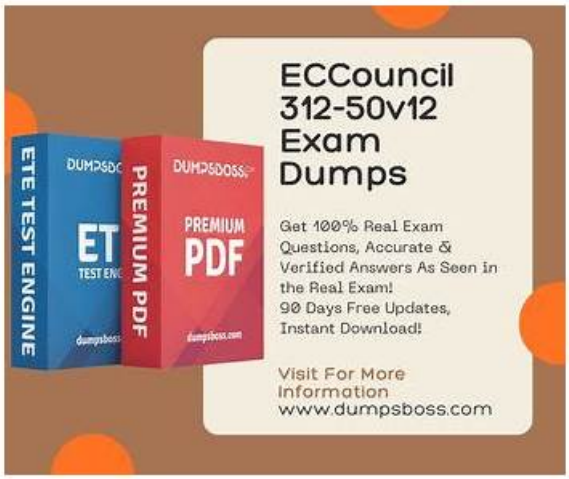
ECCouncil 312-97 Pass Leader Dumps, New 312-97 Braindumps



We have a large number of regular customers exceedingly trust our 312-97 training materials for their precise content about the exam. You may previously have thought preparing for the 312-97 preparation materials will be full of agony, actually, you can abandon the time-consuming thought from now on. Our 312-97 Exam Questions are famous for its high-efficiency and high pass rate as 98% to 100%. Buy our 312-97 study guide, and you will pass the exam easily.

ECCouncil 312-97 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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.
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 - 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.

New 312-97 Braindumps | 312-97 Test Result

Everyone has the right to pursue happiness and wealth. You can rely on the 312-97 certificate to support yourself. If you do not own one or two kinds of skills, it is difficult for you to make ends meet in the modern society. After all, you can rely on no one but yourself. At present, our 312-97 Study Materials can give you a ray of hope. Even you have no basic knowledge about the 312-97 study materials. You still can pass the 312-97 with the help of our 312-97 learning guide.

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) Sample Questions (Q92-Q97):

NEW QUESTION # 92
(Charles Drew has been working as a DevSecOps team leader in an IT company located in Nashville, Tennessee. He would like to look at the applications from an attacker's perspective and make security a part of the organizations' culture. Imagine, you are working under Charles as a DevSecOps engineer. Charles has asked you to install ThreatPlaybook, which is a unified DevSecOps Framework that allows you to go from iterative, collaborative threat modeling to application security testing orchestration. After installation, you must configure ThreatPlaybook CLI; therefore, you have created a directory for the project and then you go to the current directory where you would like to configure ThreatPlaybook. Which of the following commands will you use to configure ThreatPlaybook? (Here, < your-email > represents your email id; < host info > represents IP address; and < port > represents the nginx port.))

- A. ThreatPlaybook configure -e < your-email > -h < host-info > -p < port >.
- B. playbook configure -e < your-email > -h < host-info > -p < port >.
- C. playbook configure -e < your-email > -u < host-info > -p < port >.
- D. ThreatPlaybook configure -e < your-email > -u < host-info > -p < port >.

Answer: A

Explanation:
ThreatPlaybook CLI is configured using the ThreatPlaybook configure command, which initializes the CLI with the required connection and user details. The -e option is used to specify the user's email address, the -h option defines the host information such as IP address or hostname, and the -p option specifies the port number. This configuration enables the CLI to securely communicate with the ThreatPlaybook service for orchestrating threat modeling and application security testing workflows. Options that use playbook configure are incorrect because the executable name is explicitly ThreatPlaybook. Options using -u instead of -h do not correctly specify host information. Configuring ThreatPlaybook during the Plan stage helps teams adopt an attacker's mindset early, embedding security into the organization's culture and ensuring threats are identified and addressed before development and deployment activities begin.
═══════

NEW QUESTION # 93
(Debra Aniston has recently joined an MNC company as a DevSecOps engineer. Her organization develops various types of software products and web applications. The DevSecOps team leader provided an application code and asked Debra to detect and mitigate security issues. Debra used w3af tool and detected cross-site scripting and SQL injection vulnerability in the source code. Based on this information, which category of security testing tools is represented by w3af?.)

- A. IAST.
- B. DAST.
- C. SAST.
- D. SCA.

Answer: B

Explanation:
w3af (Web Application Attack and Audit Framework) is aDynamic Application Security Testing (DAST) tool. It analyzes running web applications by sending crafted requests and observing responses to identify vulnerabilities such as SQL injection, cross-site scripting, and authentication flaws. Unlike SAST tools, w3af does not require access to source code and instead operates externally, simulating real-world attack behavior.

SCA focuses on third-party dependencies, and IAST requires runtime instrumentation within the application.
Since Debra detected vulnerabilities by actively interacting with the application, w3af clearly represents DAST. DAST tools are especially valuable during the Build and Test stage, as they validate application behavior from an attacker's perspective before deployment.
==========

NEW QUESTION # 94
(Thomas Gibson has been working as a DevSecOps engineer in an IT company that develops software products and web applications related to law enforcement. To automatically execute a scan against the web apps, he would like to integrate InsightAppSec plugin with Jenkins. Therefore, Thomas generated a new API Key in the Insight platform. Now, he wants to install the plugin manually. How can Thomas install the InsightAppSec plugin manually in Jenkins?)

- A. By creating a .conf file and uploading to his Jenkins installation.
- B. By creating a .zip file and uploading to his Jenkins installation.
- C. By creating a .hpi file and uploading to his Jenkins installation.
- D. By creating a .war file and uploading to his Jenkins installation.

Answer: C

Explanation:
Jenkins plugins are distributed and installed as .hpi files. To manually install a plugin, administrators upload the .hpi file through the Jenkins Plugin Manager using the "Upload Plugin" option. This approach is commonly used in environments with restricted internet access or when custom plugin versions are required. .
war files are used for deploying the Jenkins application itself, not plugins, while .zip and .conf files are not recognized plugin formats.
Installing the InsightAppSec plugin allows Jenkins pipelines to automatically trigger dynamic application security scans during the Build and Test stage. This integration ensures that web applications are continuously evaluated for vulnerabilities before deployment, supporting proactive security testing and risk reduction.
==========

NEW QUESTION # 95
(Kenneth Danziger is a certified DevSecOps engineer, and he recently got a job in an IT company that develops software products related to the healthcare industry. To identify security and compliance issues in the source code and quickly fix them before they impact the source code, Kenneth would like to integrate WhiteSource SCA tool with AWS. Therefore, to integrate WhiteSource SCA Tool in AWS CodeBuild for initiating scanning in the code repository, he built a buildspec.yml file to the source code root directory and added the following command to pre-build phase curl -LJOhttps://github.com/whitesource/unified-agent-distribution/raw/master/standAlone/wss_agent.sh. Which of the following script files will the above step download in Kenneth organization's CodeBuild server?.)

- A. cbs_agent.sh.
- B. ssw_agent.sh.
- C. aws_agent.sh.
- D. wss_agent.sh.

Answer: D

Explanation:
The command shown in the pre-build phase explicitly targets a script namedwss_agent.sh. The curl -LJO flags mean: -L follows redirects, -J honors the server-provided filename in the Content-Disposition header (when present), and -O writes output to a local file using the remote name. Since the requested path ends with wss_agent.sh, the downloaded file on the AWS CodeBuild server will be wss_agent.sh. This script is the WhiteSource (now commonly referred to as Mend in many environments) unified agent shell wrapper used to run SCA scans as part of a CI pipeline. Integrating SCA during the Build and Test stage helps detect vulnerable open-source dependencies and licensing/compliance issues early, when fixes are cheapest. The other filenames (ssw_agent.sh, cbs_agent.sh, aws_agent.sh) are distractors; they are not referenced by the provided command and would not be downloaded by that step.
==========

NEW QUESTION # 96

(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'.

Answer: A

Explanation:
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.
==========

NEW QUESTION # 97
.....

Normally, you will come across almost all of the 312-97 real questions on your usual practice. Maybe you are doubtful about our 312-97 guide dumps. We have statistics to tell you the truth. The passing rate of our products is the highest. Many candidates can also certify for our 312-97 Study Materials. As long as you are willing to trust our 312-97 preparation materials, you are bound to get the 312-97 certificate. Life needs new challenge. Try to do some meaningful things.

myportal.utt.edu.tt, myportal.utt.edu.tt, aoiacademy.com, 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, sb.gradxacademy.in, www.stes.tyc.edu.tw, myportal.utt.edu.tt, learn.aglevites.org, www.stes.tyc.edu.tw, Disposable vapes