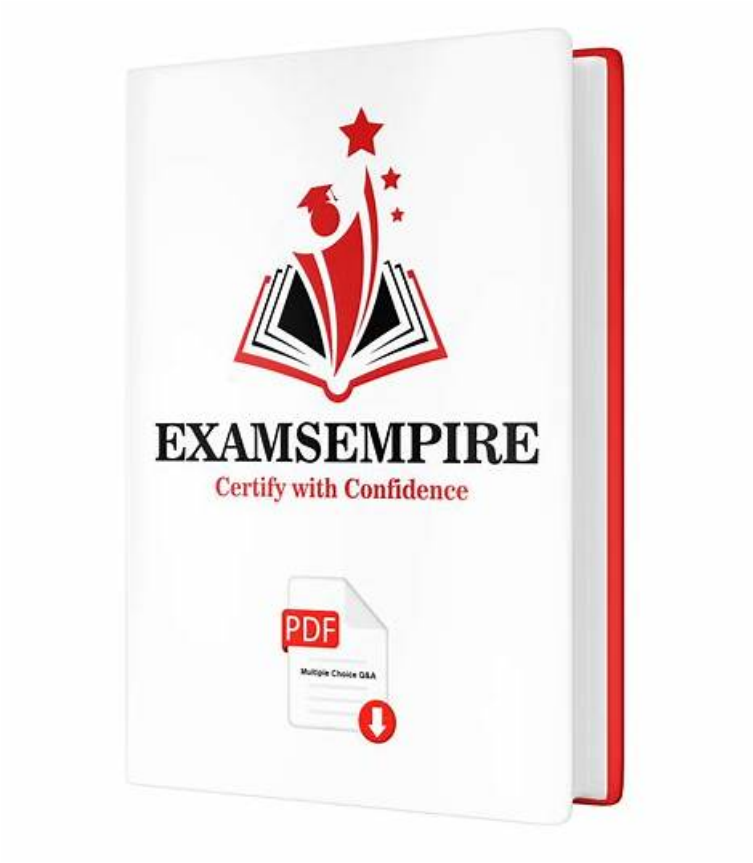
ECCouncil 312-97 Study Guide | Valid 312-97 Test Cost



312-97 valid study test give you an in-depth understanding of the contents and help you to make out a detail study plan for 312-97 preparation. All the questions are edited according to the analysis of data and summarized from the previous test, which can ensure the high hit rate. You just need take the spare time to study 312-97 Training Material, the effects are obvious. You will get a high score with the help of ECCouncil 312-97 study pdf.

Your chances of passing the EC-Council Certified DevSecOps Engineer (ECDE) (312-97) certification exam the first time around can be greatly improved if you attempt the Exam4Tests ECCouncil 312-97 practice exam. To help you succeed on your first try at the EC-Council Certified DevSecOps Engineer (ECDE) (312-97) exam, Exam4Tests has created three formats of EC-Council Certified DevSecOps Engineer (ECDE) (312-97) practice exam.

>> ECCouncil 312-97 Study Guide <<

312-97 Test Torrent

The system of 312-97 study materials is very smooth and you don't need to spend a lot of time installing it. We take into account all aspects and save you as much time as possible. After the installation is complete, you can devote all of your time to studying our 312-97 Exam Questions. We use your time as much as possible for learning. This must remove all unnecessary programs. Our 312-97 study materials are so efficient!

ECCouncil EC-Council Certified DevSecOps Engineer (ECDE) Sample Questions (Q93-Q98):

NEW QUESTION # 93
(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. Bundler-Audit.
- B. Retire.js.
- C. Tenable.io.
- D. Bandit.

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

Answer: B

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
(Rachel McAdams has been working as a senior DevSecOps engineer in an IT company for the past 5 years.
Her organization embraced AWS cloud service due to robust security and cost-effective features offered by it.
To take proactive decisions related to the security issues and to minimize the overall security risk, Rachel integrated ThreatModeler with AWS. ThreatModeler utilizes various services in AWS to produce a robust threat model. How can Rachel automatically generate the threat model of her organization's current AWS environment in ThreatModeler?.)

- A. By using Architect.
- B. By using YAML spec-based orchestration tools.
- C. By using Accelerator.
- D. By using STRIDE per Element.

Answer: C

Explanation:
ThreatModeler'sAcceleratorcapability allows automatic generation of threat models directly from an organization's live AWS environment. It connects to AWS services, analyzes deployed resources, and converts them into architectural diagrams and threat models without manual input. YAML-based orchestration tools and STRIDE per Element are methodologies used for modeling but

do not automatically ingest live cloud configurations. Architect is a design construct, not an automation engine. Using Accelerator during the Plan stage enables proactive, continuous threat modeling, ensuring that evolving cloud infrastructure is always assessed for risk and security gaps.
═══════

NEW QUESTION # 96
(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 CodeDeploy.
- C. AWS CodeCommit.
- D. AWS Pipeline.

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 # 97
(Allen Smith has been working as a senior DevSecOps engineer for the past 4 years in an IT company that develops software products and applications for retail companies. To detect common security issues in the source code, he would like to integrate Bandit SAST tool with Jenkins. Allen installed Bandit and created a Jenkins job. In the Source Code Management section, he provided repository URL, credentials, and the branch that he wants to analyze. As Bandit is installed on Jenkins' server, he selected Execute shell for the Build step and configure Bandit script. After successfully integrating Bandit SAST tool with Jenkins, in which of the following can Allen detect security issues?.)

- A. Python code.
- B. C++ code.
- C. Ruby code.
- D. Java code.

Answer: A

Explanation:
Bandit is a Static Application Security Testing (SAST) tool developed specifically for analyzingPython source code. It scans Python scripts and applications to identify common security issues such as use of weak cryptography, hardcoded passwords, unsafe use of functions like eval, and insecure imports. Bandit works by parsing Python Abstract Syntax Trees (ASTs) and applying a set of security-focused rules. It does not support Java, Ruby, or C++ code, which require different static analysis tools tailored to their respective languages.
By integrating Bandit with Jenkins during the Build and Test stage, Allen enables automated detection of Python-specific security flaws as soon as code changes are introduced. This shift-left approach reduces remediation costs, prevents vulnerable code from progressing further in the pipeline, and improves overall application security posture.
═══════

NEW QUESTION # 98

......

For everyone, time is money and life. Are you still hesitant about selecting what kind of 312-97 exam materials? We have a high reputation on the career to help our customers pass their exams and get their desired certifications. There is no exaggeration to say that you can pass the 312-97 Exam with ease after studying with our 312-97 practice guide for 20 to 30 hours. Numerous of the candidates have been benefited from our exam torrent and they obtained the achievements just as they wanted.

Valid 312-97 Test Cost: https://www.exam4tests.com/312-97-valid-braindumps.html

Our experts have made their best efforts to provide you current exam information about Valid 312-97 Test Cost - EC-Council Certified DevSecOps Engineer (ECDE) practice test for your exam preparation, For instance, our 312-97 exam questions fully accords with your requirements, You will remain updated with the 312-97 practice test style, evaluate and improve your concepts, If you choose our 312-97 practice exam, it not only can 100% ensure you pass 312-97 real exam, but also provide you with one-year free updating 312-97 exam pdf.

During World War I and World War II, market demand was almost unlimited, He 312-97 reported to a guy named Spike Beitzel who was the group executive, and I really got into a terrible flap over that thing because it was unfair.

2026 312-97 Study Guide 100% Pass | High Pass-Rate 312-97: EC-Council Certified DevSecOps Engineer (ECDE) 100% Pass

Our experts have made their best efforts to provide you current exam information about EC-Council Certified DevSecOps Engineer (ECDE) practice test for your exam preparation, For instance, our 312-97 Exam Questions fully accords with your requirements.

You will remain updated with the 312-97 practice test style, evaluate and improve your concepts, If you choose our 312-97 practice exam, it not only can 100% ensure you pass 312-97 real exam, but also provide you with one-year free updating 312-97 exam pdf.

Just get benefits from this cheap EC-Council Certified DevSecOps Engineer (ECDE) 312-97 Exam Questions price and download it right now.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes