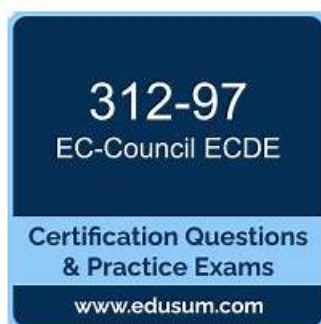


312-97 Pass Exam - Realistic EC-Council Certified DevSecOps Engineer (ECDE) Latest Braindumps



What's more, part of that Exam4Docs 312-97 dumps now are free: <https://drive.google.com/open?id=1LV7heC2FjN3dkDK2--i5tg0lNYl8bFB8>

312-97 study materials are the product for global users. Standards in all aspects are also required by international standards. The system designed of 312-97 learning guide by our IT engineers is absolutely safe. Your personal information will never be revealed. And 312-97 actual exam will certainly not cover this small profit and sell your information. 312-97 Study Materials can come today. With so many loyal users, our good reputation is not for nothing. In us, you don't have to worry about information leakage. Selecting a brand like 312-97 learning guide is really the most secure.

ECCouncil 312-97 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 3	<ul style="list-style-type: none">• 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 4	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 Pass Exam <<

312-97 Latest Braindumps - 312-97 Latest Test Pdf

Our website is here to lead you toward the way of success in 312-97 certification exams and saves you from the unnecessary preparation materials. The latest 312-97 dumps torrent are developed to facilitate our candidates and to improve their ability and expertise for the challenge of the actual test. We aimed to help our candidates get success in the 312-97 Practice Test with less time and less effort.

EC Council EC-Council Certified DevSecOps Engineer (ECDE) Sample Questions (Q45-Q50):

NEW QUESTION # 45

(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 STRIDE per Element.
- C. By using YAML spec-based orchestration tools.
- **D. By using Accelerator.**

Answer: D

Explanation:

ThreatModeler's Accelerator capability 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 # 46

(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. wss_agent.sh.**
- B. aws_agent.sh.
- C. ssw_agent.sh.

- D. cbs_agent.sh.

Answer: A

Explanation:

The command shown in the pre-build phase explicitly targets a script named `wss_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 # 47

(Charles Rettig has been working as a DevSecOps engineer in an IT company that develops software and web applications for IoT devices. He integrated Burp Suite with Jenkins to detect vulnerabilities and evaluate attack vectors compromising web applications. Which of the following features offered by Burp Suite minimizes false positives and helps detect invisible vulnerabilities?)

- A. MAST.
- **B. OAST.**
- C. NAST.
- D. QAST.

Answer: B

Explanation:

Burp Suite's Out-of-band Application Security Testing (OAST) feature is designed to detect vulnerabilities that do not produce immediate or visible responses during standard scanning. OAST works by triggering interactions such as DNS or HTTP callbacks, which occur outside the normal request-response cycle. This capability enables detection of blind vulnerabilities like blind SQL injection and server-side request forgery.

Because findings are based on confirmed external interactions, OAST significantly reduces false positives.

The other options listed are not valid Burp Suite features. Integrating OAST during the Build and Test stage improves the accuracy of dynamic security testing and ensures deeper coverage of complex and hard-to-detect vulnerability classes before applications are released.

NEW QUESTION # 48

(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, Frances 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. BeSECURE.**
- C. Black Duck.
- D. SonarQube.

Answer: B

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 # 49

(Judi Dench has recently joined an IT company as a DevSecOps engineer. Her organization develops software products and web applications related to electrical engineering. Judi would like to use Anchore tool for container vulnerability scanning and Software Bill of Materials (SBOM) generation. Using Anchore gype, she would like to scan the container images and file systems for known vulnerabilities, and would like to find vulnerabilities in major operating system packages such as Alpine, CentOS, Ubuntu, etc. as well as language specific packages such as Ruby, Java, etc. Which of the following commands should Judi run to scan for vulnerabilities in the image using gype?)

- A. gype packages < image >.
- B. gype < image >.
- C. gype < image > --scope all-layers.
- D. gype packages < image > --scope all-layers.

Answer: C

Explanation:

Gype is a vulnerability scanning tool used to analyze container images and file systems for known vulnerabilities across operating system and application dependencies. The most effective way to perform a comprehensive scan is by running the gype <image> --scope all-layers command. This ensures that vulnerabilities are detected across all layers of the container image, not just the final runtime layer. Containers often inherit vulnerabilities from base images or intermediate layers, making full-layer scanning essential. The packages subcommand is used for listing detected packages rather than performing vulnerability analysis. Running Gype during the Build and Test stage allows DevSecOps teams to identify vulnerable base images and dependencies early, reducing the risk of deploying insecure containers into production and supporting secure container lifecycle management.

NEW QUESTION # 50

.....

Our EC-Council Certified DevSecOps Engineer (ECDE) exam question can make you stand out in the competition. Why is that? The answer is that you get the 312-97 certificate. What certificate? Certificates are certifying that you have passed various qualifying examinations. Watch carefully you will find that more and more people are willing to invest time and energy on the 312-97 Exam, because the exam is not achieved overnight, so many people are trying to find a suitable way. Fortunately, you have found our 312-97 real exam materials, which is best for you.

312-97 Latest Braindumps: <https://www.exam4docs.com/312-97-study-questions.html>

- Enhance your Exam Preparation by using Real 312-97 Questions Search for ⇒ 312-97 ⇐ and download it for free immediately on ✓ www.practicevce.com ✓ Free 312-97 Exam
- Quiz ECCouncil - 312-97 –Efficient Pass Exam Search for 312-97 and download it for free on { www.pdfvce.com } website 312-97 Test Dumps
- 312-97 latest dumps - free ECCouncil 312-97 dumps torrent - 312-97 free braindumps Enter ⇒ www.vce4dumps.com ⇐ and search for ⇒ 312-97 to download for free Valid 312-97 Test Topics
- New 312-97 Mock Test Valid Exam 312-97 Book Updated 312-97 Dumps * Simply search for 312-97 for free download on ☀ www.pdfvce.com ☀ Valid 312-97 Test Topics
- Free 312-97 Exam ⇒ New 312-97 Real Test 312-97 Reliable Braindumps 「 www.troytecdumps.com 」 is best website to obtain ☀ 312-97 ☀ for free download Updated 312-97 Dumps
- HOT 312-97 Pass Exam: EC-Council Certified DevSecOps Engineer (ECDE) - Valid ECCouncil 312-97 Latest Braindumps Open ⇒ www.pdfvce.com enter 312-97 and obtain a free download 312-97 Practice Online
- ECCouncil - 312-97 - Valid EC-Council Certified DevSecOps Engineer (ECDE) Pass Exam Search for 312-97 and download it for free on ► www.prepawaypdf.com website 312-97 Test Guide
- 312-97 Exam Registration Free 312-97 Exam Reliable 312-97 Study Materials Search for ⇒ 312-97 and easily obtain a free download on 「 www.pdfvce.com 」 312-97 Valid Study Plan
- 312-97 latest dumps - free ECCouncil 312-97 dumps torrent - 312-97 free braindumps Immediately open www.testkingpass.com and search for 【 312-97 】 to obtain a free download Valid 312-97 Cram Materials

- 312-97 latest dumps - free ECCouncil 312-97 dumps torrent - 312-97 free braindumps □ Open “www.pdfvce.com” and search for ⇒ 312-97 ⇐ to download exam materials for free □ Exam 312-97 Bootcamp
- 312-97 Test Questions Vce □ Valid 312-97 Test Topics □ Key 312-97 Concepts □ Search for (312-97) and download it for free immediately on { www.troytecdumps.com } □ Updated 312-97 Dumps
- louisegdwp154380.corpfinwiki.com, mohamadviap015867.glifeblog.com, socialmphil.com, wiishlist.com, martinaymkd498069.myparisblog.com, listingbookmarks.com, sirketlist.com, robertuwyn686693.life3dblog.com, tessxjvq028187.answerblogs.com, kianansjm712609.blogitright.com, Disposable vapes

P.S. Free & New 312-97 dumps are available on Google Drive shared by Exam4Docs: <https://drive.google.com/open?id=1LV7heC2FjN3dkDK2--i5tg0fNYI8bFB8>