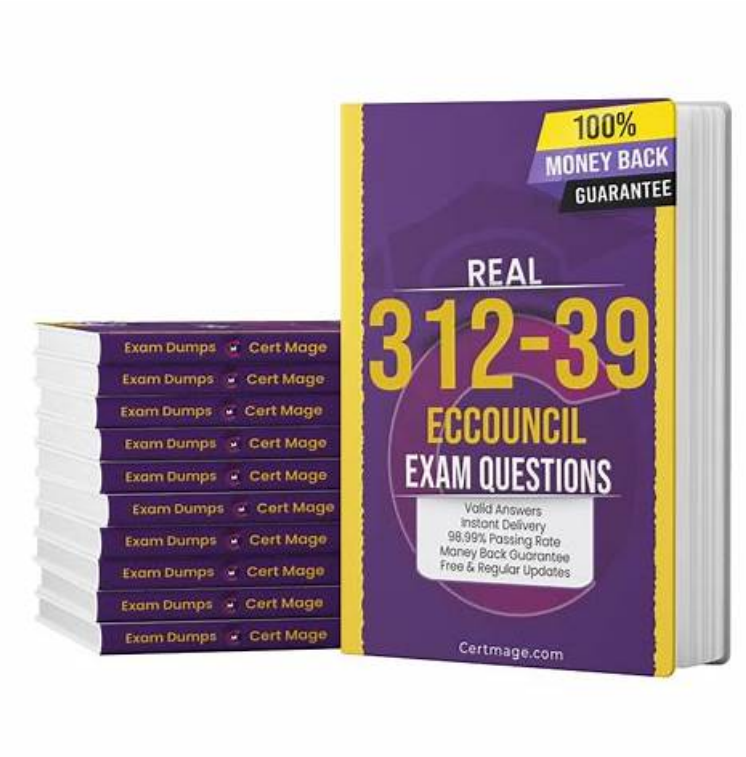
312-39 Valid Exam Discount - 312-39 Valid Exam Forum



DOWNLOAD the newest BraindumpsPrep 312-39 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=19jZ_T0UahR4iDGIbGxkLopNJK2VLk40p

Due to lots of same products in the market, maybe you have difficulty in choosing the 312-39 guide test. We can confidently tell you that our products are excellent in all aspects. You can directly select our products. Firstly, we have free trials of the 312-39 exam study materials to help you know our products. One of the great advantages is that you will soon get a feedback after you finish the exercises. So you are able to adjust your learning plan of the 312-39 Guide test flexibly. We hope that our new design can make study more interesting and colorful. You also can send us good suggestions about developing the study material.

Can You Study with Online Courses?

Yes! This is one of the best learning approaches you can adopt to crack 312-39 Exam easily. And the next section covers one such study material:

- **Certified SOC Analyst (CSA)**

  The Certified SOC Analyst (CSA) course is an intense learning program that runs for 3 days. It is a credentialing study option that equips candidates with in-demand technical skills and knowledge relating to the management of a Security Operations Center (SOC). This learning path, in particular, focuses on helping candidates master what they should know to successfully perform the fundamental SOC operations under the recognized concepts of SIEM deployment, incident response, log management along with correlation, and advanced incident detection among other skills. All in all, this course will help you understand how to perform different SOC processes and work together with CSIRT if necessary to ensure your company achieves its goals. You may want to check out the official learning page to find out more information about this course and other learning options.

>> 312-39 Valid Exam Discount <<

Perfect EC-COUNCIL Valid Exam Discount – First-grade 312-39 Valid Exam Forum

312-39 latest torrents simulate the real exam environment and does not limit the number of computer installations, which can help

you better understand the details of the exam. The online version of 312-39 test questions also support multiple devices and can be used offline permanently after being opened for the first time using the network. On buses or subways, you can use fractional time to test your learning outcomes with 312-39 Test Torrent, which will greatly increase your pro forma efficiency.

To be eligible for the 312-39 exam, candidates must have at least two years of experience in the field of information security, with a focus on SOC analysis. They must also have completed EC-COUNCIL's Certified Ethical Hacker (CEH) or EC-COUNCIL's Computer Hacking Forensic Investigator (CHFI) certification. 312-39 Exam consists of 100 multiple-choice questions and must be completed within four hours. Upon passing the exam, candidates will receive the Certified SOC Analyst (CSA) certification, which is recognized globally as a standard for SOC analysis proficiency.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q78-Q83):

NEW QUESTION # 78
Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?

- A. Tactical Threat Intelligence
- B. Operational Threat Intelligence
- C. Strategic Threat Intelligence
- D. Analytical Threat Intelligence

Answer: B

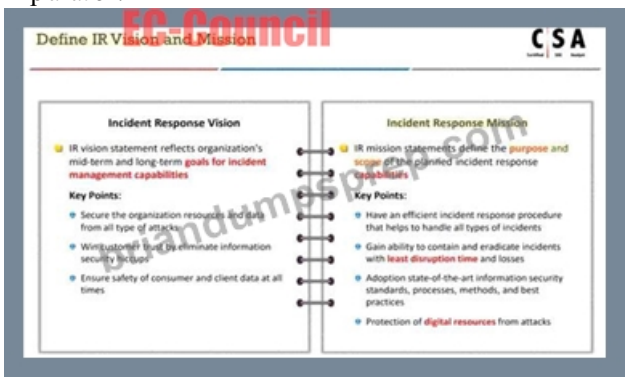
Explanation:
Operational Threat Intelligence is focused on the specifics of imminent or ongoing attacks. It provides insights into the nature of the threat, the identity of the attackers (if known), their motivation, capabilities, and objectives, as well as the tactics, techniques, and procedures (TTPs) they are likely to use. This type of intelligence is crucial for security operations managers, network operations center personnel, and incident responders because it allows them to understand and anticipate the attackers' moves, prepare specific defenses, and respond effectively to incidents.
References: The EC-Council's Certified Threat Intelligence Analyst (C|TIA) program covers the use of Operational Threat Intelligence within a SOC environment. The program emphasizes the importance of understanding and utilizing threat intelligence to predict and mitigate cyber threats. The Certified SOC Analyst (C|SA) training also discusses the role of threat intelligence in SOC operations, including Operational Threat Intelligence12.

NEW QUESTION # 79
Daniel is a member of an IRT, which was started recently in a company named Mesh Tech. He wanted to find the purpose and scope of the planned incident response capabilities.
What is he looking for?

- A. Incident Response Mission
- B. Incident Response Intelligence
- C. Incident Response Vision
- D. Incident Response Resources

Answer: A

Explanation:



NEW QUESTION # 80
In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

- A. rule-based
- B. pull-based
- C. push-based
- D. signature-based

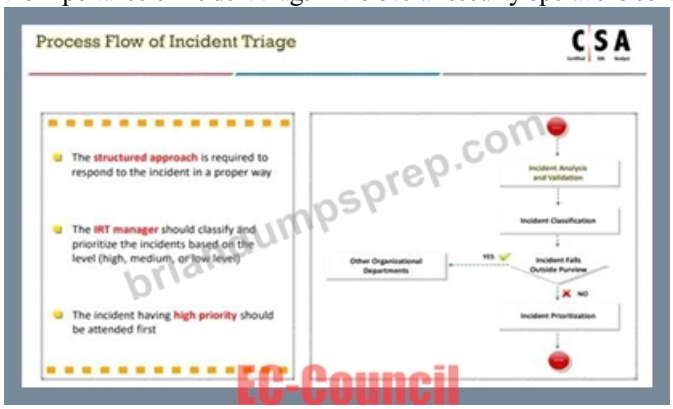
Answer: A

NEW QUESTION # 81
Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.

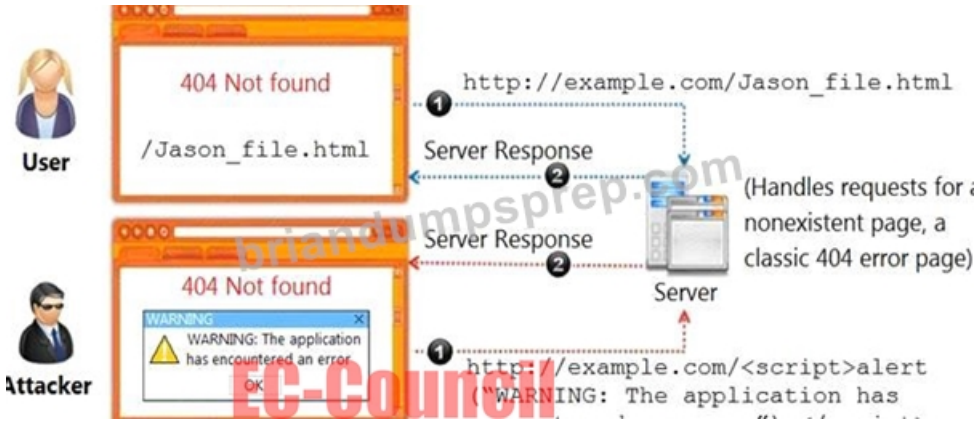
- A. Incident Triage
- B. Incident Disclosure
- C. Post-Incident Activities
- D. Incident Recording and Assignment

Answer: A

Explanation:
The stage of incident handling that involves incident analysis and validation to determine if the incident is a true incident or a false positive is known as Incident Triage. This stage is critical as it helps in prioritizing incidents based on their severity, impact, and urgency. The process of triage typically includes an initial assessment to confirm the validity of an incident, categorize its type, and determine the appropriate response.
References: The EC-Council's SOC Analyst course outlines the incident handling and response process, which includes the triage stage as a key component12. This is further supported by the NIST framework, which details the stages of incident response, including detection and analysis, where triage is a fundamental activity1. The Certified SOC Analyst (CSA) training also emphasizes the importance of incident triage in the overall security operations center (SOC) workflow3.



NEW QUESTION # 82
Identify the type of attack, an attacker is attempting on www.example.com website.



- A. Session Attack
- B. Cross-site Scripting Attack
- C. Denial-of-Service Attack
- D. SQL Injection Attack

Answer: B

Explanation:
The scenario depicted suggests an attacker is injecting a script into the URL of the website "www.example.com" which triggers an alert message. This behavior is characteristic of a Cross-site Scripting (XSS) attack. In XSS attacks, attackers exploit vulnerabilities in web applications to inject malicious scripts into web pages viewed by other users. The injected scripts can steal user data, deface web pages, or redirect users to malicious sites.
The specific attack vector here involves the attacker adding a script to the URL that causes the website to display an alert message. This indicates that the website is not properly sanitizing its inputs, which is how the attacker is able to execute the script in the context of the user's browser session.
References: The EC-Council's Certified SOC Analyst (CSA) program covers various types of cyberattacks, including XSS attacks. The CSA course materials and study guides provide detailed information on identifying, mitigating, and preventing such attacks, as well as best practices for securing web applications against them.

NEW QUESTION # 83
.....

- cerfindia.com, joshwhi204.dm-blog.com, demowithebooks.terradigita.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, dashboard.simplesphere.in, leowrig7611.pointblog.net, www.stes.tyc.edu.tw, course.biobridge.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2025 EC-COUNCIL 312-39 dumps are available on Google Drive shared by BraindumpsPrep: https://drive.google.com/open?id=19jZ_T0UahR4iDGIbGxkLopNJK2VLk40p