100% Pass Quiz Perfect EC-COUNCIL - 312-39 Boot Camp

BTW, DOWNLOAD part of ITPassLeader 312-39 dumps from Cloud Storage: https://drive.google.com/open?id=1MYzXQOuoEIeNjgyhNWiPpyitwRXqMtGM

We have three formats of study materials for your leaning as convenient as possible. Our EC-COUNCIL CSA question torrent can simulate the real operation test environment to help you pass this test. You just need to choose suitable version of our 312-39 guide question you want, fill right email then pay by credit card. It only needs several minutes later that you will receive products via email. After your purchase, 7*24*365 Day Online Intimate Service of 312-39 question torrent is waiting for you. We believe that you don't encounter failures anytime you want to learn our 312-39 guide torrent.

Career Prospects

Those candidates who achieve the passing score in the certification exam are entitled to earn the CSA certification as well as membership privileges. The certified individuals are in high demand with numerous job openings that they can explore. Without a doubt, this EC-Council certificate is a highly rewarding option that allows the professionals to take up different job roles. Some career paths that they can explore include a Security & Network Administrator, a Network Defense Analyst, a Security & Network Engineer, a Network Security Specialist, a Network Defense Technician, a Network Security Operator, and a Cybersecurity Analyst, among others.

To sit for the exam, candidates must have at least two years of experience in the field of cybersecurity and have completed the EC-COUNCIL's official training course on security operations center (SOC) analysis. 312-39 Exam consists of 100 multiple-choice questions and must be completed within 3 hours. Candidates must score at least 70% in order to pass the exam and earn the CSA certification.

Valid 312-39 Test Notes, Reliable 312-39 Test Tips

We all know that 312-39 study materials can help us solve learning problems. But if it is too complex, not only can't we get good results, but also the burden of students' learning process will increase largely. Unlike those complex and esoteric materials, our 312-39 Study Materials are not only of high quality, but also easy to learn. Our study materials do not have the trouble that users can't read or learn because we try our best to present those complex and difficult test sites in a simple way.

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q85-Q90):

NEW QUESTION # 85
Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?

- A. Throttling
- B. Ingress Filtering
- C. Egress Filtering
- D. Rate Limiting

Answer: B

Explanation:
Ingress filtering is a technique used to ensure that incoming packets are actually from the networks that they claim to originate from. This is particularly useful in mitigating IP spoofing, where an attacker might use a legitimate IP address to send malicious packets, making it appear as though the packets are coming from a trusted source. By implementing ingress filtering, networks can check that the source IP address of incoming packets is within a range that logically should be entering the network from that point. This helps in tracing back flooding attacks to their true source and is a recommended practice to protect against such attacks.
References: The concept of ingress filtering is covered in EC-Council's Certified SOC Analyst (CSA) training and is a recognized technique for protecting against flooding attacks. It is also mentioned in the context of security operations center (SOC) processes and is a part of the knowledge base required for SOC analysts12.

NEW QUESTION # 86
Banter is a threat analyst in Christine Group of Industries. As a part of the job, he is currently formatting and structuring the raw data. He is at which stage of the threat intelligence life cycle?

- A. Analysis and Production
- B. Dissemination and Integration
- C. Processing and Exploitation
- D. Collection

Answer: C

Explanation:
In the threat intelligence life cycle, the stage of Processing and Exploitation involves the formatting and structuring of raw data. This is the phase where collected data is turned into a format that can be more easily analyzed and used. Banter, as a threat analyst, is engaged in this specific activity, which indicates that he is in the Processing and Exploitation stage. This stage is crucial as it prepares the data for further analysis and production of actionable intelligence.
References: The EC-Council's Certified Threat Intelligence Analyst (C|TIA) program outlines the threat intelligence life cycle and defines the Processing and Exploitation stage as the point where data is organized and prepared for analysis. This information is detailed in the EC-Council's official training and certification resources for the SOC Analyst role12.

NEW QUESTION # 87
Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.

- A. Reconnaissance Attack

- B. Man-In-Middle Attack
- C. DoS Attack
- D. Ransomware Attack

Answer: A

Explanation:
A Reconnaissance Attack is a type of cyber attack where theattacker engages in activities to gather information about a target network before launching further attacks. This preliminary phase involves collecting data that could include network infrastructure details, system vulnerabilities, and other critical information that could be exploited in subsequent stages of an attack. Reconnaissance can be both passive, involving information gathering without directly interacting with the target system, or active, which may include more direct methods like port scanning.
References:The concept of Reconnaissance Attacks is detailed in EC-Council's cybersecurity resources, such as the Certified Threat Intelligence Analyst (C|TIA) programand articles on the Cyber Kill Chain, which describe reconnaissance as the first stage in a cyber attack12. These resources outline the methodologies and types of information gathered during reconnaissance, emphasizing its role in identifying potential attack vectors12.
Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.
pdf

NEW QUESTION # 88
Mark Reynolds, a SOC analyst at a healthcare organization, is monitoring the SIEM system when he detects a potential security threat: a series of unusual login attempts targeting critical patient data servers. After investigating the alerts and collaborating with the incident response team, the SOC determines that the threat has a "Likely" chance of occurring and could cause "Significant" damage, including operational disruptions, financial loss due to data breaches, and regulatory penalties under HIPAA. Using a standard Risk Matrix, how would this risk be categorized in terms of overall severity?

- A. Medium
- B. High
- C. Very High
- D. Low

Answer: B

Explanation:
In a standard risk matrix, overall severity is derived by combining likelihood and impact. "Likely" indicates a higher probability (not rare or unlikely), and "Significant" damage indicates a high business impact. In most common 4x4 or 5x5 matrices, pairing a high likelihood with a high impact results in a "High" risk rating (or sometimes "Very High" if both are at the extreme ends like "Almost Certain" and "Catastrophic"). Here, the wording is "Likely" and "Significant," which strongly maps to high probability and high impact, but not necessarily the highest possible category (which would typically be "Almost Certain" plus "Severe /Catastrophic"). For a healthcare organization under HIPAA, unauthorized access to patient data can trigger regulatory penalties, breach notification obligations, operational disruption, and reputational harm-so the impact is clearly material. Since the SOC has already assessed it as both probable and damaging, the risk rating should drive prioritized response: immediate containment measures, validation of access attempts, and proactive controls (MFA, conditional access, monitoring for lateral movement). Therefore, "High" is the appropriate overall severity classification.

NEW QUESTION # 89
Which of the following can help you eliminate the burden of investigating false positives?

- A. Treating every alert as high level
- B. Not trusting the security devices
- C. Keeping default rules
- D. Ingesting the context data

Answer: D

Explanation:

NEW QUESTION # 90
......

With the ever-increasing competition, people take EC-COUNCIL 312-39certification to exhibit their experience, skills, and abilities in a better way. Having Certified SOC Analyst (CSA) 312-39 certificate shows that you have better exposure than others. So, 312-39 Certification also gives you an advantage in the industry when employers seek candidates for job opportunities. However, preparing for the EC-COUNCIL 312-39 exam can be a difficult and time-consuming process.

Valid 312-39 Test Notes: https://www.itpassleader.com/EC-COUNCIL/312-39-dumps-pass-exam.html

What's more, part of that ITPassLeader 312-39 dumps now are free: https://drive.google.com/open?id=1MYzXQOuoEIeNjgyhNWiPpyitwRXqMtGM