Free PDF 2026 EC-COUNCIL The Best Reliable 312-39 Practice Materials

Top 5 Facts to Rely on EC-Council 312-39 Practice Tests

1. You get the actual EC-Council 312-39 exam experience.

2. Time management becomes easy during the actual exam.

3. Valuable insights offer more improvement scope.

4. Rigorous Practice Makes you perfect about the EC-Council 312-39 syllabus domains.

5. Self-assessment provides self-satisfaction regarding the 312-39 exam preparation.

BONUS!!! Download part of TorrentValid 312-39 dumps for free: https://drive.google.com/open?id=1BEDK3Efj-tuJQ7vNtRHQlLmH1WadmIn0

By sitting in these scenarios, you will be able to kill test anxiety. As a result, you will take the final Certified SOC Analyst (CSA) (312-39) exam with no fear. The web-based 312-39 practice exam software not only works on Windows but also on Linux, iOS, Mac, and Android. Furthermore, this online software of the Certified SOC Analyst (CSA) (312-39) practice test is compatible with Internet Explorer, MS Edge, Chrome, Firefox, Safari, and Opera.

EC-COUNCIL 312-39 Exam is designed for security professionals who are looking to advance their careers in the cybersecurity field. Certified SOC Analyst (CSA) certification is particularly valuable for those who are looking to work in security operations centers, as it provides them with the skills and knowledge needed to effectively manage and respond to security incidents. Certified SOC Analyst (CSA) certification is also useful for those who are looking to work as security consultants, as it demonstrates their expertise in security operations.

>> Reliable 312-39 Practice Materials <<

EC-COUNCIL 312-39 Valid Dumps Pdf | New 312-39 Exam Sample

EC-COUNCIL Certified SOC Analyst (CSA) Sample Questions (Q17-Q22):

NEW QUESTION # 17
InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.
Identify the job role of John.

- A. Security Analyst - L1
- B. Security Engineer
- C. Chief Information Security Officer (CISO)
- D. Security Analyst - L2

Answer: C

Explanation:
The role of finalizing strategy, policies, and procedures for a Security Operations Center (SOC) typically falls under the responsibilities of a Chief Information Security Officer (CISO). The CISO is a senior-level executive within an organization who coordinates and manages the overall strategy and defense mechanisms to protect the organization's information and technology assets. This role involves leadership and strategic decision-making, which includes establishing the SOC's framework, defining its policies, and overseeing its procedures.
References: The EC-Council provides various resources and guides that outline the roles and responsibilities within a SOC. According to the information available, a Security Analyst, whether Level 1 or Level 2, is primarily responsible for monitoring and analyzing the organization's security posture on a continuous basis.
A Security Engineer focuses on the design and implementation of security systems. In contrast, the CISO role encompasses a broader scope of strategic leadership and management, which aligns with the responsibilities described for John in the scenario12.

NEW QUESTION # 18
A healthcare organization's SIEM detects unusual HTTP requests targeting its patient portal. The requests originate from a foreign IP address and occur during non-business hours. The methods used are primarily TRACE and OPTIONS, which are rarely seen in normal web traffic. The SIEM correlates these with increased reconnaissance activity on other servers within the same subnet. What is the primary security concern with TRACE and OPTIONS requests?

- A. They allow attackers to bypass authentication controls
- B. They can be used to upload malicious payloads directly to the server
- C. They expose information about server-supported methods and request headers
- D. They make Distributed Denial of Service (DDoS) attacks easier

Answer: C

Explanation:
TRACE and OPTIONS are often associated with reconnaissance because they can reveal how a server is configured and what capabilities it supports. OPTIONS can disclose which HTTP methods are allowed (GET, POST, PUT, DELETE, etc.), helping attackers identify whether risky methods are enabled or misconfigured.
TRACE can be abused to reflect request headers back to the client, which may expose sensitive header information in certain misconfigurations and historically has been associated with cross-site tracing risks. In SOC investigations, unusual usage of TRACE/OPTIONS-especially from foreign IPs and outside business hours-often indicates probing to map the attack surface before selecting an exploit path. Uploading payloads is more associated with PUT/POST to vulnerable endpoints, not primarily TRACE/OPTIONS. DDoS facilitation is not a primary characteristic of these methods. Authentication bypass is not an inherent feature of TRACE/OPTIONS; attackers still need a separate vulnerability to bypass auth. Because the question asks for the primary concern, the best answer is that these methods can reveal supported methods and header behavior, increasing attacker knowledge and enabling follow-on exploitation attempts.

NEW QUESTION # 19

SecureTech Inc. operates critical infrastructure and applications in AWS. The SOC detects suspicious activities such as unexpected API calls, unusual outbound traffic from instances, and DNS requests to potentially malicious domains. They need a fully managed AWS security service that continuously monitors for malicious activity, analyzes CloudTrail logs, VPC Flow Logs, and DNS query logs, leverages machine learning and threat intelligence, and provides actionable findings. Which AWS service best fits?

- A. AWS Config
- B. Amazon Macie
- C. AWS Security Hub
- D. Amazon GuardDuty

Answer: D

Explanation:

Amazon GuardDuty is the fully managed AWS threat detection service designed to analyze CloudTrail events, VPC Flow Logs, and DNS logs to identify suspicious and malicious activity. It uses threat intelligence and behavioral models to detect patterns such as unusual API calls, anomalous network connections (including known malicious destinations), and suspicious DNS activity-directly matching the scenario requirements. Macie is focused on discovering and protecting sensitive data (especially in S3) through classification and data exposure detection, not broad threat detection across API/network/DNS. AWS Config is a configuration compliance and drift monitoring service; it tracks resource configurations and policy compliance but does not provide threat detection based on network and activity logs. Security Hub aggregates and normalizes findings from multiple AWS security services and partners; it is a central view and compliance

/finding management layer, but it relies on services like GuardDuty to generate threat findings. From a SOC perspective, GuardDuty provides the near-real-time detection signals the team needs, and those findings can be forwarded to SIEM/SOAR workflows for triage and response.

NEW QUESTION # 20

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. Processing and Exploitation
- C. Collection
- D. Dissemination and Integration

Answer: B

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 # 21

A rapidly growing e-commerce company wants to implement a SIEM solution to improve its security posture and comply with PCI DSS requirements. They need a solution that offers both the necessary technological features and the expertise to manage the system effectively. They also need continuous compliance support and data security assistance. Which SIEM solution is appropriate for this company?

- A. In-house SIEM
- B. Managed SIEM
- C. Security analytics
- D. Cloud-based SIEM

Answer: B

Explanation:
A managed SIEM provides both the technology platform and the operational expertise to run it effectively, which aligns with the company's need for features plus ongoing management, compliance support, and security assistance. Rapidly growing organizations often struggle to staff SIEM engineering, content tuning, and 24/7 monitoring internally. Managed SIEM offerings typically include onboarding data sources, maintaining parsers, tuning detections, handling alert triage, producing compliance reports, and advising on remediation-capabilities that directly support PCI DSS requirements and continuous audit readiness. A cloud-based SIEM is a deployment model and can be part of the answer, but it does not guarantee expert management or compliance support unless paired with a managed service. An in-house SIEM requires building and maintaining internal expertise, which conflicts with the stated need for external expertise and continuous support. "Security analytics" is a capability category, not a full SIEM solution model. From a SOC operations standpoint, managed SIEM reduces time-to-value, improves alert quality through professional tuning, and provides consistent reporting and operational coverage without needing the company to immediately build a mature internal SOC function.

NEW QUESTION # 22
......

The client can try out and download our EC-COUNCIL 312-39 Training Materials freely before their purchase so as to have an understanding of our product and then decide whether to buy them or not. The website pages of our product provide the details of our Certified SOC Analyst (CSA) learning questions.

312-39 Valid Dumps Pdf: https://www.torrentvalid.com/312-39-valid-braindumps-torrent.html