312-39인증시험공부자료100%시험패스덤프


EC-COUNCIL 312-39 Certified SOC Analyst (CSA) 4

.....

312-39퍼펙트 덤프 최신버전: https://www.passtip.net/312-39-pass-exam.html

- 시험대비 312-39덤프공부 덤프공부문제 □ □ www.itdumpskr.com □의 무료 다운로드 | 312-39 | 페이지가 지금 열립니다312-39최신버전 시험덤프문제
- 높은 통과율 312-39덤프공부 시험대비자료 □ 무료 다운로드를 위해□ 312-39 □□□를 검색하러 면⇒ www.itdumpskr.com ⇐을(를) 입력하십시오312-39덤프문제모음
- 312-39시험대비 최신버전 덤프 □ 312-39합격보장 가능 인증덤프 □ 312-39인증시험대비자료 □ 시험 자료를 무료로 다운로드하려면□ www.itdumpskr.com □을 통해□ 312-39 □를 검색하십시오312-39높은 통과율 덤프공부
- 312-39인증시험 덤프문제 ◀ 312-39시험패스 가능한 공부자료 □ 312-39인증시험 덤프문제 □ ▶ www.itdumpskr.com ◀에서 검색만 하면□ 312-39 □□□를 무료로 다운로드할 수 있습니다312-39 시험대비 최신버전 덤프
- 312-39퍼펙트 최신버전 덤프자료 □ 312-39합격보장 가능 인증덤프 □ 312-39합격보장 가능 공부 □ ▷ www.itdumpskr.com ◁에서 검색만 하면□ 312-39 □를 무료로 다운로드할 수 있습니다312-39합격보장 가능 인증덤프
- 312-39인증시험대비자료 □ 312-39퍼펙트 공부문제 □ 312-39퍼펙트 최신버전 덤프자료 □ □ www.itdumpskr.com □에서□ 312-39 □를 검색하고 무료 다운로드 받기312-39자격증덤프
- 312-39덤프공부 최신 덤프샘플문제 □ { www.itdumpskr.com }웹사이트에서□ 312-39 □를 열고 검색하여 무료 다운로드312-39최고패스자료
- 312-39덤프공부 최신 덤프샘플문제 □ □ www.itdumpskr.com □웹사이트를 열고□ 312-39 □를 검색하여 무료 다운로드312-39최신버전 시험대비 공부자료
- 312-39덤프공부최신버전 인증덤프 □ 시험 자료를 무료로 다운로드하려면□ www.itdumpskr.com □을 통해□ 312-39 □를 검색하십시오312-39높은 통과율 덤프공부
- 퍼펙트한 312-39덤프공부 덤프 최신버전 □ □ www.itdumpskr.com □웹사이트를 열고 [312-39]를 검색하여 무료 다운로드312-39최신버전 시험대비 공부자료
- 312-39덤프공부 최신 덤프로 시험패스 도전! □ □ www.itdumpskr.com □에서 검색만 하면▶ 312-39 ◀를 무료로 다운로드할 수 있습니다312-39적중율 높은 인증덤프공부

Tags: 312-39덤프공부,312-39퍼펙트 덤프 최신버전,312-39인기자격증 덤프공부자료,312-39인증덤프샘플다운,312-39시험덤프공부

312-39덤프공부 - 312-39퍼펙트덤프최신버전

참고: Itcertkr에서 Google Drive로 공유하는 무료 2026 EC-COUNCIL 312-39 시험 문제집이 있습니다: https://drive.google.com/open?id=1gyEgEyGtztgnJ7qOPRkSzSYQwXAwjKCA

EC-COUNCIL 312-39 덤프의 높은 적중율에 놀란 회원분들이 계십니다. 고객님들의 도와 EC-COUNCIL 312-39 시험을 쉽게 패스하는게 저희의 취지이자 최선을 다해 더욱 높은 적중율을 자랑할수 있다록 노력하고 있습니다. 뿐만 아니라 Itcertkr에서는한국어 온라인서비스상담, 구매후 일년무료업데이트서비스, 불합격받을수 환불혹은 덤프교환 등탄탄한 구매후 서비스를 제공해드립니다.

EC-COUNCIL 312-39: Certified SOC Analyst (CSA) 시험은 보안 산업에서 일하는 개인들에게 이상적입니다. 특히 보안 운영 센터(SOCs)에서 일하는 사람들에게 적합합니다. 이 자격증은 사이버 보안 분야에서 자신의 경력을 쌓고 싶은 IT 전문가들에게도 적합합니다.

>> 312-39인증시험 공부자료 <<

EC-COUNCIL 312-39합격보장 가능 시험, 312-39최고품질 덤프문제

EC-COUNCIL 312-39덤프구매에 관심이 있는데 선뜻 구매결정을 하지 못하는 분이라면 사이트에 있는 demo를 다운받아 보시면EC-COUNCIL 312-39시험패스에 믿음이 생길것입니다. EC-COUNCIL 312-39덤프는 시험문제변경에 따라 업데이트하여 항상 가장 최선버전이도록 유지하기 위해 최선을 다하고 있습니다.

EC-Council 312-39 (CSA)) 인증 시험은 IT 및 사이버 보안 산업의 고용주가 높이 평가하는 전 세계적으로 인정 된 인

증입니다. 인증 시험은 사이버 위협으로부터 조직을 보호 할 책임이있는 전문가의 기술과 지식을 검증하기 위해 고안되었습니다. 이 인증은 전문가가 SOC 운영에 대한 전문 지식을 보여주고 사이버 보안 분야에서 경력을 발전시키는 훌륭한 방법입니다.

최신 EC-COUNCIL CSA 312-39 무료샘플문제 (Q69-Q74):

질문 # 69
During a routine security audit, analysts discover several web servers still use a vulnerable third-party library flagged for a zero-day exploit. The vulnerability was identified previously and patches were deployed, but the application team rolled back patches due to instability and compatibility issues. The vulnerability remains unaddressed, and no alternative mitigations are in place. How should the security team classify this risk in the context of web application security?

- A. Insecure design
- B. Vulnerable and outdated components
- C. Software and data integrity failures
- D. Security logging and monitoring failures

정답：B

설명:
This is best classified as "Vulnerable and outdated components" because the organization is knowingly running a third-party library with a known exploitable vulnerability and has rolled back the available fix. In web application security, third-party dependencies are a major risk driver because attackers routinely target widely used frameworks and libraries, especially when exploit code becomes available or active exploitation is observed. Even if the rollback was motivated by stability, leaving the vulnerable component in production without compensating controls (WAF rules, disabling vulnerable functionality, strict input validation, segmentation) maintains high risk. Software and data integrity failures would focus on unauthorized changes or untrusted code deployment; the issue here is the presence of a known vulnerable dependency. Security logging/monitoring failures refer to insufficient visibility, not the root exposure. Insecure design refers to architectural weaknesses built into the application; while dependency management can be part of secure design, the immediate classification is the vulnerable component itself. From a SOC perspective, this classification drives remediation: prioritize patch-compatible fixes, upgrade dependency versions, implement compensating controls until patching is possible, and improve change management to prevent security rollback without risk acceptance and mitigation.

질문 # 70
Jackson & Co., a mid-sized law firm, is concerned about web-based cyber threats. The IT team implements a solution that serves as an intermediary for all HTTP and HTTPS requests. This allows the SOC to inspect, filter, and control web traffic to detect and block malicious websites, phishing attempts, and other online threats before they reach users. Which containment method is the organization using to gain visibility and control over web traffic?

- A. Web content filtering
- B. Whitelisting
- C. Blacklisting
- D. Proxy servers

정답：D

설명:
A proxy server acts as an intermediary between users and the internet, routing HTTP/HTTPS requests through a controlled inspection point. This provides visibility (who accessed what, when, from which device) and enables enforcement (block categories, block malicious destinations, inspect headers, apply SSL/TLS inspection where permitted, and enforce acceptable-use policies). While web content filtering is often a feature implemented through proxies or secure web gateways, the question explicitly describes an
"intermediary for all HTTP and HTTPS requests," which is the defining characteristic of a proxy.
Whitelisting and blacklisting are policy methods (allow/deny lists) that can be applied within a proxy or firewall, but they are not the architectural containment method described. From a SOC containment standpoint, proxying enables rapid response actions: block newly observed malicious domains/URLs, monitor for beaconing, and prevent users from reaching phishing infrastructure. It also supports investigations by providing centralized web activity logs for correlation with endpoint and identity telemetry. Therefore, the correct option is proxy servers.

질문 # 71
Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.
What is Ray and his team doing?

- A. Diverting the Traffic
- B. Absorbing the Attack
- C. Blocking the Attacks
- D. Degrading the services

정답： B

설명:
When a SOC team, like the one Ray is part of, provides additional bandwidth to network devices and increases the capacity of servers in response to a DoS/DDoS attack, they are implementing a strategy known as
'absorbing the attack'. This approach involves scaling up resources to handle the increased load without disrupting normal services.
Here's how it works:
* Increase Bandwidth: By increasing the bandwidth, the network can handle more traffic, which is essential when under a DoS/DDoS attack, as these attacks often flood the network with excessive traffic to overwhelm it.
* Enhance Server Capacity: Similarly, increasing server capacity allows the servers to handle more requests simultaneously. This is crucial during an attack to maintain service availability.
* Maintain Service Availability: The goal of this strategy is to keep services running and available to legitimate users, even when under attack.
* Monitor and Analyze: While absorbing the attack, it's important to monitor network traffic and analyze the attack patterns, which can help in future prevention and mitigation strategies.
References: This answer is aligned with the best practices for DoS/DDoS attack response as outlined in EC-Council's Certified SOC Analyst (CSA) training and certification program1234.
Please note that while I strive to provide accurate information, it's always best to consult the latest EC-Council SOC Analyst documents and learning resources for the most current and detailed guidance.

질문 # 72
Which of the following are the responsibilities of SIEM Agents?
1.Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
2.Normalizing data received fromvarious devices sending data to SIEM before forwarding it to the central engine.
3.Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
4.Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.

- A. 2 and 3
- B. 1 and 4
- C. 1 and 2
- D. 3 and 1

정답： C

설명:
SIEM Agents are primarily responsible for the initial stages of data processing within a SIEM system. Their duties include:
* Collecting data: SIEM Agents collect logs and other data from various devices across the network. This is a crucial step as it ensures that all relevant data is gathered for analysis.
* Normalizing data: Once the data is collected, SIEM Agents normalize it, which means they convert different log and data formats into a standardized format. This process is essential for the SIEM's central engine to analyze and correlate the data effectively.
The responsibilities of SIEM Agents generally do not include correlating data (which is typically done by the central SIEM engine) or visualizing data (which is usually a function of the SIEM's user interface or reporting tools).
References: The roles and responsibilities of SIEM Agents are outlined inEC-Council's SOC Analyst course materials and official certification guides. These resources emphasize the importance of data collection and normalization as foundational tasks performed by SIEM Agents in a Security Operations Center (SOC)12.

질문 # 73
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. Amazon GuardDuty
- D. AWS Security Hub

정답：C

설명：
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.

질문 # 74
.....