312-39試験の準備方法｜真実的な312-39関連資料試験｜最高のCertified SOC Analyst (CSA)問題と解答

BONUS！！！ It-Passports 312-39ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1S3R7Do2vdRGuJcToplQ9yxhcDhb8wgOr

私たちの312-39問題集は有名で、多くの人に知られています。利用するとき、312-39問題の精確性をみつけることができます。だから、いい好評をもらいました。それはずっと312-39問題集に取り組んでいる専門家の苦労です。そして、312-39 問題集は定期的に更新されます。できるだけ、お客様に最新版を提供します。312-39問題集を選ばない理由はないです！

試験に参加するには、候補者はサイバーセキュリティの分野で少なくとも2年の経験を持ち、セキュリティオペレーションセンター（SOC）分析に関するECカウンシルの公式トレーニングコースを修了しなければなりません。試験は100の複数選択の質問で構成されており、3時間以内に完了する必要があります。候補者は、試験に合格し、CSA認定を獲得するために、少なくとも70％を獲得する必要があります。

EC-Council 312-39認定試験は、SOC環境でのサイバー脅威に対する監視と防御を担当するIT専門家にとって重要な認定です。これは、サイバーセキュリティの分野で個人の知識とスキルを実証する世界的に認められた認定であり、さまざまな業界の雇用主によって高く評価されています。

EC-COUNCIL 312-39 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• Learn use cases that are widely used across the SIEM deployment • Gain knowledge of Incident Response Process
トピック 2	• Gain hands-on experience in SIEM use case development process • Plan, organize, and perform threat monitoring and analysis in the enterprise
トピック 3	• Gain knowledge of integrating threat intelligence into SIEM • Able to recognize attacker tools, tactics, and procedures
トピック 4	• Gain experience and extensive knowledge of Security Information and Event Management • Able to monitor emerging threat patterns and perform security threat analysis
トピック 5	• Able to develop threat cases (correlation rules), create reports • Gain a basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities
トピック 6	• Able to perform Security events and log collection, monitoring, and analysis • Gain knowledge of administering SIEM solutions

トピック 7	• Gain hands-on experience in the alert triaging process • Able to prepare briefings and reports of analysis methodology and results
トピック 8	• Able to escalate incidents to appropriate teams for additional assistance • Able to make use of varied, disparate, constantly changing threat information
トピック 9	• Gain understating of SOC and IRT collaboration for better incident response • Gain knowledge of the Centralized Log Management (CLM) process

>> 312-39関連資料 <<

312-39問題と解答、312-39資格取得

312-39練習問題のソフトテストエンジンに興味がある場合は、以下の情報をよく知っておく必要があります。ソフトテストエンジンは、最初にオンラインでパーソナルコンピューターにダウンロードしてからインストールする必要があります。 割賦後、オフラインで312-39練習問題を使用できます。 電話、iPadなどの他の電子製品にコピーすることもできます。 一方、Certified SOC Analyst (CSA)試験問題は200台以上のパソコンで使用できます。 あなたの会社の312-39練習問題のソフトテストエンジンを購入すると、非常に便利です。

EC-COUNCIL Certified SOC Analyst (CSA) 認定 312-39 試験問題 (Q82-Q87):

質問 # 82
An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company's URL as follows:
http://technosoft.com.com/<script>alert("WARNING: The application has encountered an error");</script>.
Identify the attack demonstrated in the above scenario.

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

正解：B

質問 # 83
Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

- A. DARPA
- B. HIPAA
- C. PCI-DSS
- D. FISMA

正解：C

解説：
PCI-DSS stands for Payment Card Industry Data Security Standard. It is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. The PCI-DSS is a widely recognized set of guidelines that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactivelyprotect customer account data.
References: The EC-Council's Certified SOC Analyst (CSA) course materials and study guides include information on various security standards, including PCI-DSS, which is specifically focused on the protection of account data. The course would cover the importance of adhering to such standards to ensure the security and integrity of sensitive payment card information1234.
Reference: https://library.educause.edu/topics/policy-and-law/pci-dss

質問 # 84
According to the forensics investigation process, what is the next step carried out right after collecting the evidence?

- A. Send it to the nearby police station
- B. Set a Forensic lab
- C. Create a Chain of Custody Document
- D. Call Organizational Disciplinary Team

正解：C

質問 # 85
A security team is configuring a newly deployed SIEM system. With limited resources, they must prioritize monitoring scenarios that provide the greatest security benefit. The team understands an effective SIEM relies on well-defined use cases tailored to the organization's environment. Which factor should guide their selection of use cases?

- A. Select use cases based on the availability and quality of data from existing data sources
- B. Focus on use cases required to meet industry compliance standards
- C. Prioritize use cases that address zero-day attacks
- D. Implement as many use cases as the SIEM supports to cover all threats

正解：A

解説：
Use cases should be selected based on the availability and quality of data because detections cannot work without reliable telemetry. In SOC engineering, the first constraint is data: what sources exist, how complete they are, how quickly they arrive, and whether fields are parsable and consistent. Choosing use cases that your environment can actually support produces faster time-to-value, fewer false positives, and fewer blind spots.
Prioritizing "zero-day" use cases is too vague and often unrealistic, because zero-days vary widely and require strong behavioral telemetry and baselines. Implementing as many use cases as possible spreads resources thin and increases noise, creating alert fatigue. Compliance-driven use cases are important, but if the underlying data is missing or poor quality, compliance rules will still fail operationally and can create a false sense of security. A mature approach is: start with high-value, high-feasibility detections that match available data (identity compromise, suspicious admin actions, endpoint malware, critical network anomalies), then expand as data coverage improves. Therefore, data availability and quality should guide initial use case selection.

質問 # 86
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 Recording and Assignment
- B. Incident Triage
- C. Post-Incident Activities
- D. Incident Disclosure

正解：B

解説：
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.

質問 # 87

......

激変なネット情報時代で、質の良いEC-COUNCILの312-39問題集を見つけるために、あなたは悩むことがありませんか。私たちは君がIt-Passportsを選ぶことと正確性の高いEC-COUNCILの312-39問題集を祝っています。It-PassportsのEC-COUNCILの312-39問題集が君の認定試験に合格するのに大変役に立ちます。

312-39問題と解答: https://www.it-passports.com/312-39.html

さらに、It-Passports 312-39ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1S3R7Do2vdRGuJcToplQ9yxhcDhb8wgOr