最新-素晴らしい312-85予想試験試験-試験の準備方法312-85資格問題集

無料でクラウドストレージから最新のGoShiken 312-85 PDFダンプをダウンロードする：https://drive.google.com/open?id=1dTvHYEezfe0a9MWh38v_FQRmFxOHKI5E

初心者にとって、312-85試験に合格するのはそんなに難しいことですか？実は、我々GoShikenの312-85問題集を選んで利用し、お客様は力の限りまで勉強して、合格しやすいです。万が一パースしない場合には、弊社は全額返金を承諾いたします。返金を願うのに対して、お客様は312-85に合格しない成績書を弊社に送付して、弊社は確認の後、支払い金額を全部返済します。

この認定は、セキュリティアナリスト、脅威ハンター、インシデント対応者など、サイバーセキュリティの分野で働くプロフェッショナルに最適です。また、脅威インテリジェンスのキャリアを追求することに興味のある個人にも適しています。この認定は、候補者が最新のトレンドやサイバーセキュリティ分野の動向について常に更新し続けることを示しています。

>> 312-85予想試験 <<

ECCouncil 312-85資格問題集、312-85資格専門知識

この驚くほど高く受け入れられている試験に適合するには、312-85学習教材のような上位の実践教材で準備する必要があります。彼らは時間とお金の面で最良の選択です。 312-85トレーニング準備のすべての内容は、素人にfされているのではなく、この分野のエリートによって作成されています。弊社の優秀なヘルパーによる効率に魅了された数万人の受験者を引き付けたリーズナブルな価格に沿ってみましょう。難しい難問は、312-85クイズガイドで解決します。

ECCouncil 312-85 試験は、脅威インテリジェンスに関連するさまざまな分野における候補者の知識とスキルをテストするために設計されています。試験は、3時間以内に完了する必要がある100問の多肢選択問題から構成されています。試験は、インテリジェンスデータの収集と分析、脅威インテリジェンスの方法論、脅威インテリジェンスツールやテクノロジーの使用などのトピックをカバーしています。試験に合格した候補者は、脅威インテリジェンス分野での専門知識を証明するCTIA認定を取得します。

ECCouncil Certified Threat Intelligence Analyst 認定 312-85 試験問題 (Q72-Q77):

質問 # 72
Karry, a threat analyst at an XYZ organization, is performing threat intelligence analysis. During the data collection phase, he used a data collection method that involves no participants and is purely based on analysis and observation of activities and processes going on within the local boundaries of the organization.
Identify the type data collection method used by the Karry.

- A. Passive data collection
- B. Exploited data collection
- C. Raw data collection
- D. Active data collection

正解：A

解説：
Karry's method of collecting data, which involves no active engagement with participants and is purely based on analysis and observation of activities within the organization, is known as passive data collection. This method is characterized by the non-intrusive monitoring of data and events, allowing analysts to gather intelligence without alerting potential adversaries or disrupting ongoing processes. Passive data collection is essential for maintaining operational security and obtaining an unaltered view of system and network activities.References:
* "Passive Data Collection in Cybersecurity," by Cybersecurity Guide
* "Understanding Passive and Active Data Collection for Cyber Threat Intelligence," by ThreatConnect

質問 # 73
In a team of threat analysts, two individuals were competing over projecting their own hypotheses on a given malware. However, to find logical proofs to confirm their hypotheses, the threat intelligence manager used a de-biasing strategy that involves learning strategic decision making in the circumstances comprising multistep interactions with numerous representatives, either having or without any perfect relevant information.
Which of the following de-biasing strategies the threat intelligence manager used to confirm their hypotheses?

- A. Cognitive psychology
- B. Game theory
- C. Machine learning
- D. Decision theory

正解：B

質問 # 74
Jian is a member of the security team at Trinity, Inc. He was conducting a real-time assessment of system activities in order to acquire threat intelligence feeds. He acquired feeds from sources like honeynets, P2P monitoring. infrastructure, and application logs.
Which of the following categories of threat intelligence feed was acquired by Jian?

- A. CSV data feeds
- B. Proactive surveillance feeds
- C. Internal intelligence feeds
- D. External intelligence feeds

正解：C

解説：
Internal intelligence feeds are derived from data and information collected within an organization's own networks and systems. Jian's activities, such as real-time assessment of system activities and acquiring feeds from honeynets, P2P monitoring, infrastructure, and application logs, fall under the collection of internal intelligence feeds. These feeds are crucial for identifying potential threats and vulnerabilities within the organization and form a fundamental part of a comprehensive threat intelligence program. They contrast with external intelligence feeds, which are sourced from outside the organization and include information on broader cyber threats, trends, and TTPs of threat actors.
References:
"Building an Intelligence-Led Security Program" by Allan Liska
"Threat Intelligence: Collecting, Analysing, Evaluating" by M-K. Lee, L. Healey, and P. A. Porras

質問 # 75
In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

- A. Distributed storage

- B. Object-based storage
- C. Centralized storage
- D. Cloud storage

正解：C

質問 # 76
An attacker instructs bots to use camouflage mechanism to hide his phishing and malware delivery locations in the rapidly changing network of compromised bots. In this particular technique, a single domain name consists of multiple IP addresses.
Which of the following technique is used by the attacker?

- A. Dynamic DNS
- B. DNS zone transfer
- C. DNS interrogation
- D. Fast-Flux DNS

正解：D

質問 # 77
.....