

# 312-85認証試験 & 312-85関連受験参考書

ECCouncil 312-85

Certified Threat Intelligence Analyst

1



### HOT Simulations 312-85 Pdf - High Pass-Rate ECCouncil Actual 312-85 Test: Certified Threat Intelligence Analyst

Our 312-85 study materials are simplified and compiled by many experts over many years according to the examination outline of the calendar year and industry trends. So our 312-85 learning materials are easy to be understood and grasped. There are also many people in life who want to change their industry. They often take the professional qualification exam as a stepping stone to enter an industry. If you are one of these people, [312-85 Exam Engine](#) will be your best choice.

To become certified, candidates must pass the 312-85 exam, which consists of 100 multiple-choice questions and has a time limit of three hours. 312-85 exam is challenging, and candidates are advised to have a solid understanding of the exam objectives and to prepare thoroughly using study materials and practice exams. Overall, the 312-85 certification is an excellent way for cybersecurity professionals to demonstrate their expertise in threat intelligence analysis and advance their career.

[>> Simulations 312-85 Pdf <<](#)

### UPDATED ECCouncil 312-85 PDF QUESTIONS [2023]- QUICK TIPS TO PASS

Based on the credibility in this industry, our 312-85 study braindumps have occupied a relatively larger market share and stable sources of customers. Such a startling figure -99% pass rate is not common in this field, but we have made it with our endless efforts. As this new frontier of personalizing the online experience advances, our 312-85 exam guide is equipped with comprehensive after-sale online services. It's a convenient way to contact our staff, for we have customer service people 24 hours online to deal with your difficulties. If you have any question or request for further assistance about the [312-85](#) study braindumps, you can leave us a message on the web page or email us.

HOT Simulations 312-85 Pdf - High Pass-Rate ECCouncil Actual 312-85 Test: Certified Threat Intelligence Analyst

ちなみに、Fast2test 312-85の一部をクラウドストレージからダウンロードできます：<https://drive.google.com/open?id=1axilPk5zAmsN8r-FT5MRtElja5eQ6RFX>

私たちに知られているように、Certified Threat Intelligence Analyst高い合格率は、高品質のFast2testの312-85研究急流を反映しています。試験に合格した98パーセント以上があり、これらの人々は両方ともECCouncilの312-85テストトレントを使用しました。当社の312-85ガイド急流が他の学習教材より高い合格率を持っていることは間違いありません。高いパスレートがすべての人々にとって非常に重要であることを深く知っているため、常にパスレートを改善するために最善を尽くしています。現在、合格率は99%に達しました。学習ツールとして312-85学習トレントを選択し、慎重に学習した場合、

ECCouncil 312-85（Certified Threat Intelligence Analyst）認定試験は、サイバーセキュリティの脅威インテリジェンスの分野で専門知識を習得したいと考えているプロフェッショナル向けに設計されたものです。この試験は、グローバルに認められているベンダー中立の認定であり、サイバーセキュリティ業界でキャリアを追求したいプロフェッショナルに最適です。

Eccouncil 312-85認定試験は、グローバルに認識されているベンダー中立認定です。これは、候補者が最新の脅威インテリジェンス技術とツールを完全に理解する必要がある高度なレベルの認定です。この認定は、脅威インテリジェンスの計画、収集と分析、サイバー脅威インテリジェンス、脅威インテリジェンス業務など、さまざまなトピックをカバーしています。候補者は、認定試験に合格するためにこれらのトピックをよく理解することが期待されています。

## 有用的な312-85認証試験 & 資格試験におけるリーダーオファース & 唯一無二な312-85: Certified Threat Intelligence Analyst

312-85証明書は、クライアントの知識と実用能力を向上させる実用性と役割のため、多数の証明書の中でも際立っています。テスト312-85証明書を所有することは、クライアントが仕事を見つけ、クライアントが有能な人々であることの証拠を見つけるときに重いコーリングカードを所有することと同じです。312-85クイズ準備は、クライアントがテストの準備をするのに最適なオプションです。312-85学習資料は、高い合格率とヒット率を高めます。クライアントは、それらを使用した後に高く評価し、312-85認定に合格するための重要なツールとして認識します。

CTIA試験は、情報収集、分析技術、脅威モデリング、脅威インテリジェンスの共有など、脅威インテリジェンス分析に関連する幅広いトピックをカバーしています。また、脅威インテリジェンス分析の実践に関わる法的および倫理的な考慮事項もカバーしています。この試験は、個人がデータを分析し解釈して潜在的な脅威や脆弱性を特定する能力を試験するために設計されています。

### ECCouncil Certified Threat Intelligence Analyst 認定 312-85 試験問題 (Q55-Q60):

#### 質問 # 55

A threat analyst wants to incorporate a requirement in the threat knowledge repository that provides an ability to modify or delete past or irrelevant threat data.

Which of the following requirement must he include in the threat knowledge repository to fulfil his needs?

- A. Protection ranking
- B. Evaluating performance
- C. Searchable functionality
- **D. Data management**

正解: D

解説:

Incorporating a data management requirement in the threat knowledge repository is essential to provide the ability to modify or delete past or irrelevant threat data. Effective data management practices ensure that the repository remains accurate, relevant, and up-to-date by allowing for the adjustment and curation of stored information. This includes removing outdated intelligence, correcting inaccuracies, and updating information as new insights become available. A well-managed repository supports the ongoing relevance and utility of the threat intelligence, aiding in informed decision-making and threat mitigation strategies. References:

\* "Building and Maintaining a Threat Intelligence Library," by Recorded Future

\* "Best Practices for Creating a Threat Intelligence Policy, and How to Use It," by SANS Institute

#### 質問 # 56

Mr. Bob, a threat analyst, is performing analysis of competing hypotheses (ACH). He has reached to a stage where he is required to apply his analysis skills effectively to reject as many hypotheses and select the best hypotheses from the identified bunch of hypotheses, and this is done with the help of listed evidence. Then, he prepares a matrix where all the screened hypotheses are placed on the top, and the listed evidence for the hypotheses are placed at the bottom.

What stage of ACH is Bob currently in?

- A. Evidence
- B. Diagnostics
- **C. Refinement**
- D. Inconsistency

正解: C

解説:

In the Analysis of Competing Hypotheses (ACH) process, the stage where Mr. Bob is applying analysis to reject hypotheses and select the most likely one based on listed evidence, followed by preparing a matrix with screened hypotheses and evidence, is

known as the 'Refinement' stage. This stage involves refining the list of hypotheses by systematically evaluating the evidence against each hypothesis, leading to the rejection of inconsistent hypotheses and the strengthening of the most plausible ones. The preparation of a matrix helps visualize the relationship between each hypothesis and the available evidence, facilitating a more objective and structured analysis.

References:

"Psychology of Intelligence Analysis" by Richards J. Heuer, Jr., for the CIA's Center for the Study of Intelligence

"A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis" by the CIA

#### 質問 # 57

ABC is a well-established cyber-security company in the United States. The organization implemented the automation of tasks such as data enrichment and indicator aggregation. They also joined various communities to increase their knowledge about the emerging threats. However, the security teams can only detect and prevent identified threats in a reactive approach.

Based on threat intelligence maturity model, identify the level of ABC to know the stage at which the organization stands with its security and vulnerabilities.

- A. Level 3: CTI program in place
- B. Level 1: preparing for CTI
- C. Level 0: vague where to start
- D. Level 2: increasing CTI capabilities

正解: A

解説:

ABC cyber-security company, which has implemented automation for tasks such as data enrichment and indicator aggregation and has joined various communities to increase knowledge about emerging threats, is demonstrating characteristics of a Level 3 maturity in the threat intelligence maturity model. At this level, organizations have a formal Cyber Threat Intelligence (CTI) program in place, with processes and tools implemented to collect, analyze, and integrate threat intelligence into their security operations. Although they may still be reactive in detecting and preventing threats, the existence of structured CTI capabilities indicates a more developed stage of threat intelligence maturity.

References:

\* "Building a Threat Intelligence Program," by Recorded Future

\* "The Threat Intelligence Handbook," by Chris Pace, Cybersecurity Evangelist at Recorded Future

#### 質問 # 58

SecurityTech Inc. is developing a TI plan where it can drive more advantages in less funds. In the process of selecting a TI platform, it wants to incorporate a feature that ranks elements such as intelligence sources, threat actors, attacks, and digital assets of the organization, so that it can put in more funds toward the resources which are critical for the organization's security.

Which of the following key features should SecurityTech Inc. consider in their TI plan for selecting the TI platform?

- A. Scoring
- B. Workflow
- C. Open
- D. Search

正解: A

#### 質問 # 59

Michael, a threat analyst, works in an organization named TechTop, was asked to conduct a cyber-threat intelligence analysis. After obtaining information regarding threats, he has started analyzing the information and understanding the nature of the threats.

What stage of the cyber-threat intelligence is Michael currently in?

- A. Known unknowns
- B. Unknowns unknown
- C. Unknown unknowns
- D. Known knowns

正解: A

解説:

id=1axilPk5zAmsN8r-FT5MRtElja5eQ6RFX