権威のある312-85試験過去問と更新する312-85テスト資料

BONUS！！！ It-Passports 312-85ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1k9hobMrqLKuGR8MhMZXI7r6MRuKZD6m5

ECCouncil 312-85認証試験を通るために、いいツールが必要です。ECCouncil 312-85認証試験について研究の資料がもっとも大部分になって、It-Passportsは早くてECCouncil 312-85認証試験の資料を集めることができます。弊社の専門家は経験が豊富で、研究した問題集がもっとも真題と近づいて現場試験のうろたえることを避けます。

CTIA認定試験は、サイバーセキュリティの分野で経験があり、脅威インテリジェンスを専門としている専門家向けです。この試験では、脅威分析、脅威モデリング、インテリジェンス収集、リスク管理など、幅広いトピックをカバーしています。また、候補者がさまざまなツールと手法を使用して、オープンソースインテリジェンス、マルウェア分析、ネットワークトラフィック分析などの脅威データを収集および分析する能力を評価します。

Eccouncil 312-85（認定脅威インテリジェンスアナリスト）認定試験は、高度な脅威インテリジェンススキルを習得しようとする専門家にとって不可欠な資格です。この試験では、幅広いトピックをカバーしており、成功するにはかなりの量の準備が必要です。この認定は業界で非常に尊敬されており、脅威インテリジェンス分析における専門家の専門知識を測定するためのベンチマークとして認識されています。

>> 312-85試験過去問 <<

312-85テスト資料、312-85科目対策

ECCouncil 312-85テスト質問の回答を注文する予定です。 クレジットカードが必要です。 ほとんどの場合、クレジットカードをサポートしています。 デビットカードをお持ちの場合は、クレジットカードを申請するか、他の友人に312-85テスト質問の回答の支払いを手伝ってもらってください。 通常、候補者はPayPalで支払うことをお勧めします。ここでは、PayPalアカウントを持っている必要はありません。 [PayPal]をクリックすると、クレジットカード支払いに振り替えられます。 312-85テストの質問の回答にSWREG支払いを選択した場合、一部の国では追加の税金がかかります。

Eccouncil 312-85（認定脅威インテリジェンスアナリスト）認定試験は、脅威インテリジェンスの分野で候補者の知識とスキルを検証する世界的に認められた認定です。この認定は、脅威インテリジェンスデータの収集、分析、評価を担当する専門家向けに設計されており、組織のネットワークにおける潜在的なセキュリティの脅威と脆弱性を特定します。認定試験では、脅威インテリジェンスの方法論、脅威狩猟、インシデント対応、データ分析などのさまざまなトピックをカバーしています。

ECCouncil Certified Threat Intelligence Analyst 認定 312-85 試験問題 (Q73-Q78):

質問 # 73
Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts. During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.
In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

- A. Analysis and production
- B. Dissemination and integration
- C. Planning and direction
- D. Processing and exploitation

正解：D

解説：
The phase where threat intelligence analysts convert raw data into useful information by applying various techniques, such as machine learning or statistical methods, is known as 'Processing and Exploitation'. During this phase, collected data is processed, standardized, and analyzed to extract relevant information. This is a critical step in the threat intelligence lifecycle, transforming raw data into a format that can be further analyzed and turned into actionable intelligence in the subsequent 'Analysis and Production' phase.
References:
"Intelligence Analysis for Problem Solvers" by John E. McLaughlin
"The Cyber Intelligence Tradecraft Project: The State of Cyber Intelligence Practices in the United States (Unclassified Summary)" by the Carnegie Mellon University's Software Engineering Institute

質問 # 74
Tim is working as an analyst in an ABC organization. His organization had been facing many challenges in converting the raw threat intelligence data into meaningful contextual information. After inspection, he found that it was due to noise obtained from misrepresentation of data from huge data collections. Hence, it is important to clean the data before performing data analysis using techniques such as data reduction. He needs to choose an appropriate threat intelligence framework that automatically performs data collection, filtering, and analysis for his organization.
Which of the following threat intelligence frameworks should he choose to perform such task?

- A. TC complete
- B. SIGVERIF
- C. Threat grid
- D. HighCharts

正解：C

解説：
Threat Grid is a threat intelligence and analysis platform that offers advanced capabilities for automatic data collection, filtering, and analysis. It is designed to help organizations convert raw threat data into meaningful, actionable intelligence. By employing advanced

analytics and machine learning, Threat Grid can reduce noise from large data sets, helping to eliminate misrepresentations and enhance the quality of the threat intelligence.
This makes it an ideal choice for Tim, who is looking to address the challenges of converting raw data into contextual information and managing the noise from massive data collections.References:
* "Cisco Threat Grid: Unify Your Threat Defense," Cisco
* "Integrating and Automating Threat Intelligence," by Threat Grid

質問 # 75
Which component of risk management involves evaluating and ranking risks based on their significance, allowing organizations to focus resources on addressing the most critical threats?

- A. Risk assessment
- B. Risk identification
- C. Risk prioritization
- D. Risk mitigation

正解：C

解説：
Risk Prioritization is the process of evaluating and ranking identified risks based on their likelihood, potential impact, and urgency. It helps organizations allocate resources to the most significant threats first.
This step follows risk assessment and ensures that mitigation efforts are aligned with business priorities and risk appetite.
Why the Other Options Are Incorrect:
* A. Risk identification: The initial process of recognizing potential threats or vulnerabilities.
* C. Risk assessment: Involves analyzing the probability and impact of identified risks but does not rank them.
* D. Risk mitigation: Focuses on implementing measures to reduce or eliminate risks after prioritization.
Conclusion:
The activity described-ranking risks by importance to determine response focus-is Risk Prioritization.
Final Answer: B. Risk prioritization
Explanation Reference (Based on CTIA Study Concepts):
CTIA identifies risk prioritization as the step that enables organizations to concentrate on the most severe risks after assessment, ensuring efficient allocation of defensive resources.

質問 # 76
Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts. During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.
In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

- A. Analysis and production
- B. Dissemination and integration
- C. Planning and direction
- D. Processing and exploitation

正解：D

質問 # 77
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. DNS zone transfer
- B. Dynamic DNS
- C. Fast-Flux DNS
- D. DNS interrogation

正解：C

解説：
Fast-Flux DNS is a technique used by attackers to hide phishing and malware distribution sites behind an ever-changing network of compromised hosts acting as proxies. It involves rapidly changing the association of domain names with multiple IP addresses, making the detection and shutdown of malicious sites more difficult. This technique contrasts with DNS zone transfers, which involve the replication of DNS data across DNS servers, or Dynamic DNS, which typically involves the automatic updating of DNS records for dynamic IP addresses, but not necessarily for malicious purposes. DNS interrogation involves querying DNS servers to retrieve information about domain names, but it does not involve hiding malicious content. Fast-Flux DNS specifically refers to the rapid changes in DNS records to obfuscate the source of the malicious activity, aligning with the scenario described.References:
* SANS Institute InfoSec Reading Room
* ICANN (Internet Corporation for Assigned Names and Numbers) Security and Stability Advisory Committee

質問 # 78
.....