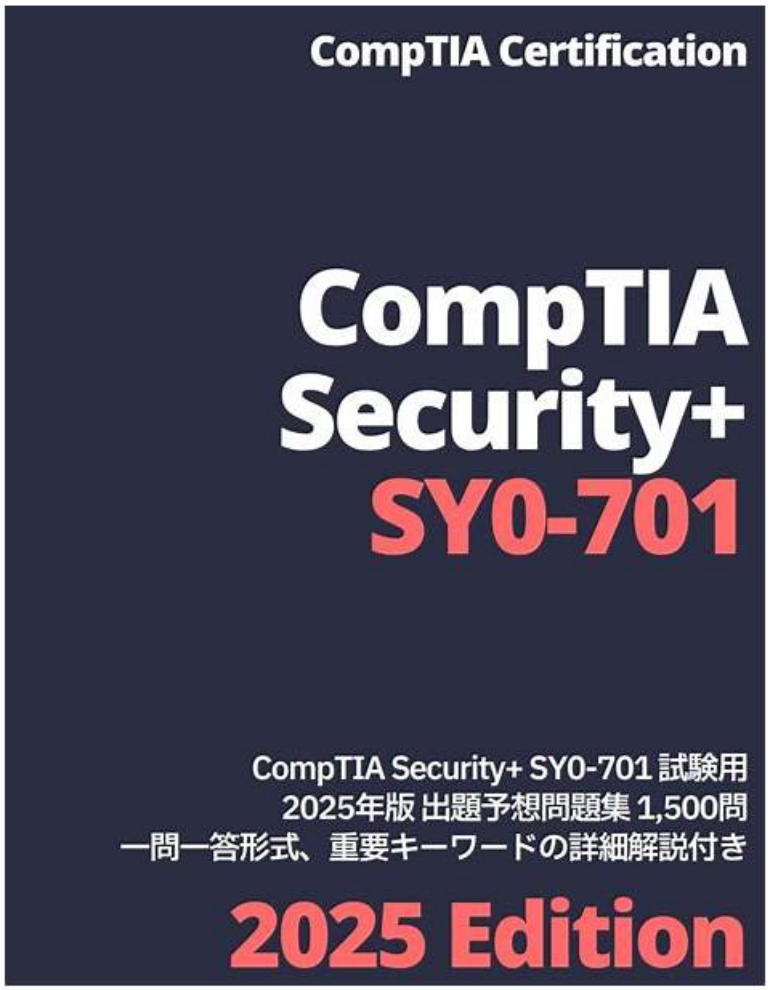
SY0-701勉強資料、SY0-701練習問題、SY0-701学習ガイド



さらに、Tech4Exam SY0-701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=1KMW7QceWU_DKpjxN6-2M8GdrpOYiJKIo

SY0-701学習教材自体については、学習者が学習教材をさまざまな角度から効率的に学習できるように複数の機能を強化します。たとえば、試験を刺激する機能は、受験者が実際のSY0-701試験の雰囲気とペースに精通し、予期しない問題の発生を回避するのに役立ちます。簡単に言えば、当社のSY0-701トレーニングガイドは品質とサービスを優先し、CompTIAお客様にSY0-701試験に合格するための新しい体験と快適な気持ちをお届けします。

CompTIA SY0-701 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• セキュリティ アーキテクチャ:ここでは、さまざまなアーキテクチャ モデルにわたるセキュリティの影響、シナリオでセキュリティ原則を適用してエンタープライズ インフラストラクチャを保護する方法、データ保護の概念と戦略の比較について学習します。このトピックでは、セキュリティ アーキテクチャにおける回復力と回復の重要性についても詳しく説明します。
トピック 2	• 一般的なセキュリティ概念:このトピックでは、さまざまな種類のセキュリティ制御、基本的なセキュリティ概念、セキュリティにおける変更管理プロセスの重要性、適切な暗号化ソリューションを使用することの重要性について説明します。

トピック 3	• 脅威、脆弱性、緩和策: このトピックでは、脅威の主体と動機の比較、一般的な脅威ベクトルと攻撃対象領域の説明、さまざまな種類の脆弱性の概要について説明します。さらに、このトピックでは、シナリオにおける悪意のあるアクティビティの指標の分析と、脅威から企業を保護するために使用される緩和手法の検討に重点を置いています。
トピック 4	• セキュリティ運用: このトピックでは、一般的なセキュリティ手法をコンピューティングリソースに適用し、適切なハードウェア、ソフトウェア、およびデータ資産管理のセキュリティへの影響に対処し、脆弱性を効果的に管理し、セキュリティ警告と監視の概念について説明します。また、セキュリティに関するエンタープライズ機能の強化、ID およびアクセス管理の実装、安全な運用のための自動化とオーケストレーションの活用についても説明します。
トピック 5	• セキュリティ プログラムの管理と監視: 最後に、このトピックでは、効果的なセキュリティ ガバナンス、リスク管理プロセス、サードパーティのリスク評価、および管理プロセスの要素について説明します。さらに、このトピックでは、セキュリティ コンプライアンスの要件、監査と評価の種類と目的、さまざまなシナリオでのセキュリティ認識プラクティスの実装に焦点を当てています。

CompTIA Security+ Certification Exam 認定 SY0-701 試験問題 (Q506-Q511):

質問 # 506
A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

- A. Quarantining
- B. Archiving
- C. Aggregating
- D. Tuning

正解：D

解説：
Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope.
Therefore, this is the best answer among the given options. References = Security Alerting and Monitoring Concepts and Tools - CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

質問 # 507
A security manager is implementing MFA and patch management. Which of the following would best describe the control type and

category? (Select two).

- A. Preventative
- B. Technical
- C. Physical
- D. Managerial
- E. Detective
- F. Administrator

正解：A、B

解説：
Multi-Factor Authentication (MFA) and patch management are both examples of preventative and technical controls. MFA prevents unauthorized access by requiring multiple forms of verification, and patch management ensures that systems are protected against vulnerabilities by applying updates. Both of these controls are implemented using technical methods, and they work to prevent security incidents before they occur.
References:
CompTIA Security+ SY0-701 Course Content: Domain 1: General Security Concepts, and Domain 4: Identity and Access Management, which cover the implementation of preventative and technical controls.

質問 # 508
A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

- A. Password spraying
- B. Pass-t he-hash
- C. Brute-force
- D. Account forgery

正解：A

解説：
Explanation
Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords12.
The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication3.
Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.
Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session4. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.
Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts5. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server. References = 1: Password spraying: An overview of password spraying attacks ... - Norton, 2: Security: Credential Stuffing vs. Password Spraying - Baeldung, 3: Brute Force Attack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition,

Types & How It Works - Fortinet

質問 # 509
A company's web filter is configured to scan the URL for strings and deny access when matches are found.
Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. :443
- B. http://
- C. www.*.com
- D. encryption=off\

正解：B

解説：
A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling",
"porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or
443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.
To
prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks.
To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.
The other options are not correct because they do not match the protocol of non-encrypted web traffic.
Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page
69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

質問 # 510
Which of the following is the best reason an organization should enforce a data classification policy to help protect its most sensitive information?

- A. The policy will result in the creation of access levels for each level of classification.
- B. The organization will have the ability to create security requirements based on classification levels.
- C. End users will be required to consider the classification of data that can be used in documents.
- D. Security analysts will be able to see the classification of data within a document before opening it.

正解：B

質問 # 511
.....

準備の時間が限られているので、多くの受験者はあなたのペースを速めることができます。 SY0-701練習資料は、SY0-701試験の質問に対する知識理解の誤りを改善し、実際のSY0-701試験に必要なものすべてを含みます。 SY0-701トレーニングガイドを選択したことを後悔することはありません。対照的に、それらは不明瞭なコンテンツを感じることなくあなたの可能性を刺激します。 SY0-701試験準備を取得した後、試験期間中に大きなストレスにさらされることはありません。

SY0-701テストサンプル問題: https://www.tech4exam.com/SY0-701-pass-shiken.html

- SY0-701資格試験 □ SY0-701復習テキスト □ SY0-701資格受験料 □ □ SY0-701 □の試験問題は（ www.passtest.jp ）で無料配信中SY0-701試験勉強書
- SY0-701最新資料 □ SY0-701復習テキスト □ SY0-701試験勉強書 □ ▹ www.goshiken.com ◃で ➡ SY0-701 □□□を検索して、無料で簡単にダウンロードできますSY0-701模擬体験
- 現実的なSY0-701技術試験 | 最初の試行で簡単に勉強して試験に合格する - 信頼できるSY0-701: CompTIA Security+ Certification Exam □ 検索するだけで ➡ jp.fast2test.com □□□から □ SY0-701 □を無料でダウンロードSY0-701資格練習
- SY0-701試験の準備方法｜検証するSY0-701技術試験試験｜更新するCompTIA Security+ Certification Examテストサンプル問題 □ “www.goshiken.com”で使える無料オンライン版▹ SY0-701 ◃の試験問題SY0-701日本語資格取得
- SY0-701関連問題資料 ☢ SY0-701試験勉強書 □ SY0-701合格受験記 □ ➽ jp.fast2test.com □サイトで□ SY0-701 □の最新問題が使えるSY0-701模擬解説集
- コンプリートSY0-701技術試験 - 資格試験のリーダー - 最新のSY0-701テストサンプル問題 □ ▸ www.goshiken.com ◂は、□ SY0-701 □を無料でダウンロードするのに最適なサイトですSY0-701無料サンプル
- 現実的なSY0-701技術試験 | 最初の試行で簡単に勉強して試験に合格する - 信頼できるSY0-701: CompTIA Security+ Certification Exam □ 時間限定無料で使える{ SY0-701 }の試験問題は □ www.mogiexam.com □サイトで検索SY0-701受験対策書
- SY0-701資格受験料 □ SY0-701最新資料 □ SY0-701関連問題資料 □ 今すぐ ➥ www.goshiken.com □を開き、⇛ SY0-701 ⇚を検索して無料でダウンロードしてくださいSY0-701トレーニング資料
- SY0-701最新資料 □ SY0-701難易度受験料 □ SY0-701資格認証攻略 □ ウェブサイト“www.mogiexam.com ”を開き、▹ SY0-701 ◃を検索して無料でダウンロードしてくださいSY0-701無料サンプル
- 権威のあるSY0-701技術試験一回合格-ハイパスレートのSY0-701テストサンプル問題 □ ⇛ www.goshiken.com ⇚から簡単に ✔ SY0-701 □✔□を無料でダウンロードできますSY0-701無料サンプル
- SY0-701最新資料 □ SY0-701資格練習 □ SY0-701模擬解説集 □ ☀ www.passtest.jp □☀□にて限定無料の ☀ SY0-701 □☀□問題集をダウンロードせよSY0-701無料サンプル
- mariyahsnwc302599.actoblog.com, anyabmlq363414.creacionblog.com, ianwcnz166401.ssnblog.com, katrinapbic522717.blogozz.com, thegreatbookmark.com, zoejzrc678652.blogsvila.com, mattiezzhc549471.verybigblog.com, harmonyaxxv966379.vigilwiki.com, mariahdkaa348985.blog-a-story.com, joanrclz085068.dreamyblogs.com, Disposable vapes

さらに、Tech4Exam SY0-701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=1KMW7QceWU_DKpjxN6-2M8GdrpOYiJKIo