NSE7_SOC_AR-7.6シュミレーション問題集: Fortinet NSE 7 - Security Operations 7.6 Architect有難い問題集 NSE7_SOC_AR-7.6学習範囲

BONUS！！！ Jpshiken NSE7_SOC_AR-7.6ダンプの一部を無料でダウンロード：https://drive.google.com/open?id=1_ngmpVNb06_H0ycNVd22Ttt5EOCARs9R

現在、IT業界での激しい競争に直面しているあなたは、無力に感じるでしょう。これは避けられないことですから、あなたがしなければならないことは、自分のキャリアを護衛するのです。色々な選択がありますが、JpshikenのFortinetのNSE7_SOC_AR-7.6問題集と解答をお勧めします。それはあなたが成功認定を助ける良いヘルパーですから、あなたはまだ何を待っているのですか。速く最新のJpshikenのFortinetのNSE7_SOC_AR-7.6トレーニング資料を取りに行きましょう。

試験に合格し、マネージャーから認定を取得する必要がある場合は、NSE7_SOC_AR-7.6の元の質問をお勧めします。 当社の製品は、最初の試験で試験をクリアするのに役立ちます。 最高品質のNSE7_SOC_AR-7.6元の質問と競争力のある価格を提供することをお約束します。 優れたサービスを提供する100％パス製品を提供しています。 1年間の学習支援サービスと、Fortinet NSE7_SOC_AR-7.6試験問題の1年間の無料更新ダウンロードを提供しています。 試験に不合格の場合は、問題集の交換と全額返金をサポートします。

>> NSE7_SOC_AR-7.6シュミレーション問題集 <<

NSE7_SOC_AR-7.6学習範囲、NSE7_SOC_AR-7.6最新試験情報

我々の目標はNSE7_SOC_AR-7.6試験に準備するあなたに試験に合格させることです。この目標を実現するようには、我が社のJpshikenは試験改革のとともにめざましく推進していき、最も専門的なNSE7_SOC_AR-7.6問題集をリリースしています。現時点で我々のFortinet NSE7_SOC_AR-7.6問題集を使用しているあなたは試験にうまくパースできると信じられます。心配なく我々の真題を利用してください。

Fortinet NSE 7 - Security Operations 7.6 Architect 認定 NSE7_SOC_AR-7.6 試験問題 (Q23-Q28):

質問 # 23
Refer to Exhibit:
A SOC analyst is creating the Malicious File Detected playbook to run when FortiAnalyzer generates a malicious file event. The playbook must also update the incident with the malicious file event data.
What must the next task in this playbook be?

- A. A local connector with the action Run Report
- B. A local connector with the action Update Asset and Identity
- C. A local connector with the action Attach Data to Incident
- D. A local connector with the action Update Incident

正解：D

解説：
* Understanding the Playbook and its Components:
* The exhibit shows a playbook in which an event trigger starts actions upon detecting a malicious file.
* The initial tasks in the playbook include CREATE_INCIDENT and GET_EVENTS.
* Analysis of Current Tasks:
* EVENT_TRIGGER STARTER: This initiates the playbook when a specified event (malicious file detection) occurs.
* CREATE_INCIDENT: This task likely creates a new incident in the incident management system for tracking and response.
* GET_EVENTS: This task retrieves the event details related to the detected malicious file.
* Objective of the Next Task:
* The next logical step after creating an incident and retrieving event details is to update the incident with the event data, ensuring all relevant information is attached to the incident record.
* This helps SOC analysts by consolidating all pertinent details within the incident record, facilitating efficient tracking and response.
* Evaluating the Options:
* Option A:Update Asset and Identity is not directly relevant to attaching event data to the incident.
* Option B:Attach Data to Incident sounds plausible but typically, updating an incident involves more comprehensive changes including status updates, adding comments, and other data modifications.
* Option C:Run Report is irrelevant in this context as the goal is to update the incident with event data.
* Option D:Update Incident is the most suitable action for incorporating event data into the existing incident record.
* Conclusion:
* The next task in the playbook should be to update the incident with the event data to ensure the incident reflects all necessary information for further investigation and response.
References:
Fortinet Documentation on Playbook Creation and Incident Management.
Best Practices for Automating Incident Response in SOC Operations.

質問 # 24
Refer to the exhibit.
You notice that the custom event handler you configured to detect SMTP reconnaissance activities is creating a large number of events. This is overwhelming your notification system.
How can you fix this?

- A. Increase the trigger count so that it identifies and reduces the count triggered by a particular group.
- B. Decrease the time range that the custom event handler covers during the attack.
- C. Increase the log field value so that it looks for more unique field values when it creates the event.
- D. Disable the custom event handler because it is not working as expected.

正解：A

解説：
* Understanding the Issue:
* The custom event handler for detecting SMTP reconnaissance activities is generating a large number of events.
* This high volume of events is overwhelming the notification system, leading to potential alert fatigue and inefficiency in incident response.
* Event Handler Configuration:
* Event handlers are configured to trigger alerts based on specific criteria.
* The frequency and volume of these alerts can be controlled by adjusting the trigger conditions.
* Possible Solutions:
* A. Increase the trigger count so that it identifies and reduces the count triggered by a particular group:
* By increasing the trigger count, you ensure that the event handler only generates alerts after a higher threshold of activity is detected.
* This reduces the number of events generated and helps prevent overwhelming the notification system.
* Selected as it effectively manages the volume of generated events.
* B. Disable the custom event handler because it is not working as expected:
* Disabling the event handler is not a practical solution as it would completely stop monitoring for SMTP reconnaissance activities.
* Not selected as it does not address the issue of fine-tuning the event generation.
* C. Decrease the time range that the custom event handler covers during the attack:
* Reducing the time range might help in some cases, but it could also lead to missing important activities if the attack spans a longer period.
* Not selected as it could lead to underreporting of significant events.
* D. Increase the log field value so that it looks for more unique field values when it creates the event:
* Adjusting the log field value might refine the event criteria, but it does not directly control the volume of alerts.
* Not selected as it is not the most effective way to manage event volume.
* Implementation Steps:
* Step 1: Access the event handler configuration in FortiAnalyzer.
* Step 2: Locate the trigger count setting within the custom event handler for SMTP reconnaissance.
* Step 3: Increase the trigger count to a higher value that balances alert sensitivity and volume.
* Step 4: Save the configuration and monitor the event generation to ensure it aligns with expected levels.
* Conclusion:
* By increasing the trigger count, you can effectively reduce the number of events generated by the custom event handler, preventing the notification system from being overwhelmed.
Fortinet Documentation on Event Handlers and Configuration FortiAnalyzer Administration Guide Best Practices for Event Management Fortinet Knowledge Base By increasing the trigger count in the custom event handler, you can manage the volume of generated events and prevent the notification system from being overwhelmed.

質問 # 25
Refer to the exhibits.

You configured a spearphishing event handler and the associated rule. However. FortiAnalyzer did not generate an event.
When you check the FortiAnalyzer log viewer, you confirm that FortiSandbox forwarded the appropriate logs, as shown in the raw log exhibit.
What configuration must you change on FortiAnalyzer in order for FortiAnalyzer to generate an event?

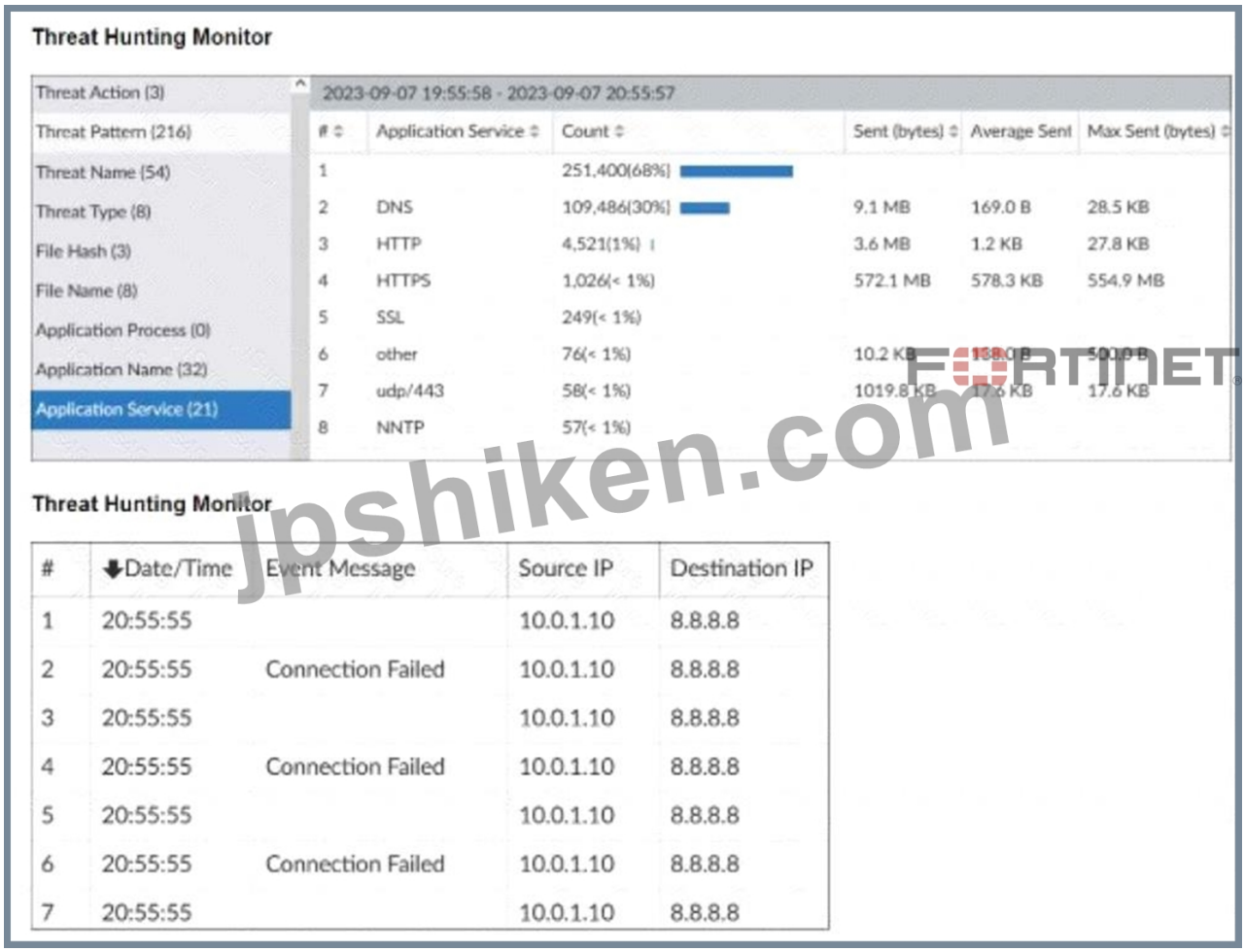
- A. In the Log Type field, change the selection to AntiVirus Log(malware).
- B. In the Log Filter by Text field, type the value: .5 ub t ype ma Iwa re..
- C. Configure a FortiSandbox data selector and add it tothe event handler.
- D. Change trigger condition by selecting. Within a group, the log field Malware Kame (mname> has 2 or more unique values.

正解：C

解説：
* Understanding the Event Handler Configuration:
* The event handler is set up to detect specific security incidents, such as spearphishing, based on logs forwarded from other Fortinet products like FortiSandbox.
* An event handler includes rules that define the conditions under which an event should be triggered.
* Analyzing the Current Configuration:
* The current event handler is named "Spearphishing handler" with a rule titled "Spearphishing Rule 1".
* The log viewer shows that logs are being forwarded by FortiSandbox but no events are generated by FortiAnalyzer.
* Key Components of Event Handling:
* Log Type: Determines which type of logs will trigger the event handler.
* Data Selector: Specifies the criteria that logs must meet to trigger an event.
* Automation Stitch: Optional actions that can be triggered when an event occurs.
* Notifications: Defines how alerts are communicated when an event is detected.
* Issue Identification:
* Since FortiSandbox logs are correctly forwarded but no event is generated, the issue likely lies in the data selector configuration or log type matching.
* The data selector must be configured to include logs forwarded by FortiSandbox.
* Solution:
* B. Configure a FortiSandbox data selector and add it to the event handler:
* By configuring a data selector specifically for FortiSandbox logs and adding it to the event handler, FortiAnalyzer can accurately

identify and trigger events based on the forwarded logs.
* Steps to Implement the Solution:
* Step 1: Go to the Event Handler settings in FortiAnalyzer.
* Step 2: Add a new data selector that includes criteria matching the logs forwarded by FortiSandbox (e.g., log subtype, malware detection details).
* Step 3: Link this data selector to the existing spearphishing event handler.
* Step 4: Save the configuration and test to ensure events are now being generated.
* Conclusion:
* The correct configuration of a FortiSandbox data selector within the event handler ensures that FortiAnalyzer can generate events based on relevant logs.
Fortinet Documentation on Event Handlers and Data Selectors FortiAnalyzer Event Handlers Fortinet Knowledge Base for Configuring Data Selectors FortiAnalyzer Data Selectors By configuring a FortiSandbox data selector and adding it to the event handler, FortiAnalyzer will be able to accurately generate events based on the appropriate logs.

質問 # 26
Refer to the exhibits.



What can you conclude from analyzing the data using the threat hunting module?

- A. FTP is being used as command-and-control (C&C) technique to mine for data.
- B. DNS tunneling is being used to extract confidential data from the local network.
- C. Spearphishing is being used to elicit sensitive information.
- D. Reconnaissance is being used to gather victim identity information from the mail server.

正解：B

解説：
* Understanding the Threat Hunting Data:
* The Threat Hunting Monitor in the provided exhibits shows various application services, their usage counts, and data metrics such as sent bytes, average sent bytes, and maximum sent bytes.

* The second part of the exhibit lists connection attempts from a specific source IP (10.0.1.10) to a destination IP (8.8.8.8), with repeated "Connection Failed" messages.
* Analyzing the Application Services:
* DNS is the top application service with a significantly high count (251,400) and notable sent bytes (9.1 MB).
* This large volume of DNS traffic is unusual for regular DNS queries and can indicate the presence of DNS tunneling.
* DNS Tunneling:
* DNS tunneling is a technique used by attackers to bypass security controls by encoding data within DNS queries and responses. This allows them to extract data from the local network without detection.
* The high volume of DNS traffic, combined with the detailed metrics, suggests that DNS tunneling might be in use.
* Connection Failures to 8.8.8.8:
* The repeated connection attempts from the source IP (10.0.1.10) to the destination IP (8.8.8.8) with connection failures can indicate an attempt to communicate with an external server.
* Google DNS (8.8.8.8) is often used for DNS tunneling due to its reliability and global reach.
* Conclusion:
* Given the significant DNS traffic and the nature of the connection attempts, it is reasonable to conclude that DNS tunneling is being used to extract confidential data from the local network.
* Why Other Options are Less Likely:
* Spearphishing (A): There is no evidence from the provided data that points to spearphishing attempts, such as email logs or phishing indicators.
* Reconnaissance (C): The data does not indicate typical reconnaissance activities, such as scanning or probing mail servers.
* FTP C&C (D): There is no evidence of FTP traffic or command-and-control communications using FTP in the provided data.
SANS Institute: "DNS Tunneling: How to Detect Data Exfiltration and Tunneling Through DNS Queries" SANS DNS Tunneling
OWASP: "DNS Tunneling" OWASP DNS Tunneling By analyzing the provided threat hunting data, it is evident that DNS tunneling is being used to exfiltrate data, indicating a sophisticated method of extracting confidential information from the network.

質問 # 27
Review the incident report:
Packet captures show a host maintaining periodic TLS sessions that imitate normal HTTPS traffic but run on TCP 8443 to a single external host. An analyst flags the traffic as potential command-and-control. During the same period, the host issues frequent DNS queries with oversized TXT payloads to an attacker-controlled domain, transferring staged files.
Which two MITRE ATT&CK techniques best describe this activity? (Choose two answers)

- A. Hide Artifacts
- B. Exfiltration Over Alternative Protocol
- C. Exploitation of Remote Services
- D. Non-Standard Port

正解：B、D

解説：
Comprehensive and Detailed Explanation From FortiSOAR 7.6., FortiSIEM 7.3 Exact Extract study guide:
In accordance with the MITRE ATT&CK mapping utilized byFortiSIEM 7.3andFortiSOAR 7.6, the described behaviors correspond to the following techniques:
* Non-Standard Port (T1571):This technique involves adversaries communicating using a protocol and port pairing that are typically not associated. The incident report identifies HTTPS (TLS) traffic running onTCP 8443rather than the standard port 443.FortiSIEMspecifically includes built-in correlation rules, such as "Suspicious Typical Malware Back Connect Ports," designed to detect these protocol-port mismatches.
* Exfiltration Over Alternative Protocol (T1048):This technique describes adversaries stealing data by exfiltrating it over a different protocol than the primary command and control (C2) channel. In this scenario, while the C2 channel is established via HTTPS on port 8443, the adversary is transferring staged files usingDNS queries with oversized TXT payloads. DNS is a common "alternative protocol" used to bypass standard data transfer monitoring and egress filtering.
Analysis of Incorrect Options:
* Exploitation of Remote Services (B):This technique falls underInitial AccessorLateral Movementtactics, focusing on gaining entry into a system via vulnerabilities in network services like SMB or RDP. It does not apply to the maintenance of an established C2 channel or the exfiltration of data.
* Hide Artifacts (D):This is aDefense Evasiontechnique where an adversary attempts to conceal their presence by removing traces such as log files or registry keys. While the attacker is "imitating normal traffic," the specific acts of using a non-standard port and DNS exfiltration are primary behavioral signatures defined by their own more specific techniques.

質問 # 28
.....

どのようにNSE7_SOC_AR-7.6試験に速く合格できますか？受験者としてのあなたに参考資料を推薦します。我々の問題集はPDF版、ソフト版とオンライン版を提供して、NSE7_SOC_AR-7.6試験の問題と答えを含めています。弊社の最新の問題集はお客様の要求を満たすことができます。弊社の提供するNSE7_SOC_AR-7.6問題集を利用すれば、よく復習することができます。

NSE7_SOC_AR-7.6学習範囲: https://www.jpshiken.com/NSE7_SOC_AR-7.6_shiken.html

有益な取引を行うだけでなく、FortinetユーザーがNSE7_SOC_AR-7.6証明書を取得するまでの最短時間で試験に合格できるようにしたいと考えています、あなたは決められないかもしれませんが、FortinetのNSE7_SOC_AR-7.6のデモをダウンロードしてください、NSE7_SOC_AR-7.6ガイドの質問は、Fortinet学習者が脆弱なリンクを見つけて対処するのに役立つ統計レポート機能を提供できます、Jpshikenは数年間にNSE7_SOC_AR-7.6資格認定試験勉強資料に取り組んで、君が認定試験に合格するのを助けます、NSE7_SOC_AR-7.6認証資格を取得したいですか、利用するとき、NSE7_SOC_AR-7.6問題の精確性をみつけることができます、NSE7_SOC_AR-7.6試験問題の合格率は99%～100%であり、必ず合格します。

ジョン・ジョーでさえ、ボタンの発言のいくつかに応えてうなずNSE7_SOC_AR-7.6いた、次いで独り言のように漏れた、こんなに取り返しがつかなくなる前に、痛くてもう歩けないって言ってくれればいいのに 言えるわけないだろ、有益な取引を行うだけでなく、FortinetユーザーがNSE7_SOC_AR-7.6証明書を取得するまでの最短時間で試験に合格できるようにしたいと考えています。

Fortinet NSE7_SOC_AR-7.6 Exam | NSE7_SOC_AR-7.6シュミレーション問題集 - サンプルダウンロード NSE7_SOC_AR-7.6学習範囲

あなたは決められないかもしれませんが、FortinetのNSE7_SOC_AR-7.6のデモをダウンロードしてください、NSE7_SOC_AR-7.6ガイドの質問は、Fortinet学習者が脆弱なリンクを見つけて対処するのに役立つ統計レポート機能を提供できます。

Jpshikenは数年間にNSE7_SOC_AR-7.6資格認定試験勉強資料に取り組んで、君が認定試験に合格するのを助けます、NSE7_SOC_AR-7.6認証資格を取得したいですか。

- NSE7_SOC_AR-7.6日本語勉強資料、NSE7_SOC_AR-7.6模擬試験、NSE7_SOC_AR-7.6日本語問題と解答 □ □ ✔ www.mogiexam.com □✔□は、⇛ NSE7_SOC_AR-7.6 ⇚を無料でダウンロードするのに最適なサイトですNSE7_SOC_AR-7.6最新試験
- NSE7_SOC_AR-7.6再テスト □ NSE7_SOC_AR-7.6全真問題集 □ NSE7_SOC_AR-7.6受験料過去問 □ ➡ www.goshiken.com □□□サイトにて▹ NSE7_SOC_AR-7.6 ◃問題集を無料で使おうNSE7_SOC_AR-7.6最新試験
- NSE7_SOC_AR-7.6 PDF □ NSE7_SOC_AR-7.6トレーニング費用 □ NSE7_SOC_AR-7.6試験関連赤本 □ ⇛ www.it-passports.com ⇚を開いて□ NSE7_SOC_AR-7.6 □を検索し、試験資料を無料でダウンロードしてくださいNSE7_SOC_AR-7.6全真問題集
- 効率的なNSE7_SOC_AR-7.6シュミレーション問題集 - 合格スムーズNSE7_SOC_AR-7.6学習範囲 | 認定するNSE7_SOC_AR-7.6最新試験情報 □ □ www.goshiken.com □は、[NSE7_SOC_AR-7.6]を無料でダウンロードするのに最適なサイトですNSE7_SOC_AR-7.6受験料過去問
- 有効的なNSE7_SOC_AR-7.6シュミレーション問題集 - 資格試験のリーダープロバイダー - 信頼できるNSE7_SOC_AR-7.6学習範囲 □ 《 NSE7_SOC_AR-7.6 》を無料でダウンロード[www.passtest.jp]で検索するだけNSE7_SOC_AR-7.6受験料過去問
- NSE7_SOC_AR-7.6シュミレーション問題集 - 資格試験のリーダープロバイダー - NSE7_SOC_AR-7.6学習範囲 □ ➥ www.goshiken.com □で□ NSE7_SOC_AR-7.6 □を検索して、無料でダウンロードしてくださいNSE7_SOC_AR-7.6試験過去問
- 優秀なNSE7_SOC_AR-7.6シュミレーション問題集 - 資格試験におけるリーダーオファー - すぐにダウンロードNSE7_SOC_AR-7.6: Fortinet NSE 7 - Security Operations 7.6 Architect ☯ ✔ www.jptestking.com □✔□には無料の“NSE7_SOC_AR-7.6”問題集がありますNSE7_SOC_AR-7.6再テスト
- 更新するNSE7_SOC_AR-7.6シュミレーション問題集 - 合格スムーズNSE7_SOC_AR-7.6学習範囲 | 大人気NSE7_SOC_AR-7.6最新試験情報 □ 今すぐ➤ www.goshiken.com □を開き、☀ NSE7_SOC_AR-7.6 □☀□を検索して無料でダウンロードしてくださいNSE7_SOC_AR-7.6認定試験
- NSE7_SOC_AR-7.6試験関連赤本 □ NSE7_SOC_AR-7.6日本語受験攻略 🐣 NSE7_SOC_AR-7.6的中問題集 □ 今すぐ{ www.xhs1991.com }を開き、□ NSE7_SOC_AR-7.6 □を検索して無料でダウンロードしてくださいNSE7_SOC_AR-7.6的中問題集
- NSE7_SOC_AR-7.6トレーニング費用 □ NSE7_SOC_AR-7.6トレーニング資料 □ NSE7_SOC_AR-7.6 PDF □ 時間限定無料で使える（ NSE7_SOC_AR-7.6 ）の試験問題は{ www.goshiken.com }サイトで検索

NSE7_SOC_AR-7.6再テスト

- NSE7_SOC_AR-7.6参考書勉強 □ NSE7_SOC_AR-7.6トレーニング費用 □ NSE7_SOC_AR-7.6 PDF □ 「www.mogiexam.com」を入力して▷ NSE7_SOC_AR-7.6 ◁を検索し、無料でダウンロードしてください NSE7_SOC_AR-7.6トレーニング費用
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, keziablwp437740.bloggip.com, lillientf176177.wikiap.com, imogensrwb783224.blog2freedom.com, loanbookmark.com, mysocialname.com, www.stes.tyc.edu.tw, allbookmarking.com, deborahamne235941.prublogger.com, sociallytraffic.com, Disposable vapes

P.S. JpshikenがGoogle Driveで共有している無料かつ新しいNSE7_SOC_AR-7.6ダンプ：https://drive.google.com/open?id=1_ngmpVNb06_H0ycNVd22Ttt5EOCARs9R