試験の準備方法-実用的なSC-200難易度受験料試験-正確的なSC-200復習対策書

2025年Fast2testの最新SC-200 PDFダンプおよびSC-200試験エンジンの無料共有：https://drive.google.com/open?id=1SfNCi6ug1csuRK-jo0p_3tpvaTTAcc2O

SC-200試験に実際に参加して資料を選択する前に、このような証明書を保持することの重要性を思い出してください。このようなSC-200証明書を取得することで、昇給、昇進の機会、上司や同僚からの信頼など、将来の多くの同意結果を習得できます。これらすべての快い結果は、もはやあなたにとって夢ではありません。

SC-200としても知られるMicrosoft Security Operations Analyst認定は、セキュリティ運用またはサイバーセキュリティでキャリアを追求したい候補者にとって求められている資格です。 Microsoft Security Technologiesを使用して、セキュリティの脅威を検出、調査、および対応する専門家のスキルを検証するように設計されています。 SC-200認定試験は、他のテクノロジーの中でも、エンドポイントのために、ID、Microsoft Cloud App Security、Azure Sentinel、およびMicrosoft Defenderのために Microsoft Defenderをナビゲートする候補者の能力を測定します。

Microsoft SC-200 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• インシデント対応の管理: このセクションでは、Microsoft Defender XDR でのアラートとインシデントへの対応について説明します。また、Microsoft Defender for Endpoint によって特定されたアラートとインシデントへの対応、および Microsoft Sentinel でのセキュリティ オーケストレーション、自動化、および対応 (SOAR) の構成についても説明します。
トピック 2	• 脅威ハンティングの実行: 試験のこのセクションでは、KQL と Microsoft Sentinel を使用して脅威をハンティングする方法について説明します。また、ワークブックを使用してデータを分析および解釈することも含まれます。
トピック 3	• 保護と検出を構成する: このセクションでは、Microsoft Defender セキュリティ テクノロジでの保護の構成、Microsoft Defender XDR での検出の構成、および Microsoft Sentinel での検出の構成について説明します。
トピック 4	• セキュリティ運用環境の管理: この試験のトピックでは、Microsoft Defender XDR での設定の構成方法、資産と環境の管理、Microsoft Sentinel ワークスペースの設計と構成、Microsoft Sentinel でのデータ ソースの取り込みについて説明します。

>> SC-200難易度受験料 <<

SC-200復習対策書 & SC-200科目対策

数年間でのIT認定試験資料向けの研究分析によって、我々社はこの業界のリーダーにだんだんなっています。弊社のチームは開発される問題集はとても全面で、受験生をMicrosoft SC-200試験に合格するのを良く助けます。周知のように、Microsoft SC-200資格認定があれば、IT業界での発展はより簡単になります。

Microsoft Security Operations Analyst 認定 SC-200 試験問題 (Q116-Q121):

質問 # 116
You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

- A. an API connection
- B. an connector
- C. a trigger
- D. authorization

正解：B

解説：
In Microsoft Sentinel, data from applications, security solutions, and services is ingested through data connectors. To integrate App1 with Sentinel and meet its monitoring or data ingestion requirements, you must configure a connector.
Microsoft Sentinel documentation specifies:
"Data connectors provide the integration point between Microsoft Sentinel and other data sources, including Microsoft services, third-party solutions, and custom applications." Connectors manage authentication, data formats, and continuous ingestion of logs or alerts into Sentinel's Log Analytics workspace.
Other options:
* API connection - supports Logic Apps but not direct Sentinel ingestion.
* Trigger - used for playbooks or automation, not data ingestion.
* Authorization - a setting used within connectors or playbooks, not configured separately.
# Correct configuration for App1: a connector

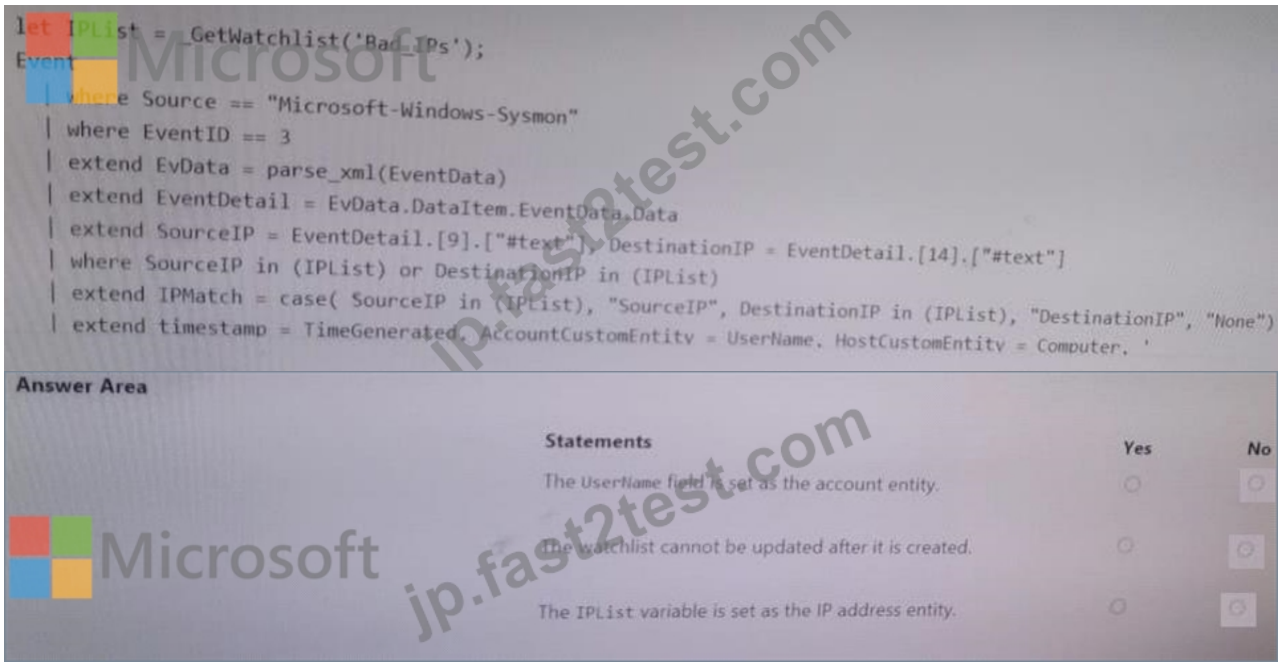
質問 # 117
You recently deployed Azure Sentinel.
You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.
You need to ensure that the Fusion rule can generate alerts.
What should you do?

- A. Add a hunting bookmark.
- B. Create a new machine learning analytics rule.
- C. Disable, and then enable the rule.
- D. Add data connectors

正解：D

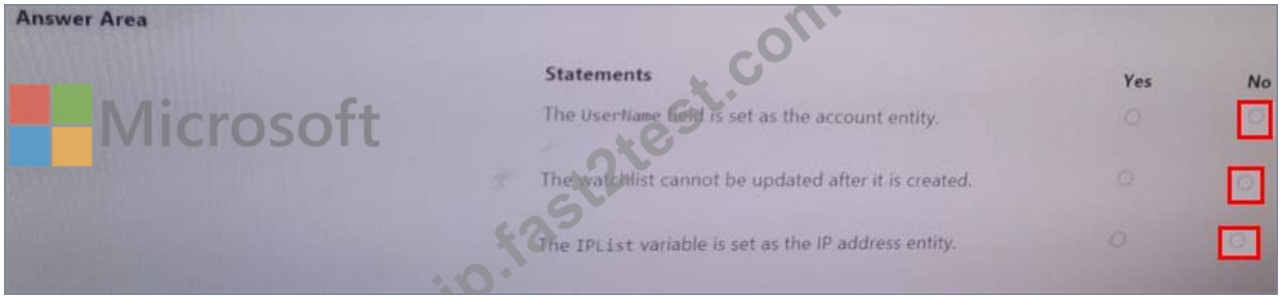
解説：
The built-in Fusion correlation rule in Microsoft Sentinel generates incidents only when it has sufficient telemetry from connected sources (e.g., Microsoft 365 Defender products, Azure AD sign-in logs, Cloud App, etc.). If no relevant data connectors are connected or sending data, Fusion will remain silent even if the rule is enabled. Connecting and authorizing the required data connectors provides the multi-signal input Fusion needs to produce incidents.

質問 # 118
You have the following SQL query.



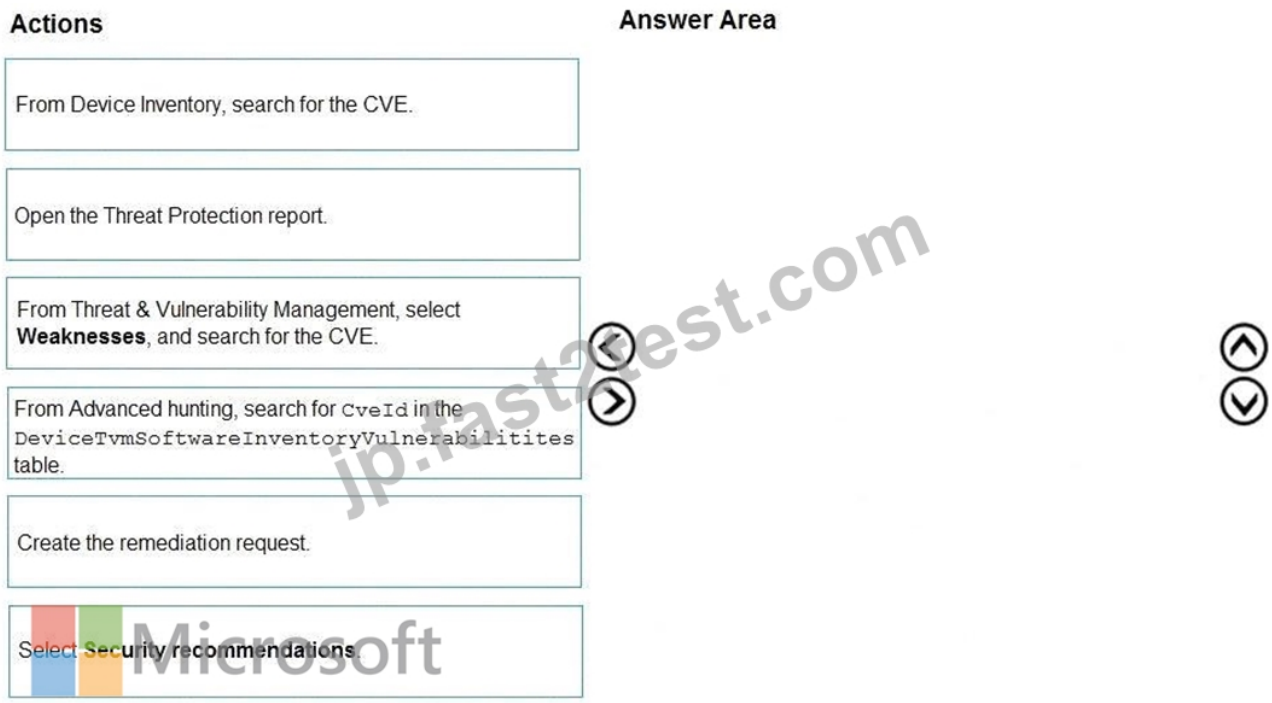
正解：

解説：



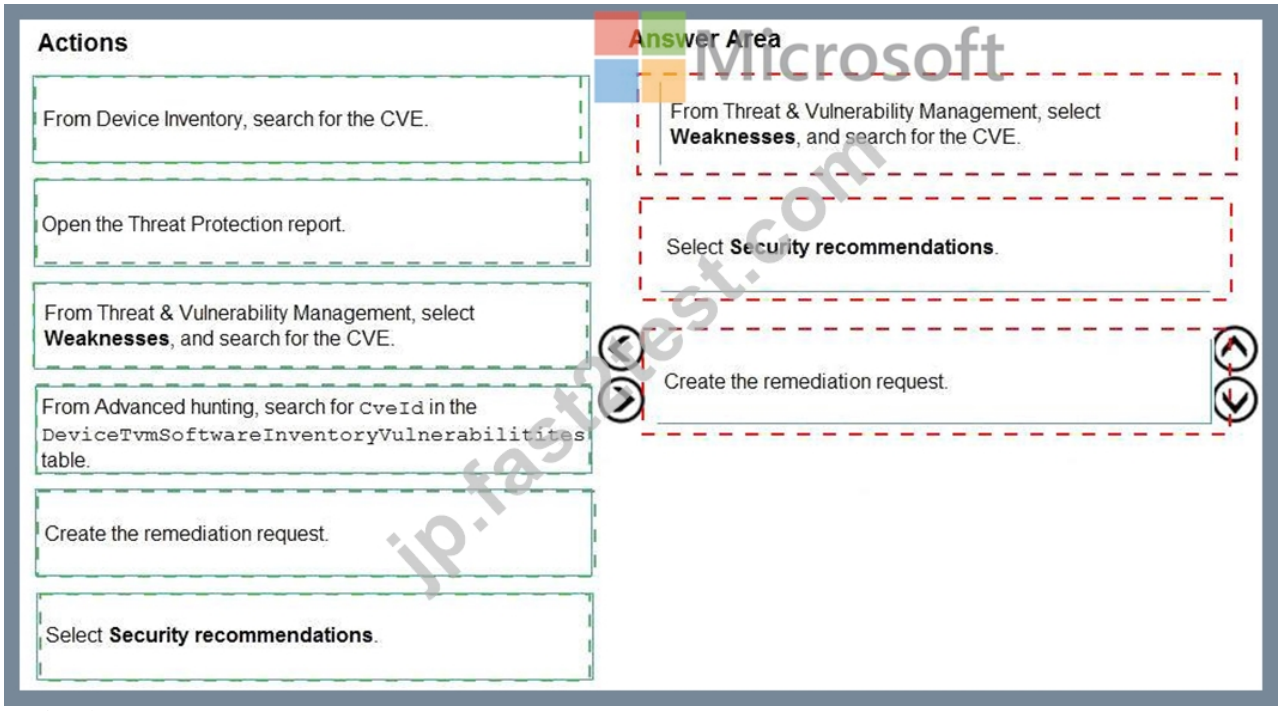
質問 # 119

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

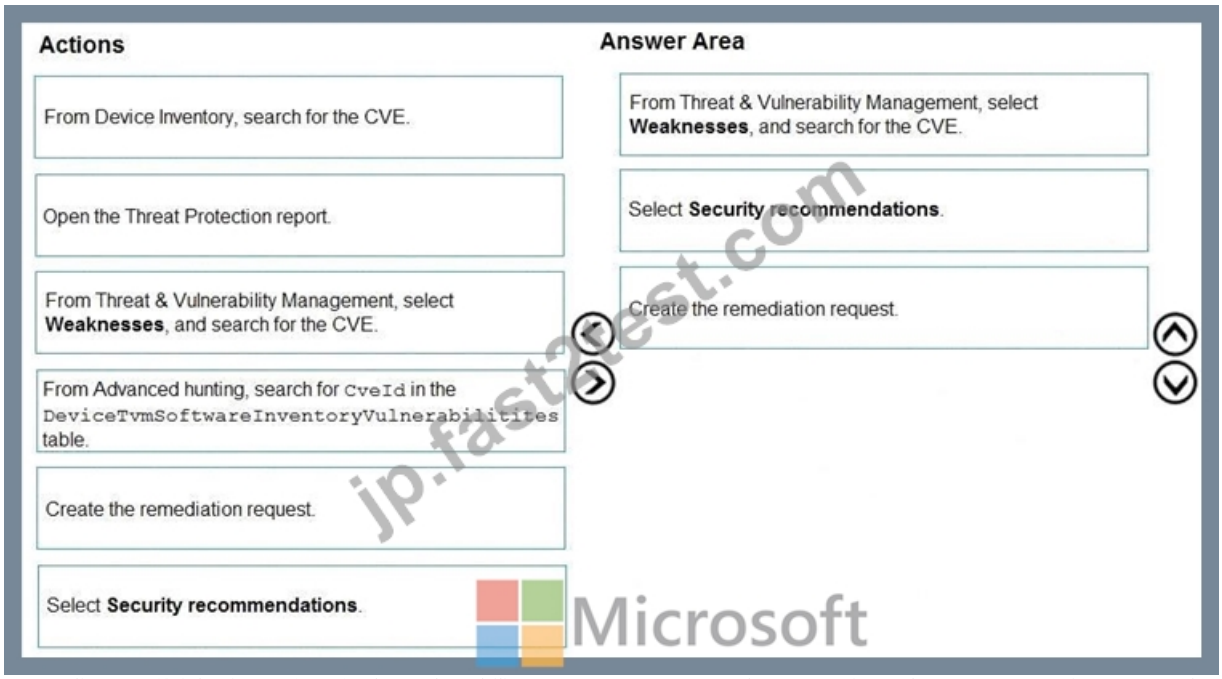


正解：

解説：



Explanation:



According to official Microsoft Defender Vulnerability Management (TVM) documentation, when a new CVE is announced, analysts can use Microsoft 365 Defender Security Center to investigate exposure and initiate remediation workflows. The proper sequence to handle such a case is:

* From Threat & Vulnerability Management (TVM), select Weaknesses and search for the CVE.In Microsoft 365 Defender, all known vulnerabilities are cataloged under the Weaknesses tab. Searching for the CVE there allows security teams to determine whether any managed assets are affected and to view metadata such as severity, exploitability, and exposure score.
* Select Security recommendations.Once the CVE is located, associated Security recommendations appear. These recommendations include actionable steps like "Update software" or "Remove vulnerable version." Each recommendation aggregates affected devices, user exposure, and related CVEs.
* Create the remediation request.From the recommendation, analysts can create a remediation request directly in the Defender portal. This task is automatically assigned to the appropriate remediation group or IT operations team, with a due date and priority based on the risk assessment.

This workflow minimizes administrative effort, ensures alignment with the principle of least privilege, and leverages Defender's built-in Threat & Vulnerability Management (TVM) automation to move from detection to remediation efficiently.

Final Sequence:
(1) From Threat & Vulnerability Management # Weaknesses
(2) Select # Security recommendations
(3) Create # Remediation request

質問 # 120
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:

* App name: App1
* IP address: 192.168.1.2
* Computer name: Device1
* Used client app: Microsoft Edge
* Email address: user1@company.com
* Sign-in URL: https://www.company.com

Which entities can be investigated by using UEBA?

- A. IP address only
- B. app name, computer name, IP address, email address, and used client app only
- C. used client app and app name only
- D. IP address and email address only

正解：D

解説：

Microsoft Sentinel UEBA (User and Entity Behavior Analytics) focuses on users and hosts (devices) and enriches data with contextual information.
When enabling UEBA with Audit logs and Signin logs, the only entities supported for investigation are:
* User accounts (email addresses)
* Hosts or devices (including IP addresses)
Other values like App name, Used client app, and Sign-in URL are attributes in log data but not tracked entities in UEBA investigations.

質問 # 121
.....

Fast2testは最高な品質で最速なスピードでMicrosoftのSC-200認定試験の資料を更新するサイトでございます。もしかすると君はほかのサイトもMicrosoftのSC-200認証試験に関する資料があるのを見つけた、比較したらFast2testが提供したのがいちばん全面的で品質が最高なことがわかりました。

SC-200復習対策書: https://jp.fast2test.com/SC-200-premium-file.html

- SC-200最新問題 □ SC-200試験内容 □ SC-200最新問題 □ ⇒ www.mogiexam.com ⇐で⇒ SC-200 ⇐を検索して、無料で簡単にダウンロードできますSC-200復習内容
- 試験の準備方法-素敵なSC-200難易度受験料試験-ユニークなSC-200復習対策書 □ サイト➥ www.goshiken.com □で（ SC-200 ）問題集をダウンロードSC-200資格参考書
- SC-200模擬試験サンプル □ SC-200勉強時間 □ SC-200復習過去問 □ 今すぐ《 www.jpexam.com 》を開き、➡ SC-200 □□□を検索して無料でダウンロードしてくださいSC-200予想試験
- 認定するMicrosoft SC-200丨完璧なSC-200難易度受験料試験丨試験の準備方法Microsoft Security Operations Analyst復習対策書 □ サイト{ www.goshiken.com }で✔ SC-200 □✔□問題集をダウンロードSC-200日本語認定
- SC-200認定資格 □ SC-200最新な問題集 □ SC-200最新問題 □ □ www.xhs1991.com □を入力して□ SC-200 □を検索し、無料でダウンロードしてくださいSC-200学習体験談
- 認定するMicrosoft SC-200丨完璧なSC-200難易度受験料試験丨試験の準備方法Microsoft Security Operations Analyst復習対策書 □ （ www.goshiken.com ）には無料の□ SC-200 □問題集がありますSC-200トレーニング
- SC-200最新な問題集 !! SC-200試験勉強書 □ SC-200復習内容 □ 《 www.passtest.jp 》で「 SC-200 」を検索して、無料で簡単にダウンロードできますSC-200受験料過去問
- 試験の準備方法-素晴らしいSC-200難易度受験料試験-完璧なSC-200復習対策書 □ “ www.goshiken.com ”で▸ SC-200 ◂を検索して、無料で簡単にダウンロードできますSC-200模擬試験サンプル
- SC-200資格参考書 □ SC-200合格体験記 □ SC-200最新な問題集 □ ☀ www.goshiken.com □☀□サイトにて▸ SC-200 ◂問題集を無料で使おうSC-200最新問題
- 試験の準備方法-素晴らしいSC-200難易度受験料試験-完璧なSC-200復習対策書 □ 今すぐ[www.goshiken.com]で[SC-200]を検索して、無料でダウンロードしてくださいSC-200英語版
- SC-200受験料過去問 □ SC-200英語版 □ SC-200認定資格 □ □ www.passtest.jp □で使える無料オンライン版□ SC-200 □ の試験問題SC-200英語版
- www.stes.tyc.edu.tw, 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, 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, www.stes.tyc.edu.tw, 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, 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, www.stes.tyc.edu.tw, class.dtechnologys.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S.Fast2testがGoogle Driveで共有している無料の2025 Microsoft SC-200ダンプ：https://drive.google.com/open?id=1SfNCi6ug1csuRK-jo0p_3tpvaTTAcc2O