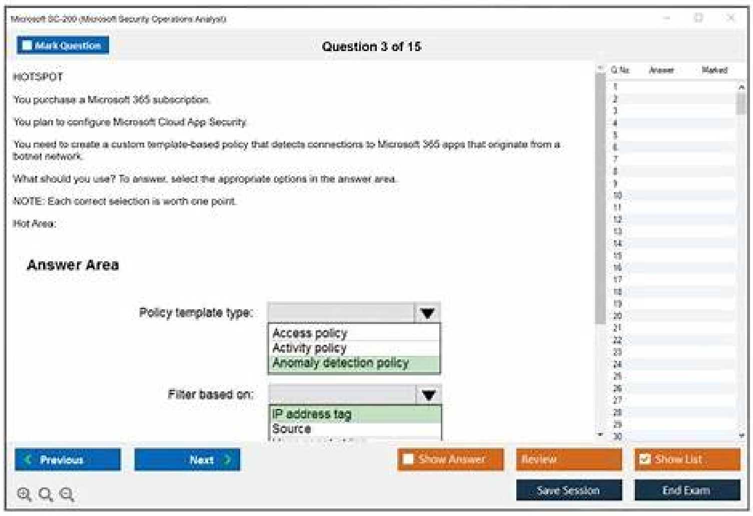
# SC-200 Test Torrent - SC-200 Latest Mock Test



HOTSPOT

You purchase a Microsoft 365 subscription.

You plan to configure Microsoft Cloud App Security.

You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Policy template type:
- Access policy
- Activity policy
- Anomaly detection policy

Filter based on:
- IP address tag
- Source

BTW, DOWNLOAD part of Exam4Docs SC-200 dumps from Cloud Storage: https://drive.google.com/open?id=11_ay0QM5u_FgpBbSsyjpoCfOr_82DEu_

The system of our SC-200 latest exam file is great. It is developed and maintained by our company's professional personnel and is dedicated to provide the first-tier service to the clients. Our system updates the SC-200 exam questions periodically and frequently to provide more learning resources and responds to the clients' concerns promptly. Our system will supplement new SC-200 latest exam file and functions according to the clients' requirements and surveys the clients' satisfaction degrees about our SC-200 cram materials. Our system will do an all-around statistics of the sales volume of our SC-200 exam questions at home and abroad and our clients' positive feedback rate of our SC-200 latest exam file. Our system will deal with the clients' online consultation and refund issues promptly and efficiently. So our system is great.

## Skills measured

- Mitigate threats using Microsoft 365 Defender (25-30%)
- Mitigate threats using Azure Sentinel (40-45%)
- Mitigate threats using Azure Defender (25-30%)

The Microsoft SC-200 exam is divided into several sections, including threat management, endpoint security, identity and access management, cloud security, and compliance management. Each section tests the candidate's knowledge and skills in a specific area of security operations, making it a comprehensive exam that covers all aspects of security operations.

Microsoft SC-200 Certification Exam is aimed at professionals who work in a security operations center (SOC) and are responsible for monitoring, detecting, and responding to security threats. Microsoft Security Operations Analyst certification validates the candidate's ability to use Microsoft security technologies to identify and mitigate security risks, as well as to manage and monitor security operations. It also tests the candidate's knowledge of threat intelligence, data analysis, incident response, and compliance.

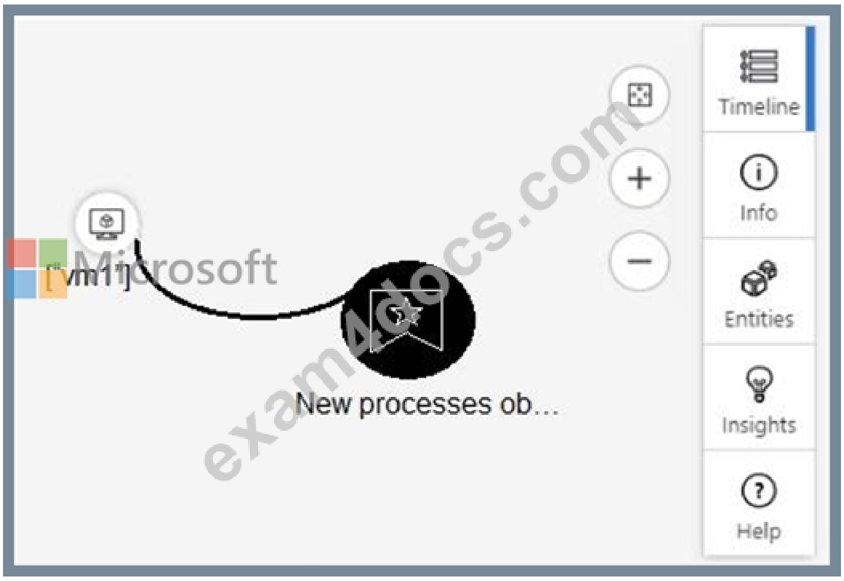
**>> SC-200 Test Torrent <<**

## SC-200 Exam Test Torrent- Updated SC-200 Latest Mock Test Pass Success

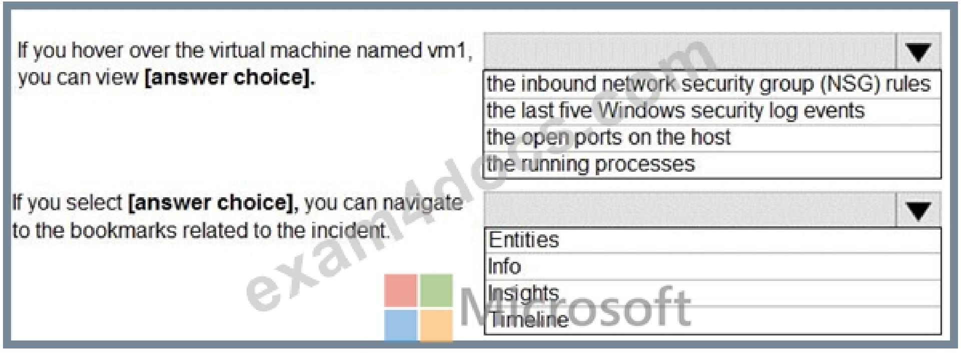
Before the clients buy our SC-200 guide prep they can have a free download and tryout. The client can visit the website pages of our product and understand our SC-200 study materials in detail. You can see the demo, the form of the software and part of our titles. To better understand our SC-200 Preparation questions, you can also look at the details and the guarantee. So it is convenient for you to have a good understanding of our SC-200 exam questions before you decide to buy our SC-200 training materials.

## Microsoft Security Operations Analyst Sample Questions (Q329-Q334):

**NEW QUESTION # 329**
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



If you hover over the virtual machine named vm1, you can view **[answer choice].**

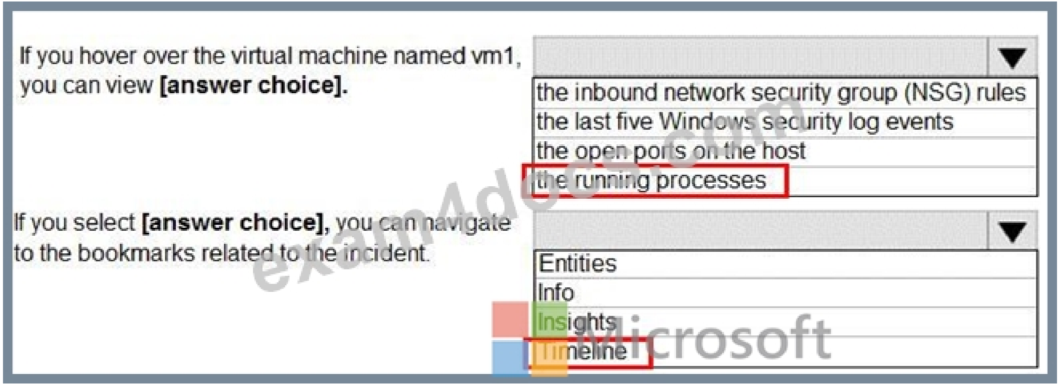
- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

**Answer:**

Explanation:



If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- [✓ the running processes]

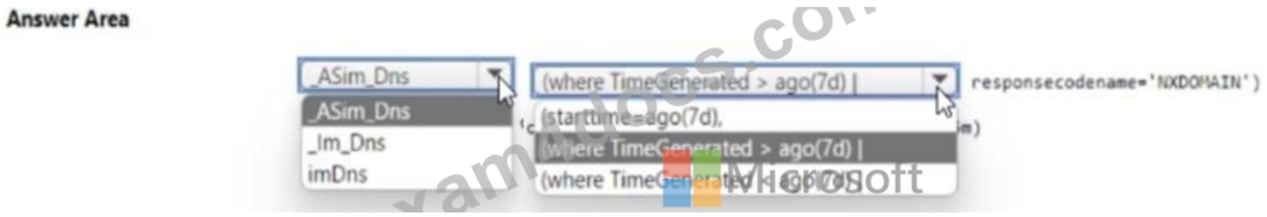
If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- [✓ Timeline]

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive

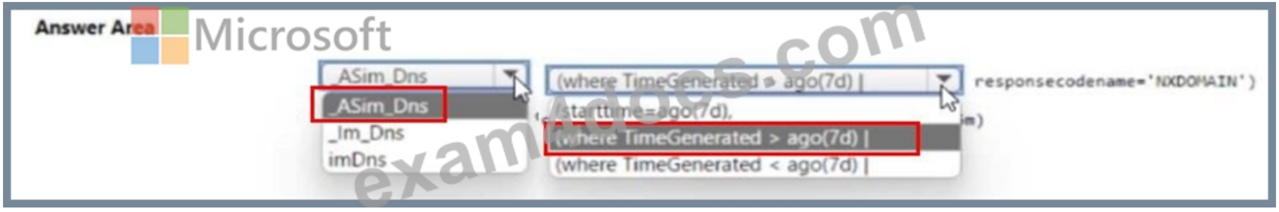
**NEW QUESTION # 330**

You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements. How should you complete the Query? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.


Answer Area
_ASim_Dns
_ASim_Dns
_Im_Dns
imDns
(where TimeGenerated > ago(7d) |
(starttime=ago(7d),
(where TimeGenerated > ago(7d) |
(where TimeGenerated < ago(7d) |
responsecodename='NXDOMAIN')

**Answer:**

Explanation:

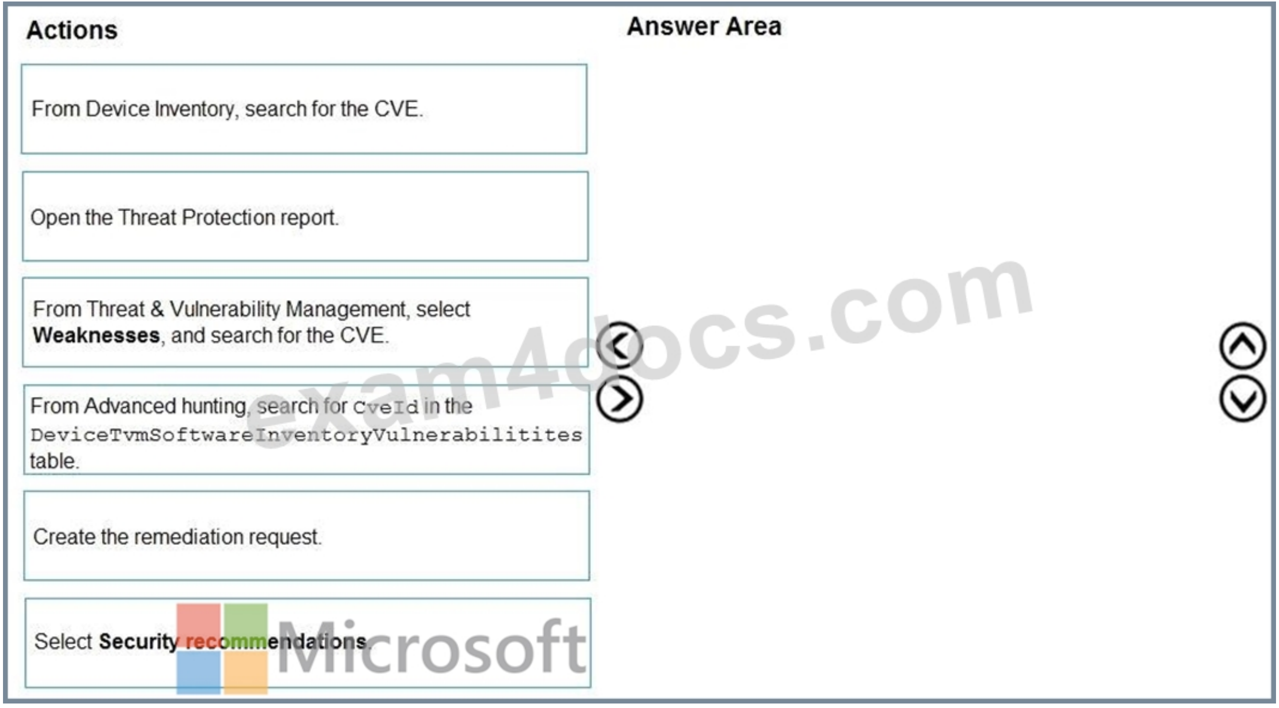

Answer Area
_ASim_Dns
_ASim_Dns
_Im_Dns
imDns
(where TimeGenerated > ago(7d) |
(starttime=ago(7d),
(where TimeGenerated > ago(7d) |
(where TimeGenerated < ago(7d) |
responsecodename='NXDOMAIN')

**NEW QUESTION # 331**

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.



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

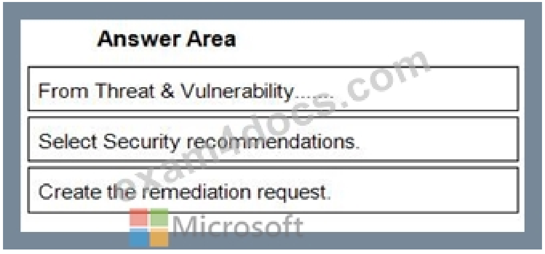
Create the remediation request.

Select **Security recommendations**

Answer Area

**Answer:**

Explanation:



Answer Area

From Threat & Vulnerability.......

Select Security recommendations.

Create the remediation request.

1 - From Threat & Vulnerability.......

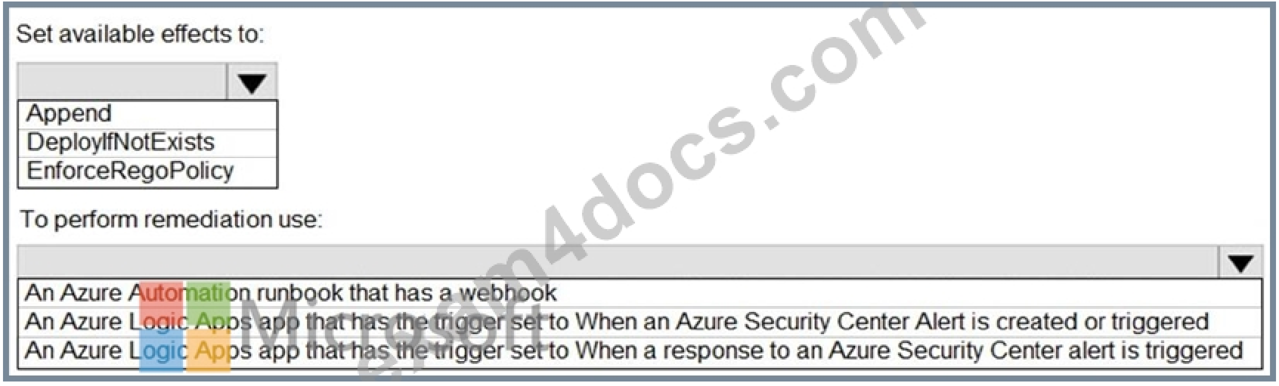
2 - Select Security recommendations.

3 - Create the remediation request.

Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

**NEW QUESTION # 332**

You have an Azure subscription that uses Azure Defender.
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.
You need to create an Azure policy that will perform threat remediation automatically.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Set available effects to:

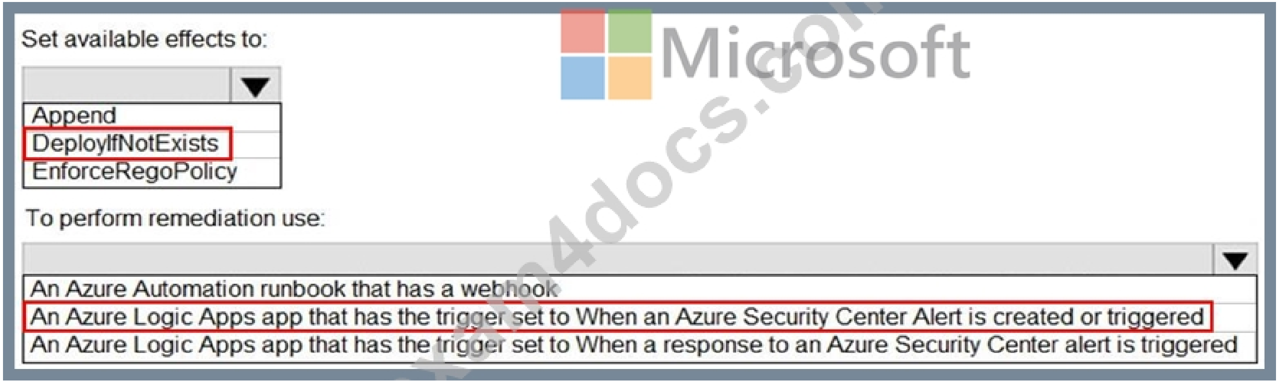
▼
- Append
- DeployIfNotExists
- EnforceRegoPolicy

To perform remediation use:

▼
- An Azure Automation runbook that has a webhook
- An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

**Answer:**

Explanation:



Set available effects to:

▼
- Append
- [✓ DeployIfNotExists]
- EnforceRegoPolicy

To perform remediation use:

▼
- An Azure Automation runbook that has a webhook
- [✓ An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered]
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

**NEW QUESTION # 333**

You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

- A. Incidents
- B. Playbooks
- C. Analytics
- D. Threat intelligence

**Answer: A**

Explanation:
In Microsoft Sentinel, playbooks (Logic Apps) that are connected to Sentinel are most commonly run in context of an incident. From the Incidents blade, you select an incident, then choose Actions # Run playbook to trigger a manual test against that specific incident's entities and alert context. This is the recommended way to validate playbook inputs (entities, alert details, incident properties) and permissions end-to-end without changing analytics rules. While the Playbooks blade shows the Logic Apps and their connections, the incident view is where Sentinel exposes manual execution with full security operations context (assignments,

comments, evidence), which is what "test a playbook manually in the Azure portal (from Sentinel)" refers to.

**NEW QUESTION # 334**

......

SWREG payment costs more tax. Especially for part of countries, intellectual property taxation will be collected by your countries if you use SWREG payment for SC-200 exam test engine. So if you want to save money, please choose PayPal. Here choosing PayPal doesn't need to have a PayPal. In fact here you should have credit card. If you click PayPal payment, it will automatically transfer to credit card payment for SC-200 Exam Test engine. On the other hands, PayPal have strict restriction for sellers account to keep buyers' benefits, so that you can share worry-free purchasing for SC-200 exam test engine.

**SC-200 Latest Mock Test**: https://www.exam4docs.com/SC-200-study-questions.html

- 2025 Microsoft SC-200: Microsoft Security Operations Analyst Unparalleled Test Torrent □ Open 《 www.getvalidtest.com 》 enter 「 SC-200 」 and obtain a free download □Valid SC-200 Cram Materials
- Actual SC-200 Test □ SC-200 Test Prep □ SC-200 Free Download Pdf □ Search on □ www.pdfvce.com □ for （ SC-200 ） to obtain exam materials for free download □SC-200 Exam Objectives
- Valid SC-200 Cram Materials □ SC-200 Reliable Exam Braindumps □ Free SC-200 Exam Dumps □ Download { SC-200 } for free by simply entering 【 www.examcollectionpass.com 】 website □SC-200 Pass Rate
- Exam SC-200 Guide □ Free SC-200 Exam Dumps □ SC-200 Pass Rate □ Search for □ SC-200 □ and download it for free immediately on ➤ www.pdfvce.com □ □New Study SC-200 Questions
- Exam SC-200 Voucher □ Downloadable SC-200 PDF □ SC-200 Valid Braindumps □ Open □ www.pdfdumps.com □ enter ➠ SC-200 □ and obtain a free download □SC-200 Free Download Pdf
- SC-200 Reliable Study Guide □ SC-200 Reliable Exam Braindumps ♣ New Study SC-200 Questions □ Open ▸ www.pdfvce.com ◂ enter 《 SC-200 》 and obtain a free download □Exam SC-200 Guide
- Exam SC-200 Papers □ SC-200 Reliable Study Guide □ Free SC-200 Exam Dumps □ Search for 「 SC-200 」 and download it for free immediately on ➻ www.examcollectionpass.com □ ⓂSC-200 Pass Rate
- Pass Guaranteed Quiz 2025 Unparalleled SC-200: Microsoft Security Operations Analyst Test Torrent □ Immediately open { www.pdfvce.com } and search for ➡ SC-200 □□□ to obtain a free download □SC-200 Latest Torrent
- SC-200 Test Prep □ Exam SC-200 Papers □ SC-200 Pass Rate □ Open （ www.testsdumps.com ） and search for □ SC-200 □ to download exam materials for free □SC-200 Valid Braindumps
- Free PDF Quiz 2025 Useful Microsoft SC-200: Microsoft Security Operations Analyst Test Torrent □ Go to website （ www.pdfvce.com ） open and search for [ SC-200 ] to download for free ✉SC-200 Latest Torrent
- SC-200 Reliable Exam Braindumps □ SC-200 Latest Torrent □ Actual SC-200 Test □ Search for ⇛ SC-200 ⇚ and download it for free immediately on ➠ www.itcerttest.com □ □SC-200 Pass Rate
- lms.slikunedu.in, elearning.eauqardho.edu.so, shikhaw.com, mikemil988.mybuzzblog.com, 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, shortcourses.russellcollege.edu.au, www.teachtechacademy.com.ng, 47.121.119.212, Disposable vapes

BONUS!!! Download part of Exam4Docs SC-200 dumps for free: https://drive.google.com/open?id=11_ay0QM5u_FgpBbSsyjpoCfOr_82DEu_