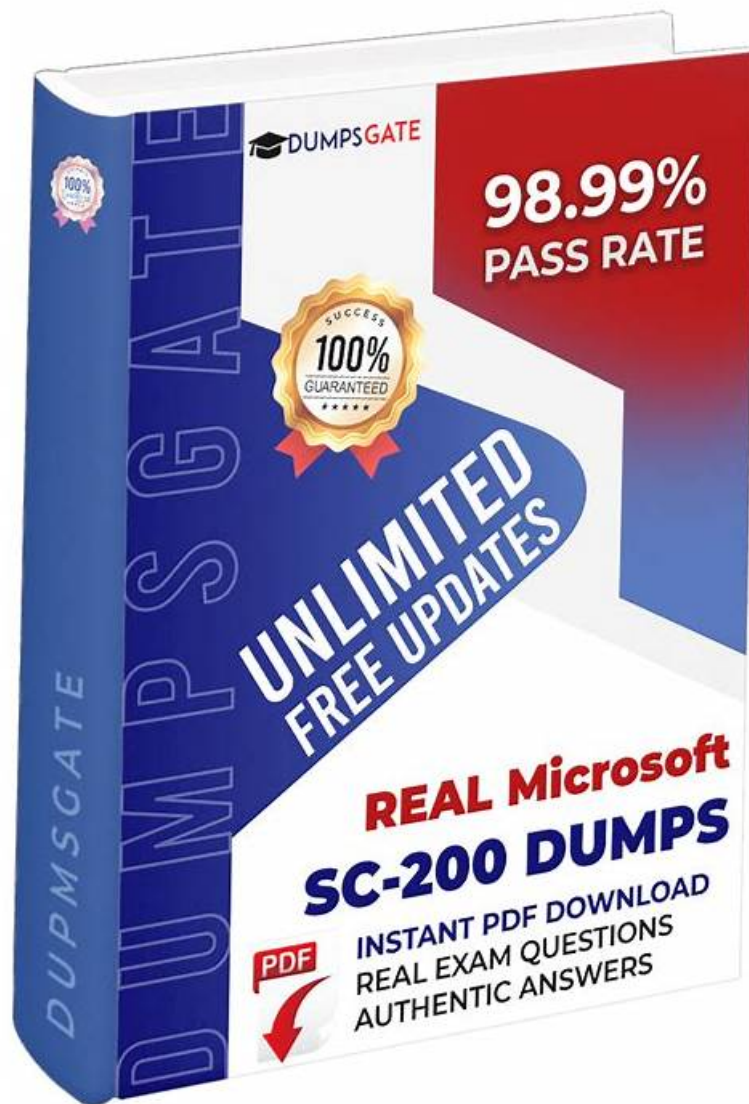


Get the Actual Microsoft SC-200 Dumps to Reduce Exam Anxiety



P.S. Free & New SC-200 dumps are available on Google Drive shared by DumpStillValid: <https://drive.google.com/open?id=13nFMdsjUr-q4IWogMDrRYcnAsLXJoZSy>

We hope that you can use your time as much as possible for learning on the SC-200 practice questions. So we have considered every detail of the SC-200 study guide to remove all unnecessary programs. If you try to download our SC-200 study materials, you will find that they are so efficient! And even you free download the demos on the website, you can feel the convenience and efficiency. It is simple and easy to study with our SC-200 learning braindumps.

Microsoft SC-200 (Microsoft Security Operations Analyst) Certification Exam is a highly respected certification that is designed to test the skills and knowledge required to analyze and respond to security threats and incidents in a Microsoft environment. SC-200 exam is intended for security analysts who work in a security operations center (SOC) and are responsible for monitoring and analyzing security incidents. SC-200 exam focuses on topics such as threat detection and response, incident investigation and analysis, and vulnerability management.

Microsoft SC-200 is an exam designed for security operations analysts who want to validate their skills and knowledge in identifying, investigating, and responding to security threats in a Microsoft environment. Microsoft Security Operations Analyst certification exam is a part of the Microsoft Certified: Security Operations Analyst Associate certification path and is intended for individuals who work with Microsoft security solutions on a regular basis.

SC-200 Vce Download | Test SC-200 Simulator Online

The passing rate of our SC-200 study materials is the issue the client mostly care about and we can promise to the client that the passing rate of our product is 99% and the hit rate is also high. Our SC-200 practice braindumps are selected strictly based on the Real SC-200 Exam and refer to the exam papers in the past years. Our expert team devotes a lot of efforts on them and guarantees that each answer and question is useful and valuable.

Microsoft Security Operations Analyst Sample Questions (Q185-Q190):

NEW QUESTION # 185

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You are investigating an attacker that is known to use the Microsoft Graph API as an attack vector. The attacker performs the tactics shown the following table.



Name	Tactic
Tactic1	Conditional Access policy reconnaissance
Tactic2	Mailbox reconnaissance
Tactic3	Invites guest users to the tenant

You need to search for malicious activities in your organization.

Which tactics can you analyze by using the MicrosoftGraphActivityLogs table?

- A. Tactic1 and Tactic2 only
- B. Tactic2 and Tactic3 only
- **C. Tactic1, Tactic2, and Tactic3**
- D. Tactic2 only

Answer: C

Explanation:

The MicrosoftGraphActivityLogs table in Microsoft Defender XDR (formerly part of Microsoft 365 Defender and Microsoft Sentinel) records API activity involving the Microsoft Graph API. This includes calls made to endpoints that interact with Azure AD, Exchange Online, SharePoint, Teams, and other Microsoft 365 services.

According to Microsoft's official documentation:

"The MicrosoftGraphActivityLogs table provides visibility into activities performed via Microsoft Graph API.

These include directory enumeration, mailbox data access, policy queries, and user management actions. The table helps detect misuse of Graph API for reconnaissance or lateral movement." Here's how it applies to the tactics listed:

* Tactic1 - Conditional Access policy reconnaissance: Attackers can use Graph API calls (e.g., GET /identity/conditionalAccess/policies) to enumerate Conditional Access policies. This activity is logged in MicrosoftGraphActivityLogs, showing which API endpoints were accessed, by whom, and when.

* Tactic2 - Mailbox reconnaissance: Using Graph API calls such as GET /users/{id}/messages, attackers can read or enumerate mailbox data. These API interactions are also captured within MicrosoftGraphActivityLogs, allowing analysts to correlate them to potential reconnaissance behavior.

* Tactic3 - Invites guest users to the tenant: Graph API requests like POST /invitations are used to invite external users (B2B collaboration). These events are also recorded in the same table, providing audit visibility into cross-tenant invitation attempts. Because all three tactics - Conditional Access reconnaissance, mailbox reconnaissance, and guest user invitations - involve the Microsoft Graph API, they are all detectable through the MicrosoftGraphActivityLogs table.

Therefore, the verified correct answer is:

D. Tactic1, Tactic2, and Tactic3

NEW QUESTION # 186

You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.


NOTE: Each correct selection is worth one point.

Microsoft Teams:

Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

	▼
Custom	
Office 365	
Security Events	
Syslog	



Answer:


Explanation:

Microsoft Teams:

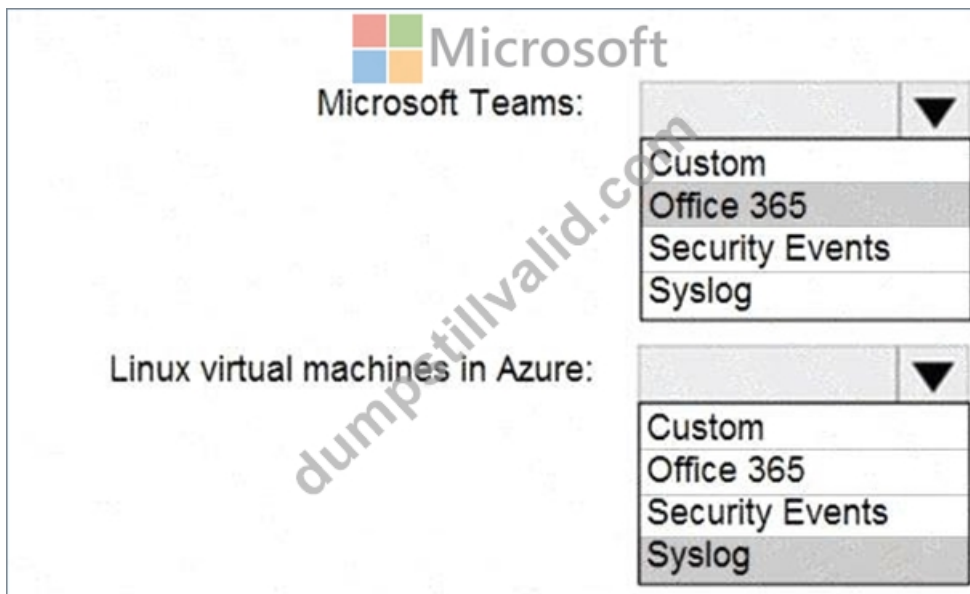
Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

	▼
Custom	
Office 365	
Security Events	
Syslog	



Explanation:



In Microsoft Sentinel (part of Microsoft Defender XDR), data connectors are used to integrate log sources for security analytics and monitoring.

For Microsoft Teams, the correct and most efficient connector is Office 365. Microsoft Teams logs- including user activities, chat events, and team management actions-are part of the Office 365 audit logs.

Microsoft Sentinel provides a built-in Office 365 connector that ingests auditing data from Exchange Online, SharePoint Online, and Microsoft Teams directly from the Microsoft 365 security and compliance center.

This connector requires only minimal configuration (enabling audit logging and connecting the tenant), satisfying the requirement to minimize administrative effort.

For Linux virtual machines hosted in Azure, the appropriate connector is Syslog. Linux systems send their security and operational events via Syslog, and Microsoft Sentinel supports this natively through the Syslog data connector. The Syslog agent (Log Analytics agent or AMA) collects logs and sends them to the Sentinel workspace. This connector is purpose-built for Linux VMs and ensures that authentication, authorization, and system logs are captured for correlation and threat detection.

Therefore:

* Microsoft Teams # Office 365 (because Teams audit data flows via Office 365 logs)

* Linux virtual machines in Azure # Syslog (because Linux uses Syslog for event forwarding) This configuration follows Microsoft's documented best practices for Sentinel data ingestion with minimal setup and maximum native integration.

NEW QUESTION # 187

You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in the Microsoft Entra tenant. The solution must use the principle of least privilege.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area

The screenshot shows two dropdown menus. The first, labeled 'Microsoft Entra role:', has a list with 'Security Administrator' highlighted. The second, labeled 'Azure role:', has a list with 'Microsoft Sentinel Contributor' highlighted. A callout box points to the 'Security Administrator' role with the text 'These are the selections for Azure's'.

Explanation:

The screenshot shows the 'Answer Area' with the 'Microsoft Entra role:' dropdown set to 'Security Administrator' and the 'Azure role:' dropdown set to 'Microsoft Sentinel Contributor'.

Enabling User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel requires specific permissions in both Microsoft Entra ID (Azure AD) and the Azure Sentinel workspace. The goal is to grant the least privilege necessary for the user (User1) to enable UEBA and manage entity behavior analytics.

Microsoft's documentation for UEBA setup specifies that to enable UEBA for an Entra tenant, the user must have access to identity-related signals and security settings within the Microsoft Entra environment.

Specifically:

"To enable UEBA and connect Microsoft Entra ID data, the user must be assigned the Security Administrator role in Microsoft Entra ID. This role allows management of security-related features without granting full directory or global admin privileges." The Security Administrator role provides just enough access to security configurations, alerts, and risk data, aligning with the principle of least privilege.

Other roles:

- * Global Administrator is overly privileged.
- * Security Operator can only view alerts, not configure settings.
- * Identity Governance Administrator focuses on access reviews and entitlement management, not UEBA setup.

Hence, the correct Entra role is Security Administrator.

For the Azure side, Microsoft's official Sentinel RBAC guidance states:

"To enable or configure UEBA in a Sentinel workspace, the user must have the Microsoft Sentinel Contributor role. This role allows enabling and configuring UEBA, managing analytics, and viewing data within Sentinel." The Sentinel Contributor role grants permissions to configure data connectors, UEBA settings, and entity analytics features but not workspace-wide administrative rights.

Other options:

- * Microsoft Sentinel Automation Contributor is limited to playbook and automation configurations.
- * Security Admin and Security Assessment Contributor roles apply to Microsoft Defender for Cloud and general Azure security posture, not UEBA configuration.

Final Correct Roles:

- * Microsoft Entra role: Security Administrator
- * Azure role: Microsoft Sentinel Contributor

NEW QUESTION # 188

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 Management, select Weaknesses, and search for the CVE.

Select Security recommendations.

Create the remediation request.

- 1 - From Threat & Vulnerability Management, select Weaknesses, and search for the CVE.
- 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 # 189

You need to create the analytics rule to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

Create the rule of type:

Fusion

Microsoft incident creation

Scheduled

Configure the playbook to include:

Diagnostics settings

A service principal

A trigger

Answer:

Explanation:

of type:

Microsoft incident type:

Scheduled

Diagnostics service

A service principal

P.S. Free & New SC-200 dumps are available on Google Drive shared by DumpStillValid: <https://drive.google.com/open?id=13nFMdsjUr-q4fWOgMDrRYcnAsLXJoZSsy>