Free Questions for MS-500 by dumpshq

Shared by Cooley on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

You have multiple Microsoft 365 subscriptions.

You need to build an application that will retrieve the Microsoft Secure Score data of each subscription.

What should you use?

Options:

A- the Microsoft Defender for Endpoint API

B- the Microsoft Graph Security API

C- the Microsoft Office 365 Management API

D- the Azure Monitor REST API

Answer:

C

Question 2

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription that has Microsoft 365 Defender enabled.

You plan to deploy a third-party app named App1 that will receive alert data from Microsoft 365 Defender.

Which format will Microsoft 365 Defender use to send the alert data to App1?

Options:

A- JSON

B- ZIP

C- XML

D- CSV

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts?view=o365-worldwide

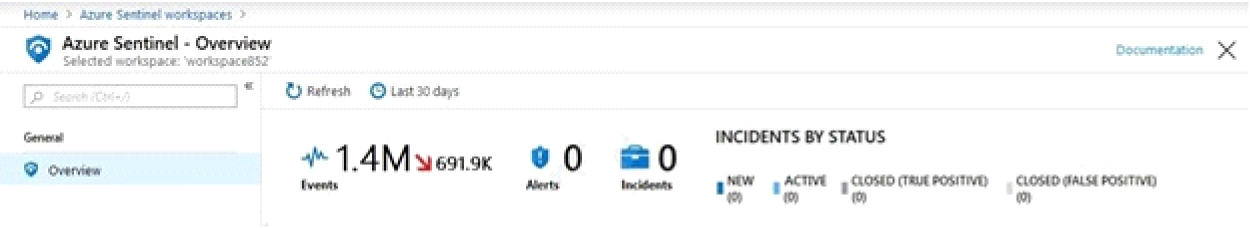
Question 3

Question Type: MultipleChoice

You create an Azure Sentinel workspace.

You configure Azure Sentinel to ingest data from Azure Active Directory (Azure AD).

In the Azure Active Directory admin center, you discover Azure AD Identity Protection alerts. The Azure Sentinel workspace shows the status as shown in the following exhibit.


Home > Azure Sentinel workspaces >
Azure Sentinel - Overview
Selected workspace: 'workspace852'
Documentation
Search (Ctrl+/)
General
Overview
Refresh
Last 30 days
1.4M
691.9K
Events
0
Alerts
0
Incidents
INCIDENTS BY STATUS
NEW (0)
ACTIVE (0)
CLOSED (TRUE POSITIVE) (0)
CLOSED (FALSE POSITIVE) (0)

In Azure Log Analytics, you can see Azure AD data in the Azure Sentinel workspace.

What should you configure in Azure Sentinel to ensure that incidents are created for detected threats?

Options:

A- data connectors

B- rules

C- workbooks

D- hunting queries

Answer:

B

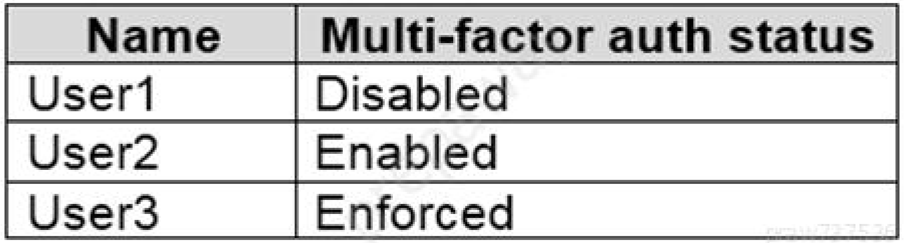
Explanation:

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

Question 4

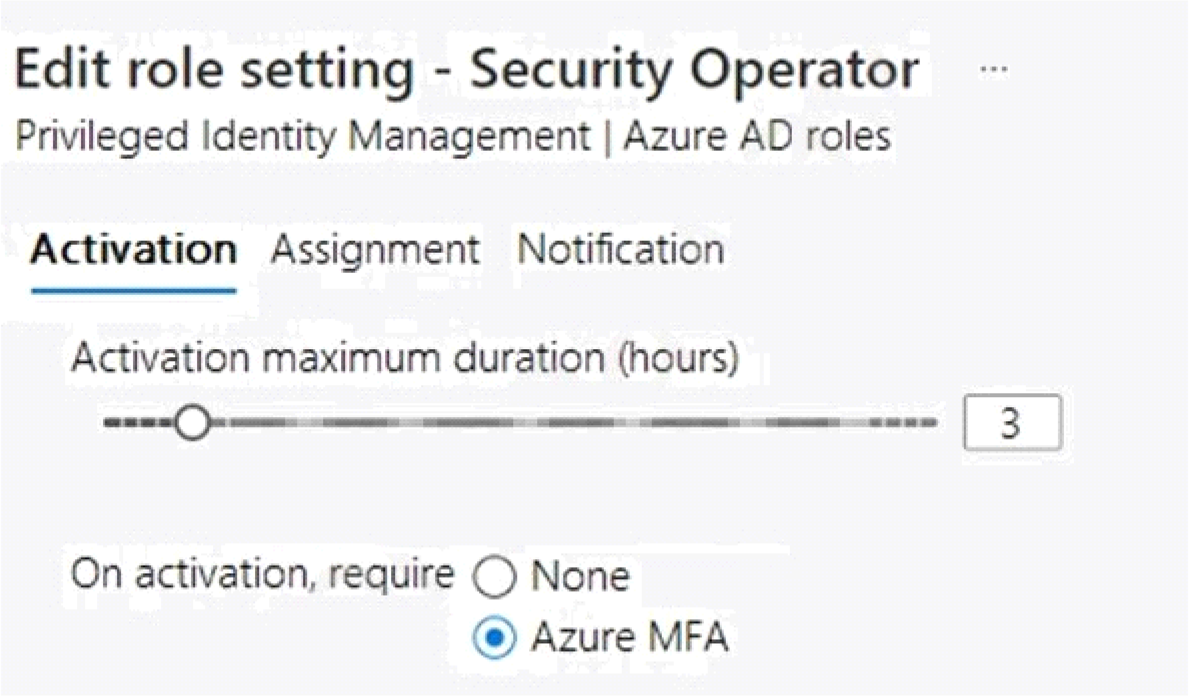
Question Type: **MultipleChoice**

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

You configure the Security Operator role in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.



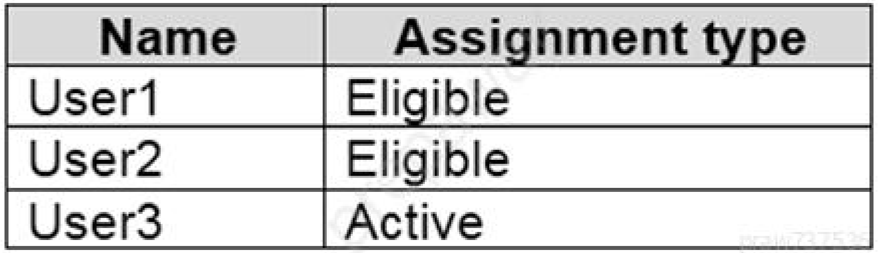
Edit role setting - Security Operator

Privileged Identity Management | Azure AD roles

Activation maximum duration (hours) 3

On activation, require ○ None ● Azure MFA

You add assignments to the Security Operator role as shown in the following table.



Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

Which users can activate the Security Operator role?

Options:

A- User2 only

B- User3 only

C- Used and User2 only

D- User2 and User3 only

E- User1,User2, and User3

Answer:

D

Question 5

Question Type: MultipleChoice

Your network contains an on-premises Active Directory domain named contoso.local that has a forest functional level of Windows Server 2008 R2.

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to install Azure AD Connect and enable single sign-on (SSO).

You need to prepare the domain to support SSO. The solution must minimize administrative effort.

What should you do?

Options:

A- Raise the forest functional level to Windows Server 2016.

B- Modify the UPN suffix of all domain users.

C- Populate the mail attribute of all domain users.

D- Rename the domain.

Answer:

B

Explanation:

https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide

Question 6

Question Type: **MultipleChoice**

You have a Microsoft 365 E5 subscription that uses Microsoft Teams and contains a user named User1.

You configure information barriers.

You need to identify which information barrier policies apply to User1.

Which cmdlet should you use?

Options:

A- Get-InformationBarrierRecipientStatus

B- Get-InformationBarrierPoliciesApplicationStatus

C- Get-InformationBarrierPolicy

D- Get-OrganizationSegment

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/office365/troubleshoot/information-barriers/information-barriers-troubleshooting

Question 7

Question Type: MultipleChoice

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.

From the workspace, you plan to create a scheduled query rule that will use a custom query. The rule will be used to generate alerts when inbound access to Office 365 from specific user accounts is detected.

You need to ensure that when multiple alerts are generated by the rule, the alerts are consolidated as a single incident per user account.

What should you do?

Options:

A- From Set rule logic, map the entities.

B- From Analytic rule details, configure Severity.

C- From Set rule logic, set Suppression to Off.

D- From Analytic rule details, configure Tactics.

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/sentinel/map-data-fields-to-entities

Question 8

Question Type: **MultipleChoice**

You have several Conditional Access policies that block noncompliant devices from connecting to services.

You need to identify which devices are blocked by which policies.

What should you use?

Options:

A- the Device compliance report in the Microsoft Endpoint Manager admin center

B- the Device compliance trends report in the Microsoft Endpoint Manager admin center

C- Activity log in the Cloud App Security admin center

D- the Conditional Access Insights and Reporting workbook in the Azure Active Directory admin center

Answer:

D

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

Question 9

Question Type: MultipleChoice

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.

You plan to deploy a hybrid Azure Active Directory (Azure AD) tenant that has Azure AD Identity Protection risk policies enabled.

You need to configure Azure AD Connect to support the planned deployment.

Which Azure AD Connect authentication method should you select?

Options:

A- Federation with AD FS

B- Federation with PingFederate

C- Password Hash Synchronization

D- Pass-through authentication

Answer:

C

Question 10

Question Type: **MultipleChoice**

You have a Microsoft 365 subscription.

You need to recommend a passwordless authentication solution that uses biometric authentication.

What should you include in the recommendation?

Options:

A- Windows Hello for Business

B- a smart card

C- the Microsoft Authenticator app

D- a PIN

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Question 11

Question Type: **MultipleChoice**

You have a Microsoft 365 tenant that is linked to a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

You need to enable Azure AD Seamless Single Sign-On (Azure AD SSO) for contoso.com.

What should you use?

Options:

A- Azure AD Connect

B- the Azure Active Directory admin center

C- the Microsoft 365 Security admin center

D- the Microsoft 365 admin center

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start