SC-900 Q&As

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/sc-900.html

100% Passing Guarantee
100% Money Back Assurance

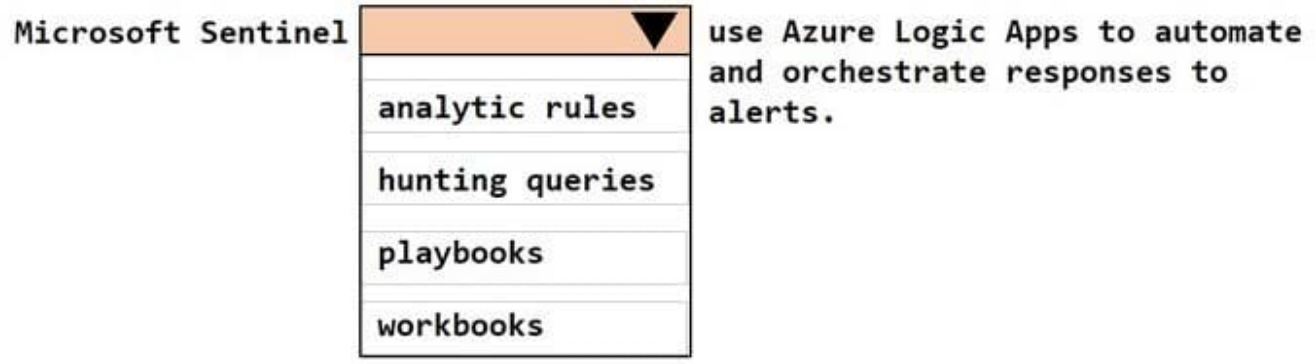
Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

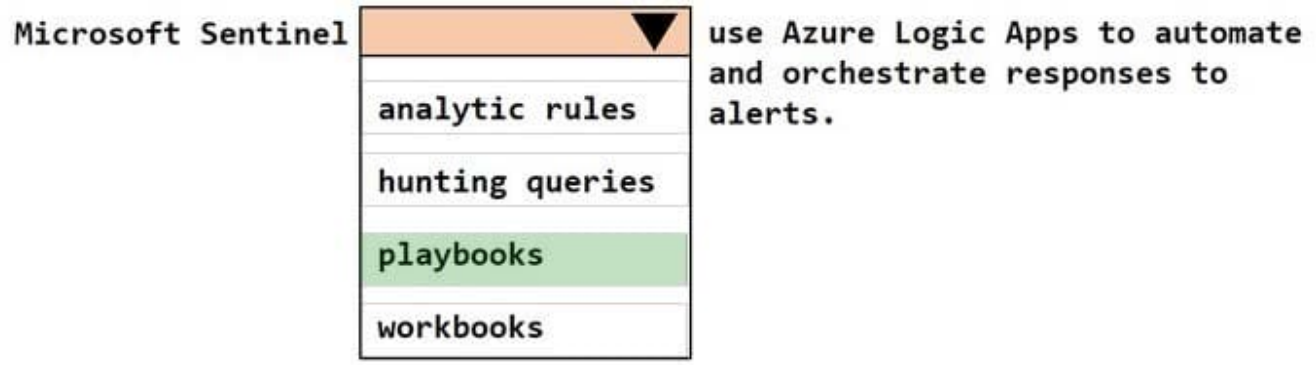
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Correct Answer:



https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 2

Which feature provides the extended detection and response (XDR) capability of Azure Sentinel?

A. integration with the Microsoft 365 compliance center

B. support for threat hunting

C. integration with Microsoft 365 Defender

D. support for Azure Monitor Workbooks

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide

QUESTION 3

Which three statements accurately describe the guiding principles of Zero Trust? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Define the perimeter by physical locations.

B. Use identity as the primary security boundary.

C. Always verify the permissions of a user explicitly.

D. Always assume that the user system can be breached.

E. Use the network as the primary security boundary.

Correct Answer: BCD

Reference: https://docs.microsoft.com/en-us/security/zero-trust/

QUESTION 4

Which three authentication methods can Azure AD users use to reset their password? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. mobile app notification

B. text message to a phone

C. security questions

D. certificate

E. picture password

Correct Answer: ABC

Azure Active Directory (Azure AD) self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user\\'s account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work. This ability reduces help desk calls and loss of productivity when a user can\\'t sign in to their device or an application.

Authentication methods When a user is enabled for SSPR, they must register at least one authentication method. We highly recommend that you choose two or more authentication methods so that your users have more flexibility in case they\\'re unable to access one method when they need it. For more information, see What are authentication methods?.

The following authentication methods are available for SSPR:

Mobile app notification Mobile app code Email Mobile phone Office phone (available only for tenants with paid subscriptions) Security questions Users can only reset their password if they have registered an authentication method

that the administrator has enabled.

Note: Select authentication methods and registration options When users need to unlock their account or reset their password, they\\'re prompted for another confirmation method. This extra authentication factor makes sure that Azure AD finished only approved SSPR events. You can choose which authentication methods to allow, based on the registration information the user provides.

1.

From the menu on the left side of the Authentication methods page, set the Number of methods required to reset to 2.

To improve security, you can increase the number of authentication methods required for SSPR.

2.

Choose the Methods available to users that your organization wants to allow. For this tutorial, check the boxes to enable the following methods:

Mobile app notification Mobile app code Email Mobile phone You can enable other authentication methods, like Office phone or Security questions, as needed to fit your business requirements.

3.

To apply the authentication methods, select Save.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

QUESTION 5

What can you use to provide a user with a two-hour window to complete an administrative task in Azure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

B. Azure Multi-Factor Authentication (MFA)

C. Azure Active Directory (Azure AD) Identity Protection

D. conditional access policies

Correct Answer: A

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management: Provide just-in-time privileged access to Azure AD and Azure resources Assign time-bound access to resources using start and end dates Require approval to activate privileged roles Enforce multi-factor authentication to activate any role Use justification to understand why users activate Get notifications when privileged roles are activated Conduct access reviews to ensure users still need roles Download audit history for internal or external audit Prevents removal of the last active Global Administrator role assignment.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure