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.leads4pass.com/sc-900.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What do you use to provide real-time integration between Azure Sentinel and another security source?

A. Azure AD Connect

B. a Log Analytics workspace

C. Azure Information Protection

D. a connector

Correct Answer: D

To on-board Azure Sentinel, you first need to connect to your security sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, including Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity, and Microsoft Cloud App Security, etc.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/overview

---

QUESTION 2

Which three forms of verification can be used with Azure AD Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution.

NOTE: Each correct answer is worth one point.

A. security questions

B. the Microsoft Authenticator app

C. SMS messages

D. a smart card

E. Windows Hello for Business

Correct Answer: BCE

Available verification methods

When users sign in to an application or service and receive an MFA prompt, they can choose from one of their registered forms of additional verification. Users can access My Profile to edit or add verification methods.

The following additional forms of verification can be used with Azure AD Multi-Factor Authentication:

*

Microsoft Authenticator Authenticator Lite (in Outlook)

*

Windows Hello for Business FIDO2 security key OATH hardware token (preview) OATH software token

*

SMS Voice call

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

QUESTION 3

Which pillar of identity relates to tracking the resources accessed by a user?

A. authorization

B. auditing

C. administration

D. authentication

Correct Answer: B

Audit logs in Azure Active Directory

As an IT administrator, you want to know how your IT environment is doing. The information about your system\\'s health enables you to assess whether and how you need to respond to potential issues.

To support you with this goal, the Azure Active Directory portal gives you access to three activity logs:

Sign-ins

QUESTION 4

DRAG DROP

You are evaluating the compliance score in Compliance Manager.

Match the compliance score action subcategories to the appropriate actions.

To answer, drag the appropriate action subcategory from the column on the left to its action on the right. Each action subcategory may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:

Action Subcategories

Corrective

Detective

Preventative

Answer Area

Action subcategory Encrypt data at rest.

Action subcategory Perform a system access audit.

Action subcategory Make configuration changes in response to a security incident.

Correct Answer:

Action Subcategories

Answer Area

Preventative Encrypt data at rest.

Detective Perform a system access audit.

Corrective Make configuration changes in response to a security incident.

Box 1: Preventative

Preventative actions address specific risks. For example, protecting information at rest using encryption is a preventative action against attacks and breaches. Separation of duties is a preventative action to manage conflict of interest and

guard against fraud.

Box 2: Detective

Detective actions actively monitor systems to identify irregular conditions or behaviors that represent risk, or that can be used to detect intrusions or breaches. Examples include system access auditing and privileged administrative actions.

Regulatory compliance audits are a type of detective action used to find process issues.

Box 3: Corrective

Corrective actions try to keep the adverse effects of a security incident to a minimum, take corrective action to reduce the immediate effect, and reverse the damage if possible. Privacy incident response is a corrective action to limit damage

and restore systems to an operational state after a breach.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation

---

QUESTION 5

Which score measures an organization\\'s progress in completing actions that help reduce risks associated to data protection and regulatory standards?

A. Microsoft Secure Score

B. Productivity Score

C. Secure score in Azure Security Center

D. Compliance score

Correct Answer: D

The Compliance Manager dashboard displays your overall compliance score. This score measures your progress in completing recommended improvement actions within controls. Your score can help you understand your current compliance posture. It can also help you prioritize actions based on their potential to reduce risk.

A score value is assigned at these levels:

*

Improvement action: Each action has a different impact on your score depending on the potential risk involved. See Action types and points below for details.

*

Assessment: This score is calculated using improvement action scores. Each Microsoft action and each improvement action managed by your organization is counted once, regardless of how often it\\'s referenced in a control.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide