SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

https://www.passapply.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:

1.

Computers that run either Windows 10 or Windows 11

2.

Tablets and phones that run either Android or iOS

You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored.

What should you include in the recommendation?

A. eDiscovery

B. Microsoft Information Protection

C. Compliance Manager

D. retention policies

Correct Answer: B

Protect your sensitive data with Microsoft Purview.

Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.

Note: You can use Microsoft Information Protection: Microsoft Purview for Auditing and Analytics in Outlook for iOS, Android, and Mac (DoD).

Incorrect:

Not A: Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft Purview to search for content in Exchange

Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use Microsoft

Purview eDiscovery (Standard) cases to identify, hold, and export content found in mailboxes and sites. If your organization has an Office 365 E5 or Microsoft 365 E5 subscription (or related E5 add-on subscriptions), you can further manage

custodians and analyze content by using the feature-rich Microsoft Purview eDiscovery (Premium) solution in Microsoft 365.

Not C: What does compliance Manager do?

Compliance managers ensure that a business, its employees and its projects comply with all relevant regulations and

specifications. This could include health and safety, environmental, legal or quality standards, as well as any ethical policies

the company may have.

Not D: A retention policy (also called a \\'schedule\\') is a key part of the lifecycle of a record. It describes how long a business needs to keep a piece of information (record), where it\\'s stored and how to dispose of the record when its time.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection

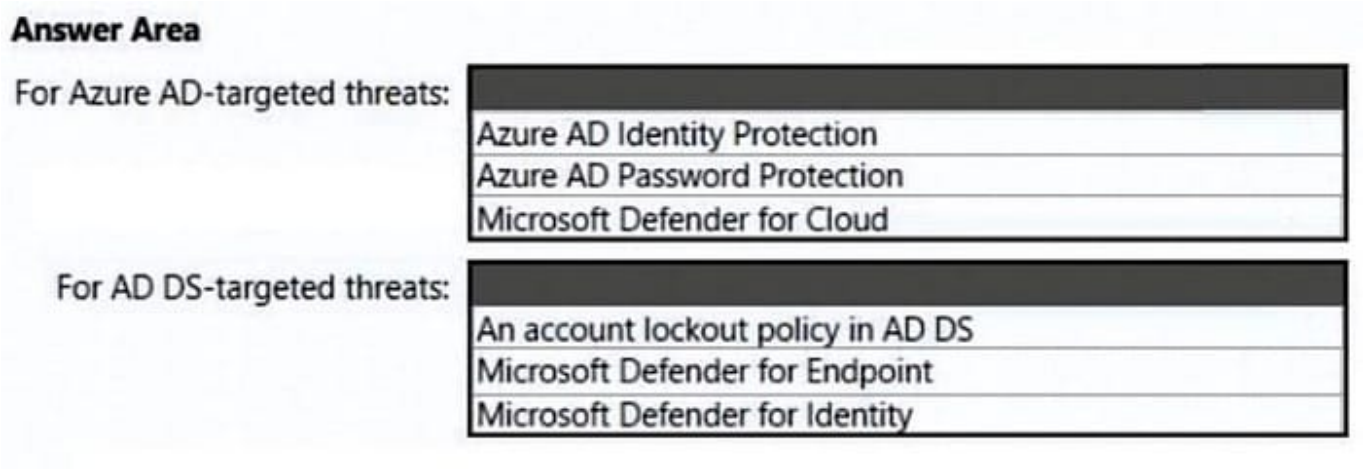
https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

QUESTION 2

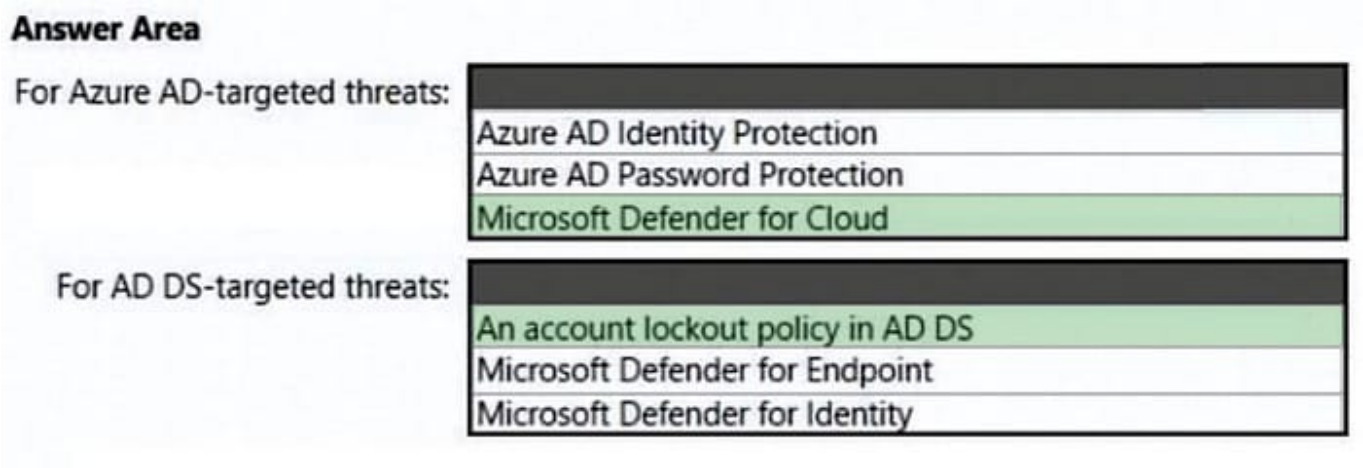
You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE; Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Microsoft defender for cloud

Scenario: Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

When Microsoft Defender for Cloud detects a Brute-force attack, it triggers an alert to bring you awareness that a brute force attack took place. The automation uses this alert as a trigger to block the traffic of the IP by creating a security rule in

the NSG attached to the VM to deny inbound traffic from the IP addresses attached to the alert. In the alerts of this type, you can find the attacking IP address appearing in the \\'entities\\' field of the alert.

Box 2: An account lockout policy in AD DS

Scenario:

Detect brute force attacks that directly target AD DS user accounts.

Smart lockout helps lock out bad actors that try to guess your users\\' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other

unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

Verify on-premises account lockout policy

To verify your on-premises AD DS account lockout policy, complete the following steps from a domain-joined system with administrator privileges:

1.

Open the Group Policy Management tool.

2.

Edit the group policy that includes your organization\\'s account lockout policy, such as, the Default Domain Policy.

3.

Browse to Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy.

4.

Verify your Account lockout threshold and Reset account lockout counter after values.

Reference: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/automation-to-block-brute-force-attacked-ip-detected-by/ba-p/1616825 https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#verify-on-premises-account-lockout-policy

---

QUESTION 3

You have a Microsoft 365 E5 subscription and an Azure subscription.

You are designing a Microsoft deployment.

You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events.

What should you recommend using in Microsoft Sentinel?

A. playbooks

B. workbooks

C. notebooks

D. threat intelligence

Correct Answer: B

After you connected your data sources to Microsoft Sentinel, you get instant visualization and analysis of data so that you can know what\\'s happening across all your connected data sources. Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.

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

---

QUESTION 4

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.

You plan to remove all the domain accounts from the Administrators groups on the Windows computers.

You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator

account on a computer is compromised.

What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. Privileged Access Workstations (PAWs)

Correct Answer: A

Microsoft\\'s "Local Administrator Password Solution" (LAPS) provides management of local administrator account passwords for domain-joined computers. Passwords are randomized and stored in Active Directory (AD), protected by ACLs, so only eligible users can read it or request its reset.

Microsoft LAPS is short for Microsoft Local Administrator Password Solution. When installed and enabled on domain-joined computers it takes over the management of passwords of local accounts. Passwords are automatically changed to random characters that meet the domain\\'s password policy requirements at a frequency that you define through Group Policy.

The passwords are stored in a protected “confidential” attribute on the Computer object in AD. Unlike most other attributes which can be read by all domain users by default, the confidential attributes require extra privileges to be granted in order to read them, thus securing the managed passwords.

Incorrect: Not B: Integrate on-premises Active Directory domains with Azure Active Directory Validate security configuration and policy, Actively monitor Azure AD for signs of suspicious activity

Consider using Azure AD Premium P2 edition, which includes Azure AD Identity Protection. Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised. For example, it can detect potentially unusual activity such as irregular sign-in activities, sign-ins from unknown sources or from IP addresses with suspicious activity, or sign-ins from devices that may be infected. Identity Protection uses this data to generate reports and alerts that enable you to investigate these risk events and take appropriate action.

Not C: Azure AD PIM is a service in Azure AD that enables you to manage, control, and monitor access to resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Not D: Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides very strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket.

Reference: https://craighays.com/microsoft-laps/ https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad

QUESTION 5

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an

administrator

authorizes the application.

Which security control should you recommend?

A. adaptive application controls in Defender for Cloud

B. app protection policies in Microsoft Endpoint Manager

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure Security Benchmark compliance controls in Defender for Cloud

Correct Answer: A

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software.

Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.

When you\\'ve enabled and configured adaptive application controls, you\\'ll get security alerts if any application runs other than the ones you\\'ve defined as safe.

Incorrect:

Not B: App protection policies (APP) are rules that ensure an organization\\'s data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of

actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Not C: Cloud Discovery anomaly detection policy reference. A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded

data, uploaded data, transactions, and users are considered for each cloud application.

Not D: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy

https://docs.microsoft.com/en-us/security/benchmark/azure/overview