



- Expert Verified, Online, **Free**.

Custom View Settings

Topic 1 - Single Topic**Question #1****Topic 1****HOTSPOT -**

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	<input type="radio"/>	<input checked="" type="radio"/>
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	<input type="radio"/>	<input checked="" type="radio"/>

✉ **kset** Highly Voted 2 years, 1 month ago

1) No - <https://azure.microsoft.com/en-us/pricing/details/active-directory/>: Azure Active Directory comes in four editions—Free, Office 365 apps, Premium P1, and Premium P2.
 2) Yes - <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant> You can do all of your administrative tasks using the Azure Active Directory (Azure AD) portal, including creating a new tenant for your organization.
 3) No - <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis> Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service

upvoted 43 times

✉ **AKYK** Highly Voted 2 years, 7 months ago

Correct Answers.

upvoted 14 times

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证
微信添加 hello231119

✉ **lecoh** Most Recent 5 days, 16 hours ago

Planning for SC-900 wanted to set out on a journey into the profundities of Microsoft security and consistence.<https://shorturl.at/wGKO6>
 upvoted 5 times

✉ **kodol75469** 3 weeks ago

Passed with these today, they are valid. Keep studying and believe in yourself
<https://www.pinterest.com/pin/1110770695589426167>

upvoted 1 times

✉ **JCChien** 1 month, 1 week ago

Correct Answers.

upvoted 1 times

✉ **AGA81** 1 month, 2 weeks ago

Passed Exam with 954 marks. Thank you team. Took exam on 24/01/2024

upvoted 1 times

✉ **incywincy** 3 months, 3 weeks ago

I think that the right answers are NNN.

The second question asks if you can access and manage Azure AD through Azure Portal and not through Azure Admin Center. Azure Portal is used to manage Azure Resource and not Azure AD resources. Any comment on that?

upvoted 2 times

✉ **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 2 times

justlooking_movealong 10 months, 2 weeks ago

adding here so people can see, just passed with 910/1000. some new questions around pruvew (~4) as exam content was updated on the 05/05/2023, i would say 80% of the questions were from this site. good luck.

upvoted 5 times

DanPicardi 8 months, 2 weeks ago

congrats!

upvoted 1 times

zellck 11 months ago

NYN is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis#what-are-the-azure-ad-licenses>

To enhance your Azure AD implementation, you can also add paid features by upgrading to Azure Active Directory Premium P1 or Premium P2 licenses. Azure AD paid licenses are built on top of your existing free directory. The licenses provide self-service, enhanced monitoring, security reporting, and secure access for your mobile users.

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. Azure AD enables your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure Active Directory also helps them access internal resources like apps on your corporate intranet, and any cloud apps developed for your own organization.

upvoted 2 times

Jm_123 11 months, 1 week ago

last week I cleared my SC-900 exam with 976 marks thanks to Examtopics

upvoted 1 times

tdasuni001 11 months, 3 weeks ago

NO , Yes, No

upvoted 2 times

Wandz 1 year ago

1)No

2)Yes

3)No

upvoted 2 times

Pady1234 1 year ago

N, Y, N

upvoted 2 times

MeisAdriano 1 year ago

Correct

upvoted 2 times

Ken28132 1 year, 1 month ago

No

Yes

No

upvoted 3 times

FBrabble 1 year, 4 months ago

Just some feedback post exam - I passed! Exam Topics is a great resource to use when studying. Yes it helps to know and understand the material as well, no doubt. But the social nature of Exam Topics was a great way to better explore each subject and I did see similar questions on the exam. Many exam study practice test products are out there - this one is pretty darn great! Yes, some answers as given are incorrect, and that is where the community steps in to correct the Q & A. I would recommend Exam Topics.

upvoted 4 times

Question #2

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证
微信添加 hello231119**Answer Area**

Azure Blueprints
Azure Policy
The Microsoft Cloud Adoption Framework for Azure
A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

Correct Answer:**Answer Area**

Azure Blueprints
Azure Policy
The Microsoft Cloud Adoption Framework for Azure
A resource lock

provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/>**AKYK** Highly Voted 2 years, 7 months ago

Correct

upvoted 22 times

kset Highly Voted 2 years, 1 month ago<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/>

"The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey."

upvoted 17 times

user_666 Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 2 times

RahulX 7 months, 2 weeks ago

The Cloud Adoption Framework is correct ans.

upvoted 1 times

Mehe323 8 months, 1 week ago

Tip: without much knowledge, some questions can be answered by common sense (and a bit of luck). Go over the names of the other features and think about how they relate to the question. Even if you don't know exactly what CAF is, the other answers don't seem to be really relevant to the question.

upvoted 3 times

tdasuni001 11 months, 3 weeks ago

The Cloud Adoption Framework brings together cloud adoption best practices from Microsoft employees, partners, and customers. The framework provides tools, guidance, and narratives.

upvoted 1 times

Ken28132 1 year, 1 month ago

CAF is the right answer

upvoted 2 times

Mcelona 1 year, 3 months ago

Correct

upvoted 1 times

Justin0020 1 year, 11 months ago

Had this question on exam. Right answer.

upvoted 5 times

Tommo 1 year, 11 months ago

Correct answer

upvoted 2 times

BlackdaRipper 2 years ago

Correct answer

upvoted 1 times

AZ_Student 2 years, 1 month ago

CAF is the right one.

upvoted 1 times

TJ001 2 years, 2 months ago

CAF is the right answer (as given)

upvoted 1 times

Chris_Chen 2 years, 2 months ago

Correct.

upvoted 2 times

mcsank 2 years, 3 months ago

correct

upvoted 1 times

Melwin86 2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/>

upvoted 5 times

Question #3

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Customer Lockbox
Data loss prevention (DLP)
eDiscovery
A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Correct Answer:**Answer Area**

Customer Lockbox
Data loss prevention (DLP)
eDiscovery
A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview>

 **Rada89** Highly Voted 2 years, 9 months ago

I feel like the correct answer is eDiscovery

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide>
upvoted 170 times

 **Hot_156** 2 years, 1 month ago

Customer Lockbox is used by MS engineers when they need to have access to your data. They use this for requesting permissions to access the data and there is an approval process for it.

upvoted 18 times

 **PrajnaRao** Highly Voted 2 years, 8 months ago

Answer is eDiscovery

upvoted 54 times

 **Levock1** Most Recent 6 days, 18 hours ago

eDiscovery is the correct option

upvoted 1 times

 **excelchips11** 1 week ago

eDiscovery is the answer

upvoted 1 times

 **MoiLearning** 1 month ago

the answer is ediscovery

upvoted 1 times

 **tc_praveen** 3 months ago

eDiscovery

upvoted 1 times

 **frych** 3 months, 2 weeks ago

why not eDiscovery ?

upvoted 1 times

 **MGJG** 5 months ago

IA:eDiscovery refers to the process of discovering, collecting, and producing electronic information (such as emails, documents, databases, and other digital files) for legal purposes, particularly in the context of litigation or investigations. It involves identifying and preserving relevant electronic records in a manner that ensures their authenticity and integrity.

upvoted 2 times

MGJG 5 months ago

The other options you mentioned—customer lockbox, data loss prevention, and resource lock—do not specifically pertain to the process of identifying, holding, and exporting electronic information for investigative purposes. They have different purposes:

Customer Lockbox: This is a feature in cloud services that allows customers to have explicit control over when and how a cloud service provider can access their data. It's primarily a security and privacy feature.

Data Loss Prevention (DLP): DLP refers to a set of tools and processes used to prevent sensitive information from being accessed, shared, or distributed in an unauthorized manner.

Resource Lock: This is a term that might refer to a feature in cloud computing environments that allows users to prevent resources (such as virtual machines or storage) from being modified or deleted. It's a form of access control.

upvoted 2 times

MayTheForceBeWithYou 5 months, 3 weeks ago

eDiscovery

upvoted 1 times

stewbiee 6 months ago

The correct answer is eDiscovery

upvoted 1 times

lukecage5 6 months, 1 week ago

The correct answer is eDiscovery.

To use Microsoft Purview eDiscovery to identify, hold, and export electronic information, users can follow these steps:

Create an eDiscovery case.

Place eDiscovery holds on the relevant content locations.

Search for the relevant content.

Export the relevant content for further review.

Microsoft Purview eDiscovery is a powerful tool that can help organizations to comply with legal and regulatory requirements, and to manage their data risks. It is also a valuable tool for organizations that are conducting investigations.

upvoted 1 times

BantyLee 7 months, 2 weeks ago

The correct answer is eDiscovery

upvoted 2 times

RahulX 7 months, 2 weeks ago

The correct answer is eDiscovery.

upvoted 2 times

Darkfire 8 months ago

Answer should be eDiscovery

<https://learn.microsoft.com/en-us/purview/ediscovery?view=o365-worldwide>

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.

<https://learn.microsoft.com/en-us/purview/customer-lockbox-requests>

However, some cases require a Microsoft engineer to access your content to determine the root cause and fix the issue. Customer Lockbox requires the engineer to request access from you as a final step in the approval workflow.

upvoted 2 times

Kopter 9 months ago

I feel the correct answer is eDiscovery

See copied from Microsoft "eDiscovery (Premium). The eDiscovery (Premium) tool builds on the existing case management, preservation, search, and export capabilities in eDiscovery (Standard). eDiscovery (Premium) provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations."

upvoted 1 times

jaaake 9 months ago

eDiscovery is the right answer; the data quarantined in the Customer Lockbox is used by Microsoft Engineers for their (support-related) investigation

upvoted 1 times

Molota 10 months ago

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 eDiscovery cases to identify, hold, and export content found in mailboxes and sites.

<https://learn.microsoft.com/en-ca/training/modules/describe-ediscovery-capabilities-of-microsoft-365/2-describe-ediscovery-solutions>

upvoted 1 times

Question #4

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can manage Microsoft Intune by using the

Azure Active Directory admin center.
Microsoft 365 compliance center.
Microsoft 365 Defender portal.
Microsoft Endpoint Manager admin center.

Correct Answer:**Answer Area**

You can manage Microsoft Intune by using the

Azure Active Directory admin center.
Microsoft 365 compliance center.
Microsoft 365 Defender portal.
Microsoft Endpoint Manager admin center.

 **gustavomelquiades** Highly Voted 1 year, 9 months ago

The answer is: Microsoft Endpoint Manager

"Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk."

Source - <https://docs.microsoft.com/en-us/mem/endpoint-manager-overview>

upvoted 17 times

 **sensa** Highly Voted 1 year, 11 months ago

appeared on my exam today

upvoted 6 times

 **user_666** Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 4 times

 **XtraWest** 11 months, 2 weeks ago

Microsoft Endpoint Manager Admin Center [Correct]

upvoted 2 times

 **hululolo** 1 year ago

Appeared in exam on 3rd March

upvoted 2 times

 **cleristonm** 1 year, 1 month ago

Why do we have this question, if the learning path for SC-900, does not talk about Microsoft Endpoint Manager and Intune ?

upvoted 3 times

 **_Toluwalase11** 1 year, 2 months ago

This question came out in my exam today. 24th of Jan2023. This sight is really helpful. I appreciate the administrators

upvoted 2 times

 **Asabs** 1 year, 2 months ago

The Microsoft Endpoint Manager admin center is where you can find the Microsoft Intune service, as well as other device management related settings. Understanding the features available in Intune will help you accomplish various Mobile Device Management (MDM) and Mobile Application Management (MAM) tasks.

upvoted 2 times

 **Lizzylizzy** 1 year, 3 months ago

Microsoft intune is part of Microsoft endpoint manager

upvoted 1 times

 **OrangeSG** 1 year, 3 months ago

Answer: Microsoft Endpoint Manager admin center

Microsoft Intune, which is a part of Microsoft Endpoint Manager, provides the cloud infrastructure, the cloud-based mobile device management (MDM), cloud-based mobile application management (MAM), and cloud-based PC management for your organization.

Tutorial: Walkthrough Intune in Microsoft Endpoint Manager

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager>

upvoted 2 times

✉ **Shubham_8084** 1 year, 4 months ago

Answer: Microsoft Endpoint Manager.

"Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints."

upvoted 3 times

✉ **Lone_Wolf** 1 year, 5 months ago

Correct Answer!

upvoted 1 times

✉ **jimmysplash** 1 year, 9 months ago

keyword-endpoint

upvoted 2 times

✉ **egriaguo** 1 year, 9 months ago

Microsoft Endpoint Manager admin center

upvoted 2 times

✉ **jdemeter** 1 year, 10 months ago

Correct answer: Microsoft Endpoint Manager admin center

<https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-management>

upvoted 3 times

✉ **jdemeter** 1 year, 10 months ago

<https://docs.microsoft.com/en-us/learn/modules/set-up-microsoft-intune/>

upvoted 1 times

✉ **edvaldonardi** 1 year, 11 months ago

KK KK KK KK

upvoted 1 times

Question #5

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Federation is used to establish

between organizations.

- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Answer Area

Federation is used to establish

between organizations.

Correct Answer:

- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Federation is a collection of domains that have established trust.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>  **Melwin86** Highly Voted 2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

upvoted 22 times

  **RahulX** Most Recent 7 months, 2 weeks ago

Trust Relationship is correct ans.

upvoted 1 times

  **Darkfire** 8 months ago

Correct

upvoted 1 times

  **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

  **studytonight** 10 months ago

This was on the exam a week ago

upvoted 1 times

  **kxa57482** 1 year ago

Correct

upvoted 3 times

  **MS10** 1 year, 2 months ago

Trust Relationship

upvoted 3 times

  **orionduo** 1 year, 2 months ago

correct

"Federation enables the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain's identity provider."

<https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/6-describe-concept-federation>

upvoted 2 times

  **Lizzylizzy** 1 year, 3 months ago

Answer is trust relationship

upvoted 1 times

  **eli2022** 1 year, 4 months ago

On exam 11/02/2022

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

 **gustavomelquiades** 1 year, 9 months ago

Answer is - federation

"Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources."

Source - <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

upvoted 4 times

 **PaulB_NZ** 1 year, 5 months ago

Federation is the question..the answer is trust between orgs

upvoted 2 times

 **egriaguo** 1 year, 9 months ago

Correct answer

upvoted 1 times

 **sensa** 1 year, 11 months ago

appeared on my exam today

upvoted 2 times

 **Tommo** 1 year, 11 months ago

Correct answer

upvoted 1 times

 **BlackdaRipper** 2 years ago

Correct answer

upvoted 1 times

 **TJ001** 2 years, 2 months ago

right answer

upvoted 3 times

Question #6

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Microsoft Defender for Cloud	<input type="radio"/>	<input type="radio"/>
The secure score in Microsoft Defender for Cloud can evaluate resources across multiple Azure subscriptions	<input type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Microsoft Defender for Cloud	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
Applying system updates increases an organization's secure score in Microsoft Defender for Cloud	<input checked="" type="radio"/>	<input type="radio"/>
The secure score in Microsoft Defender for Cloud can evaluate resources across multiple Azure subscriptions	<input checked="" type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Microsoft Defender for Cloud	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes -

Box 3: Yes -

If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls>

 **Rayo80** Highly Voted  1 year, 6 months ago

Correct

upvoted 8 times

 **Tahamaffia** Most Recent  6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 1 times

 **Mage10** 5 months ago

which answer did you select

upvoted 1 times

 **RahulX** 7 months, 2 weeks ago

Box 1: Yes -

Box 2: Yes -

Box 3: Yes -

upvoted 1 times

 **kxa57482** 1 year ago

yes yes yes

upvoted 3 times

 **Cololand** 1 year, 1 month ago

3 times YES

upvoted 2 times

 **ErosTargaryen** 1 year, 3 months ago

It's on my exam today 12/27/2022
upvoted 2 times

✉ **Mouratov** 1 year, 4 months ago

Updates score or not?

upvoted 1 times

✉ **xeni66** 1 year, 4 months ago

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>

upvoted 1 times

✉ **somenick** 1 year, 5 months ago

It is NYY now.

Apply system updates - Not scored

upvoted 3 times

✉ **Whyest** 1 year, 2 months ago

somenick is wrong

upvoted 1 times

✉ **AlbertKwan** 1 year, 4 months ago

You are wrong.

Apply system updates - is surely scored.

upvoted 2 times

✉ **Lanka22** 1 year, 4 months ago

6 Apply system updates - Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks. Use these recommendations to maintain operational efficiency, reduce security vulnerabilities, and provide a more stable environment for your end users. To deploy system updates, you can use the Update Management solution to manage patches and updates for your machines.

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>

upvoted 5 times

✉ **Segowax** 9 months ago

I guess maybe it is not scoring because question is about Microsoft Defender for Cloud not about Microsoft 365 Defender, please see (Differences between secure score in Microsoft 365 Defender and Microsoft Defender for Cloud):

<https://learn.microsoft.com/en-us/training/modules/describe-threat-protection-with-microsoft-365-defender/7-describe-microsoft-defender-portal>

upvoted 1 times

✉ **Lone_Wolf** 1 year, 5 months ago

Correct Answer!

upvoted 4 times

✉ **LukeFever** 1 year, 5 months ago

Correct

upvoted 4 times

Question #7

Topic 1

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

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>

Community vote distributionD (100%)

✉  **eddie_network_jedi**  2 years, 5 months ago

Correct. "regulatory" is the keyword here.
regulatory:compliance

upvoted 44 times

✉  **KoosDuppen** 1 year, 11 months ago

to be honest, I barely paid attention to this specific word. Looking here why the answer is 'D'.... I'm surprised that I was surprised by the specific word. Good looking out and great advice for us all (will not forget, thank you)

upvoted 11 times

✉  **qdam**  2 years, 2 months ago

Selected Answer: D

D is correct

upvoted 21 times

✉  **RahulX**  7 months, 2 weeks ago

Compliance score

upvoted 2 times

✉  **Juliamaira** 9 months ago

This question came today's exam.

upvoted 1 times

✉  **zellck** 11 months ago

Got this in Apr 2023 exam.

upvoted 5 times

✉  **Kelsi999** 11 months ago

D is the correct answer.
I had this question on the exam today

upvoted 2 times

✉  **lalalakis** 1 year ago

Am I the only one who has serious trouble identifying the differences between Microsoft 365 Defender, Defender for Cloud, Defender for Endpoint and the remaining 300 similar named Microsoft Defenders?
What;s wrong with these Microsoft people, they are masochists or sth?

upvoted 18 times

✉  **Tbag90** 6 months, 2 weeks ago

I did always say that Microsoft needs to change the guys who are naming their products... It is so confusing

upvoted 4 times

✉  **kaheri** 1 year, 1 month ago

D correct answer

upvoted 2 times

✉  **clebsonjesus** 1 year, 2 months ago

Letra D

upvoted 1 times

走开 1 年, 3 个月 ago

Selected Answer: D

D - Compliance Score is the correct answer. The question doesn't ask you whether the tool is part of Azure cloud service or not. Don't be trapped on Secure score in Azure Security Center (and note that ASC is no longer the name now. It is Microsoft Defender for Cloud).

upvoted 2 times

Lizzylizzy 1 年, 3 个月 ago

Compliance score

upvoted 1 times

mikcs 1 年, 3 个月 ago

on exam 12/12/22

upvoted 1 times

Mouratov 1 年, 4 个月 ago

Selected Answer: D

Correct

upvoted 1 times

eli2022 1 年, 4 个月 ago

On exam 11/02/2022

upvoted 1 times

cantbeme 1 年, 7 个月 ago

on the exam today

upvoted 2 times

AdityaGupta 1 年, 7 个月 ago

Selected Answer: D

D is correct

upvoted 1 times

AbhilAM 1 年, 8 个月 ago

In exam today

upvoted 2 times

Question #8

Topic 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>

Community vote distribution

D (100%)

 **Melwin86** Highly Voted 2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>
upvoted 23 times

 **zellck** Most Recent 11 months ago

Got this in Apr 2023 exam.
upvoted 3 times

 **oiuyiyo** 11 months, 1 week ago

correct
upvoted 2 times

 **Johnvic** 12 months ago

On exam 3/30/23
upvoted 2 times

 **hululolo** 1 year ago

Appeared in exam on 3rd March
upvoted 3 times

 **ErosTargaryen** 1 year, 3 months ago

on exam 12/27/22
upvoted 3 times

 **mikcs** 1 year, 3 months ago

Selected Answer: D
on exam 12/12/22
upvoted 3 times

 **OrangeSG** 1 year, 3 months ago

Selected Answer: D
After you onboard Microsoft Sentinel into your workspace, you can use data connectors to start ingesting your data into Microsoft Sentinel. Microsoft Sentinel comes with many out-of-the-box connectors for Microsoft services, which you can integrate in real time.

Microsoft Sentinel data connectors

<https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources>
upvoted 3 times

 **eli2022** 1 year, 4 months ago

On exam 11/02/2022
upvoted 2 times

 **Lone_Wolf** 1 year, 5 months ago

Correct Answer: D!

upvoted 4 times

 **pborlas** 1 year, 5 months ago

Selected Answer: D

Correct Answer : D

upvoted 3 times

 **Armanas** 1 year, 6 months ago

Selected Answer: D

Correct Answer : D

<https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>

upvoted 1 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 2 times

 **AdityaGupta** 1 year, 7 months ago

Selected Answer: D

D is correct

upvoted 1 times

 **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 1 times

 **gustavomelquiades** 1 year, 9 months ago

Selected Answer: D

Answer is: D

"Microsoft Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity (formerly Azure ATP), and Microsoft Defender for Cloud Apps, and more. "

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

upvoted 3 times

 **Pedre** 1 year, 9 months ago

Selected Answer: D

correct

upvoted 3 times

Question #9

Topic 1

Which Microsoft portal provides information about how Microsoft cloud services comply with regulatory standard, such as International Organization for Standardization (ISO)?

- A. the Microsoft Endpoint Manager admin center
- B. Azure Cost Management + Billing
- C. Microsoft Service Trust Portal
- D. the Azure Active Directory admin center

Correct Answer: C

The Microsoft Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide>

Community vote distribution

C (100%)

 **Melwin86** Highly Voted 2 years, 8 months ago
correct

<https://servicetrust.microsoft.com/>
upvoted 24 times

 **qdam** Highly Voted 2 years, 2 months ago

Selected Answer: C
C is correct
upvoted 12 times

 **Tahamaffia** Most Recent 6 months, 2 weeks ago

Got this question on my exam 05/09/2023
upvoted 1 times

 **Darkfire** 8 months ago

Selected Answer: C
C is correct
upvoted 1 times

 **franky_sagan** 9 months, 2 weeks ago

Selected Answer: C
C is Correct
upvoted 1 times

 **King_Lam** 12 months ago

In Exam 31st March.
upvoted 3 times

 **Ibbxtreme** 1 year ago

Selected Answer: C
C is the way to go
upvoted 2 times

 **hululolo** 1 year ago

Appeared in exam on 3rd March
upvoted 1 times

 **ErosTargaryen** 1 year, 3 months ago

I agree
<https://servicetrust.microsoft.com/>

It also shows in exam today 12/27/2022
upvoted 2 times

②  **OrangeSG** 1 year, 3 months ago

Selected Answer: C

The Service Trust Portal is Microsoft's public site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services.

Get started with Microsoft Service Trust Portal

<https://learn.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal>

upvoted 2 times

②  **ricardo_27_04_1978** 1 year, 3 months ago

I agree, and it is intuitive. Actually, it is correct based on the evidences too.

upvoted 1 times

②  **eli2022** 1 year, 4 months ago

On exam 11/02/2022

upvoted 1 times

②  **ICTZaakwaarnemer2022** 1 year, 5 months ago

sdvsdvs

upvoted 2 times

②  **Emmuyah** 1 year, 5 months ago

Microsoft Service Trust Portal is the correct answer

upvoted 2 times

②  **CataM22** 1 year, 6 months ago

A variant of this question appeared in the exam today, September 5th 2022

upvoted 1 times

②  **AdityaGupta** 1 year, 7 months ago

Selected Answer: C

C is correct

upvoted 1 times

②  **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 1 times

Question #10

Topic 1

In the shared responsibility model for an Azure deployment, what is Microsoft solely responsible for managing?

- A. the management of mobile devices
- B. the permissions for the user data stored in Azure
- C. the creation and management of user accounts
- D. the management of the physical hardware

Correct Answer: D

Community vote distribution

D (100%)

 **Melwin86** Highly Voted 2 years, 8 months ago
correct

<https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
upvoted 28 times

 **KoosDuppen** Highly Voted 1 year, 11 months ago
if in doubt, try to eliminate the obvious. If you do this here, you will probably end up at D anyways...
upvoted 5 times

 **stewbiee** Most Recent 5 months, 3 weeks ago
Selected Answer: D
Correct
upvoted 2 times

 **Darkfire** 8 months ago
Selected Answer: D
D is correct

<https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
upvoted 1 times

 **Mouratov** 1 year, 4 months ago
Selected Answer: D
Correct
upvoted 4 times

 **exampro99** 1 year, 5 months ago
Selected Answer: D
correct
upvoted 2 times

 **pborlas** 1 year, 5 months ago
Answare is D:
upvoted 1 times

 **AdityaGupta** 1 year, 7 months ago
Selected Answer: D
IaaS services used by any customer is always MS responsibility.
upvoted 3 times

 **Yelad** 1 year, 8 months ago
On the exam 10/07/2022
upvoted 2 times

 **gustavomelquiades** 1 year, 9 months ago
Selected Answer: D
Answare is D:
"Diagram showing responsibility zones."
<https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
upvoted 4 times

Endi99 1 year, 11 months ago

Selected Answer: D

correct answer

upvoted 2 times

Tommo 1 year, 11 months ago

Selected Answer: D

correct

upvoted 2 times

yamanktish 2 years ago

Selected Answer: D

D is correct

upvoted 2 times

BlackdaRipper 2 years ago

Correct answer

upvoted 2 times

AZ_Student 2 years, 1 month ago

D is the right option.

upvoted 1 times

AJ86 2 years, 2 months ago

Selected Answer: D

D is correct

upvoted 3 times

qdam 2 years, 2 months ago

D is correctly

upvoted 2 times

Question #11

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	<input type="radio"/>	<input type="radio"/>
Assume breach is one of the guiding principles of Zero Trust.	<input type="radio"/>	<input type="radio"/>
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	<input checked="" type="radio"/>	<input type="radio"/>
Assume breach is one of the guiding principles of Zero Trust.	<input checked="" type="radio"/>	<input type="radio"/>
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

Box 2: Yes -

Box 3: No -

The Zero Trust model does not assume that everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network.

Reference:

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

✉  **yulexam** Highly Voted 2 years, 4 months ago

Correct...

principles of zero trust: Verify explicitly, Least privileged access, Assume breach

upvoted 29 times

✉  **Matic_Prime** Highly Voted 2 years, 7 months ago

correct

upvoted 17 times

✉  **user_666** Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 2 times

✉  **JXC** 3 months, 2 weeks ago

Got this - Dec2023

upvoted 1 times

✉  **RahulX** 7 months, 2 weeks ago

Microsoft Zero Trust is a security strategy based on the principle of Verify explicitly, Use least privilege access, Assume breach.

upvoted 2 times

✉  **zellck** 11 months ago

Got this in Apr 2023 exam.

upvoted 3 times

✉  **Kelsi999** 11 months ago

The answers are correct.

I had this question on the exam today

upvoted 3 times

✉ **kxa57482** 1 year ago

YES YES NO

upvoted 3 times

✉ **Whyiest** 1 year, 2 months ago

Correct

upvoted 3 times

✉ **mikcs** 1 year, 3 months ago

on exam 12/12/22

upvoted 3 times

✉ **eli2022** 1 year, 4 months ago

On exam 11/02/2022

upvoted 2 times

✉ **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected Y Y N

upvoted 2 times

✉ **cantbeme** 1 year, 7 months ago

on exam today

upvoted 1 times

✉ **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 1 times

✉ **gustavomelquiades** 1 year, 9 months ago

Answare is - Y Y N

"This is the core of Zero Trust. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network."

<https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-overview>

upvoted 3 times

✉ **sensa** 1 year, 11 months ago

appeared on my exam today

upvoted 2 times

✉ **GMardones** 1 year, 12 months ago

Correct

upvoted 1 times

Question #12

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	<input type="radio"/>	<input type="radio"/>
Transparency is a key privacy principle of Microsoft.	<input type="radio"/>	<input type="radio"/>
Shared responsibility is a key privacy principle of Microsoft.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	<input checked="" type="radio"/>	<input type="radio"/>
Transparency is a key privacy principle of Microsoft.	<input checked="" type="radio"/>	<input type="radio"/>
Shared responsibility is a key privacy principle of Microsoft.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://privacy.microsoft.com/en-US/>

 **An_is_here** Highly Voted 2 years, 8 months ago

The answer is CORRECT.

The Six privacy principles are:

Control: We will put you in control of your privacy with easy-to-use tools and clear choices.

Transparency: We will be transparent about data collection and use so you can make informed decisions.

Security: We will protect the data you entrust to us through strong security and encryption.

Strong legal protections: We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

No content-based targeting: We will not use your email, chat, files or other personal content to target ads to you.

Benefits to you: When we do collect data, we will use it to benefit you and to make your experiences better.

upvoted 120 times

 **Indy429** 1 year, 5 months ago

thanks for explaining in the comments!

upvoted 4 times

 **yulexam** Highly Voted 2 years, 4 months ago

correct...

6 key privacy principle: control, transparency, security, strong legal protection, no content based targeting, benefits to you

upvoted 20 times

 **user_666** Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 2 times

 **RahulX** 7 months, 2 weeks ago

Ans by Chat GPT: Customer control, transparency, and strong legal protections for privacy

Security and encryption of data

No content-based targeting of advertising

Inclusive, fair, and easy-to-use tools and choices

Supervisable and environmentally responsible digital identity

upvoted 2 times

 **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 2 times

studytonight 10 months ago

This was on the May 2023 exam. I got a lot of HOTSPOT type questions.

upvoted 2 times

zellck 11 months ago

Got this in Apr 2023 exam.

upvoted 3 times

Kelsi999 11 months ago

The answer is correct.

I had this question on the exam today.

upvoted 2 times

mikcs 1 year, 3 months ago

on exam 12/12/22

upvoted 2 times

eli2022 1 year, 4 months ago

On exam 11/02/2022

upvoted 1 times

Vinci123 1 year, 5 months ago

Six privacy principles

Firstly, Control. Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.

Secondly, Transparency. Being transparent about data collection and use so that everyone can make informed decisions.

Thirdly, Security. Protecting the data that's entrusted to Microsoft by using strong security and encryption.

Then, Strong legal protections. Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

After that, No content-based targeting. Not using email, chat files, or other personal content to target advertising.

Lastly, Benefits. When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better.

upvoted 2 times

Vinci123 1 year, 5 months ago

<https://learn.microsoft.com/en-us/training/modules/responsible-ai-principles/>

1. fairness
2. Reliability and safety
3. Privacy and security
4. Inclusiveness
5. Transparency
6. Accountability.

upvoted 1 times

cantbeme 1 year, 7 months ago

in exam today

upvoted 2 times

cormorant 1 year, 8 months ago

SHARED RESPONSIBILITY IS NOT A PRINCIPLE

upvoted 8 times

Yelad 1 year, 8 months ago

On the exam 10/07/2022

upvoted 3 times

Twitchy_A2 1 year, 11 months ago

This link is a better to review the principles, <https://www.microsoft.com/en-us/trustcenter/privacy/%E2%80%AF#section3>

upvoted 5 times

sensa 1 year, 11 months ago

appeared on my exam today

upvoted 3 times

Question #13

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

▼
Archiving
Compressing
Deduplicating
Encrypting

a file makes the data in the file readable and usable to viewers that have the appropriate key.

Correct Answer:**Answer Area**

▼
Archiving
Compressing
Deduplicating
Encrypting

a file makes the data in the file readable and usable to viewers that have the appropriate key.

✉ **P_2311** Highly Voted 2 years, 8 months agoabsolutely right
upvoted 26 times✉ **objegli** Highly Voted 2 years, 2 months agoIs this typo mistake? Should be decryption, right?
Encryption is a process of converting normal data into an unreadable form.
Decryption is a method of converting the unreadable/coded data into its original form.
upvoted 17 times✉ **Clouddog** 2 years ago

I thought the same. But in the question it says "to viewers that have the appropriate key". So keyword is the word "KEY".

Encryption is a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information.

Decryption is a process that transforms encrypted information into its original format. To do this, parties to a private conversation use an encryption scheme, called an algorithm, and the keys to encrypt and decrypt messages.
upvoted 10 times✉ **AshutoshSingh** 2 years, 2 months agoI have the same doubt
upvoted 3 times✉ **BantyLee** 7 months, 2 weeks agoThe KEYword there is "KEY"... so anyone with appropriate key will be able to read it when it's encrypted.
upvoted 2 times✉ **Kopter** Most Recent 9 months agoI will exam next month. I think the correct answer is Encryption
upvoted 1 times✉ **jaaake** 9 months agoYes, the question is tricky. But indeed it's encryption (the other 3 answers don't make sense).
upvoted 2 times✉ **latoupi** 11 months, 1 week agoLa réponse est correct, car l'encryption permet à celui qui a la clé de déchiffrement de pouvoir lire le message et le texte dit "a file makes the data in the file readable and usable to viewers that have the appropriate key"
upvoted 1 times✉ **Distinctive** 11 months, 1 week agoEncryption is the right answer
upvoted 3 times✉ **Nicochet** 1 year, 1 month ago

Correct. D is the option.

upvoted 1 times

✉ **ErosTargaryen** 1 year, 3 months ago

on exam 12/27/22

upvoted 1 times

✉ **walkaway** 1 year, 3 months ago

I don't understand why Decryption is an answer. Decryption can't happen without encryption. You all should read and repeat the sentence several times. Encryption is the method to make the file readable to people that have an appropriate key. I don't see any reason why Decryption is an answer. It must be ENCRYPTION.

Archiving, Compressing, Deduplicating are all irrelevant.

upvoted 3 times

✉ **Lizzylizzy** 1 year, 3 months ago

Question is kinda tricky I will go with encryption

upvoted 1 times

✉ **sibirnayek** 1 year, 3 months ago

YES CORRECT ANSWER

upvoted 1 times

✉ **SamNas** 1 year, 3 months ago

Correct

upvoted 1 times

✉ **AlbertKwan** 1 year, 4 months ago

how would "encrypting" makes the data in a file readable to human?

upvoted 1 times

✉ **PaulMD** 1 year, 3 months ago

...usable by viewers that have the appropriate key..

upvoted 1 times

✉ **npish** 1 year, 4 months ago

ENCRYPTION

upvoted 1 times

✉ **rama161** 1 year, 4 months ago

Correct

upvoted 2 times

✉ **YJC** 1 year, 5 months ago

Correct

upvoted 2 times

✉ **vskordas** 1 year, 6 months ago

C is DEDUPLICATING which is wrong not DECRYPTING

So the only correct is D

upvoted 1 times

Question #14

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	<input type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the public key of the signer.	<input type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the private key of the signer.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	<input checked="" type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the public key of the signer.	<input checked="" type="radio"/>	<input type="radio"/>
Verifying the authenticity of a digitally signed document requires the private key of the signer.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

A certificate is required that provides a private and a public key.

Box 2: Yes -

The public key is used to validate the private key that is associated with a digital signature.

Box 3: Yes -

The private key, or rather the password to the private key, validates the identity of the signer.

Reference:

<https://support.microsoft.com/en-us/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512>

<https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/fin-ops/organization-administration/electronic-signature-overview>

 **ThomasDehottay** Highly Voted  2 years, 5 months ago

Shouldn't it be Y,Y,N ? As the private key is only used (and owned) by the signer to sign the document, and the associated public key is used to verify the authenticity.

upvoted 185 times

 **Ravikant84** 1 year, 9 months ago

Yes Correct. It's YYN. Private key can not be used to verify the authenticity.

upvoted 7 times

 **TJ001** 2 years, 2 months ago

Y,Y,N - Agree

upvoted 11 times

 **Alexado** 2 years, 2 months ago

YYN, fully agree

upvoted 9 times

 **Tokiki** 2 years ago

Agree,it's yyn

upvoted 6 times

 **Contactfornitish** Highly Voted  2 years, 1 month ago

Appeared in exam on 12/02/2022

YYN is correct, I scored 1000/1000
upvoted 114 times

✉ **arpgaur** 1 year, 11 months ago

How many question did you encounter from these dumps. want to make sure if I am using legit dumps or not ? or is there any other forums where I can find more dumps
upvoted 10 times

✉ **SR1991** **Most Recent** 3 months, 1 week ago

For signature you use assymetric encryption.(<https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/5-describe-encryption-hashing>)

The sender's private key encrypts the data -- this is the digital signature -- and the receiver uses the public key to decrypt it and verify it matches the attachment. The public key and private key in digital signatures are mathematically related but cannot be generated from each other. (<https://www.techtarget.com/searchsecurity/answer/Which-private-keys-and-public-keys-can-create-a-digital-signature#:~:text=The%20sender's%20private%20key%20encrypts,be%20generated%20from%20each%20other.>)

So with this information the answers will be:

Q1 Yes, private key is used for digital signature.
Q2 Yes, authenticity for the signature requires a public key
Q3 No, this is for encrypting the data.

upvoted 1 times

✉ **jg_85** 3 months, 3 weeks ago

YYN for Sure
upvoted 1 times

✉ **xRiot007** 6 months, 2 weeks ago

Yes, Yes, No
The private key of the signer is known only by the signer.
upvoted 1 times

✉ **RahulX** 7 months, 2 weeks ago

Yes
Yes
NO
upvoted 1 times

✉ **Kopter** 9 months ago

I agree YYN.
upvoted 1 times

✉ **jaaake** 9 months ago

YYN. If you have access to another party's private key, something is amiss!
upvoted 1 times

✉ **AKATTHULA** 10 months, 2 weeks ago

YYN. Private key is only used for signing and not for authenticating.
upvoted 2 times

✉ **NitinRajNigam** 10 months, 2 weeks ago

Y,Y,N should be the right answer.
upvoted 1 times

✉ **Misty39** 11 months, 3 weeks ago

digitally signing a document requiring a private key is correct. However, the second statement is incorrect. Verifying the authenticity of a digitally signed document requires the public key of the signer, not the private key.
When a document is digitally signed, the signer uses their private key to create a unique signature for the document. This signature is then attached to the document. To verify the authenticity of the signed document, the recipient uses the signer's public key, which is openly shared. The public key allows the recipient to confirm that the signature was indeed created with the signer's private key, thus verifying the document's authenticity and ensuring that it has not been tampered with.

upvoted 1 times

✉ **Pady1234** 1 year ago

Y, Y, N
upvoted 1 times

✉ **Asirpa** 1 year ago

I know and understand why for the exam the answer is YYN, but for discussion sake can't you theoretically sign something with someone's public key so that only the intended recipient can read it? So rather than authenticity you are focusing on confidentiality.
upvoted 1 times

✉ **hululolo** 1 year ago

Appeared in exam on 3rd March
upvoted 1 times

✉  **kaheri** 1 year, 1 month ago

YYN

For any reason you should share your private key

upvoted 1 times

✉  **Cololand** 1 year, 1 month ago

YYN ist korrekt

upvoted 1 times

✉  **Eduardo_S** 1 year, 2 months ago

If you have the private key of the signer then it is not private anymore. The correct answer should be YYN

upvoted 1 times

Question #15

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

When users sign in to the Azure portal, they are first

assigned permissions.
authenticated.
authorized.
resolved.

Answer Area

When users sign in to the Azure portal, they are first

Correct Answer:

assigned permissions.
authenticated.
authorized.
resolved.

AZ_Student Highly Voted 2 years, 1 month ago

HIGHLY correct.

Authentication is who you say you are.

Authorization is what permission to do you have.

upvoted 26 times

gustangelo Highly Voted 2 years, 4 months ago

Correct

upvoted 13 times

Kelsi999 Most Recent 11 months ago

On the exam today. The answer is correct

upvoted 2 times

Cololand 1 year, 1 month ago

Wording of this question is a bit confusing.

upvoted 1 times

Whyest 1 year, 2 months ago

When you want to connect, here is the pattern :

Authentication → Roles attributed → Authorization in function of the permission of the roles

upvoted 5 times

Lizzylizzy 1 year, 3 months ago

Authenticated

upvoted 1 times

mikcs 1 year, 3 months ago

on exam 12/12/22

upvoted 1 times

JulianDres5845 1 year, 5 months ago

Correct

upvoted 2 times

cantbeme 1 year, 7 months ago

on exam today

upvoted 2 times

AdityaGupta 1 year, 7 months ago

legitimacy of user is checked first (Authentication) later the permissions/ roles are checked to give him Authorization to work on resources.

upvoted 4 times

AbhilAM 1 year, 8 months ago

In exam today

upvoted 2 times

✉  **AhmedEn** 1 year, 10 months ago

correct

upvoted 2 times

✉  **idhashi** 1 year, 10 months ago

Correct

upvoted 1 times

✉  **Tommo** 1 year, 11 months ago

Correct

upvoted 1 times

✉  **Justin0020** 1 year, 11 months ago

Had this question on exam. Right answer.

upvoted 4 times

✉  **Tokiki** 2 years ago

Correct

upvoted 3 times

✉  **BlackdaRipper** 2 years ago

Absolutely correct

upvoted 4 times

Question #16

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

▼	is the process of identifying whether a signed-in user can access a specific resource.
Authentication	
Authorization	
Federation	
Single sign-on (SSO)	

Correct Answer:**Answer Area**

▼	is the process of identifying whether a signed-in user can access a specific resource.
Authentication	
Authorization	
Federation	
Single sign-on (SSO)	

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>

✉ **[Removed]** Highly Voted 2 years, 4 months ago

Correct - from: <https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization> > "...authorization (providing access to secure data)..."

upvoted 30 times

✉ **gustangelo** Highly Voted 2 years, 4 months ago

correct, next.

upvoted 11 times

✉ **Distinctive** 11 months, 1 week ago

next 😁😁😁😁

upvoted 1 times

✉ **jrop** 10 months, 1 week ago

next!!!

upvoted 1 times

✉ **xRiot007** Most Recent 6 months, 2 weeks ago

Authentication - done first, will verify user credentials.

Authorization - done second, will verify if the user action is permissible based on his roles/permissions

upvoted 1 times

✉ **hululolo** 1 year ago

Appeared in exam on 3rd March

upvoted 5 times

✉ **Whyiest** 1 year, 2 months ago

It's correct. Pattern of connection :

Authentication → Roles attributed → Authorization in function of the permission of the roles

upvoted 1 times

✉ **FBrabble** 1 year, 4 months ago

yes correct answer!

upvoted 1 times

✉ **Juliandres5845** 1 year, 5 months ago

Correct

upvoted 2 times

✉ **AdityaGupta** 1 year, 7 months ago

legitimacy of user is checked first (Authentication) later the permissions/ roles are checked to give him Authorization to work on resources.

upvoted 3 times

□ **AbhilAM** 1 year, 8 months ago

In exam today with some rewording
upvoted 2 times

□ **cormorant** 1 year, 8 months ago

authorisation to check a user's eligibility to use a resource
upvoted 4 times

□ **Yelad** 1 year, 8 months ago

On the exam 10/07/2022
upvoted 4 times

□ **idhashi** 1 year, 10 months ago

Correct
upvoted 2 times

□ **Tommo** 1 year, 11 months ago

Correct
upvoted 1 times

□ **Justin0020** 1 year, 11 months ago

Had this question on exam. Right answer.
upvoted 3 times

□ **Tokiki** 2 years ago

Correct
upvoted 1 times

□ **bikewun** 2 years ago

CORRECT
upvoted 2 times

□ **BlackdaRipper** 2 years ago

Correct answer. Easy!!
upvoted 2 times

Question #17

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Active Directory Domain Services (AD DS)
Active Directory forest trusts
Azure Active Directory (Azure AD) business-to-business (B2B)
Azure Active Directory business-to-consumer B2C (Azure AD B2C)

enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Correct Answer:**Answer Area**

Active Directory Domain Services (AD DS)
Active Directory forest trusts
Azure Active Directory (Azure AD) business-to-business (B2B)
Azure Active Directory business-to-consumer B2C (Azure AD B2C)

enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b>

✉  **TheSwedishGuy**  2 years, 5 months ago

Correct.

"Azure Active Directory (Azure AD) business-to-business (B2B) collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization. With B2B collaboration, you can securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data."

upvoted 44 times

✉  **Yelad**  1 year, 8 months ago

On the exam 10/07/2022

upvoted 6 times

✉  **furq2904**  8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 2 times

✉  **gggggggggggggggg** 10 months, 3 weeks ago

business-to-business (B2B) is the correct answer

upvoted 1 times

✉  **pifpaff** 1 year ago

correct !

upvoted 3 times

✉  **Nicochet** 1 year, 1 month ago

Correct

upvoted 2 times

✉  **AdityaGupta** 1 year, 7 months ago

Azure Active Directory (Azure AD) business-to-business (B2B)

upvoted 4 times

✉  **kazan** 1 year, 9 months ago

Correct

upvoted 1 times

✉  **Tommo** 1 year, 11 months ago

Correct

upvoted 1 times

✉  **Justin0020** 1 year, 11 months ago

Had this question on exam. Right answer.

upvoted 3 times

✉  **bikewun** 2 years ago

CORRECT

upvoted 2 times

 **BlackdaRipper** 2 years ago

CORRECT ANSWER

upvoted 2 times

 **AZ_Student** 2 years, 1 month ago

Correct

upvoted 3 times

 **Contactfornitish** 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 4 times

 **Adil251** 2 years, 3 months ago

cORRECT

upvoted 4 times

 **Jitusrit** 2 years, 5 months ago

Correct.

upvoted 4 times

Question #18

Topic 1

In the Microsoft Cloud Adoption Framework for Azure, which two phases are addressed before the Ready phase? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Plan
- B. Manage
- C. Adopt
- D. Govern
- E. Define Strategy

Correct Answer: AE

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview>

Community vote distribution



AE (100%)

✉  **yulexam**  2 years, 4 months ago

A, E Correct...
cloud adoption framework: strategy, plan, ready, adopt, govern, manage (SPRAGM) :)
upvoted 96 times

✉  **TJ001** 2 years, 2 months ago

nice acronym , correct answer
upvoted 7 times

✉  **JA2018** 2 years, 2 months ago

Hi, I think you had missed out the "Migrate" stage. Just my 2 cents' worth.
upvoted 3 times

✉  **Swapdevs** 2 years, 1 month ago

Adoption includes Migrate and Innovate
upvoted 4 times

✉  **lime568** 2 years, 2 months ago

Adopt include migrate
upvoted 1 times

✉  **Contactfornitish**  2 years, 1 month ago

Appeared in exam on 12/02/2022
upvoted 14 times

✉  **theptr**  7 months ago

Selected Answer: AE

AE ==> correct
upvoted 3 times

✉  **ltp1120** 9 months, 2 weeks ago

i dont see this term in microsoft learn sc-900 :(
upvoted 4 times

✉  **ConfusedPM** 9 months ago

yeah me too, I think they removed it
upvoted 1 times

✉  **Molota** 10 months ago

AE - Plan and define your strategy
upvoted 1 times

✉  **emmye** 1 year, 2 months ago

The 2022 article outlined the 6 methodologies including Migrate Innovate secure and organise
upvoted 1 times

✉  **yonie** 1 year, 3 months ago

Selected Answer: AE

AE correct

upvoted 2 times

 Lizzylizzy 1 year, 3 months ago

Plan and define your strategy

upvoted 1 times

 ricardo_27_04_1978 1 year, 3 months ago

Like in some other cases it is self intuitive. Actions like adopt, govern or manage, require something to be built first. Strategy and plan, do not.

upvoted 1 times

 yogur83 1 year, 4 months ago**Selected Answer: AE**

Plan and Define Strategy

upvoted 2 times

 Rayo80 1 year, 6 months ago

A and E

upvoted 2 times

 AdityaGupta 1 year, 7 months ago**Selected Answer: AE**

Plan and Define Strategy

upvoted 3 times

 cormorant 1 year, 8 months ago

adopt strategy and plan makes more sense to be the beginning anyway

upvoted 1 times

 daveyk00 1 year, 8 months ago**Selected Answer: AE**Correct <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview>

upvoted 2 times

 jmartingnlz 1 year, 9 months ago**Selected Answer: AE**

A,E Correct

upvoted 1 times

 kazan 1 year, 9 months ago**Selected Answer: AE**

Looks correct

upvoted 1 times

 Sussi04 1 year, 9 months ago**Selected Answer: AE**

A,E are correct answers

upvoted 1 times

Question #19

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input type="radio"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	<input type="radio"/>	<input checked="" type="radio"/>
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input checked="" type="radio"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input checked="" type="radio"/>	<input type="radio"/>

✉  **sas000** Highly Voted  2 years, 2 months ago

NYY is correct

upvoted 62 times

✉  **AbdullahSalam** Highly Voted  2 years, 2 months ago

Not correct. It should be N N Y

upvoted 23 times

✉  **TJ001** 2 years, 2 months ago

cloud providers own the physical networks(underlying fabric network) the virtual networks are defined by organization

upvoted 21 times

✉  **ZenLeow** 1 year, 9 months ago

Question says physical network not virtual network. That's microsoft's baby

upvoted 19 times

✉  **Eagrob_11** 9 months, 3 weeks ago

In IAAS it's managing physical network is the responsibility of cloud provider not the organization, so answer is NY.

upvoted 4 times

✉  **f8c8be5** 3 months, 2 weeks ago

In the second question, it says "PHYSICAL NETWORK" which would be the the responsibility of the cloud provider.

upvoted 2 times

✉  **user_666** Most Recent  1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 1 times

✉  **SR1991** 3 months, 1 week ago

Correct answer is NY.

See the link below for the responsibilities:

<https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/2-describe-shared-responsibility-model>

upvoted 1 times

✉  **RahulX** 7 months, 2 weeks ago

NO

Yes

NO

upvoted 3 times

□  **Darkfire** 8 months ago

NYY is correct

IaaS

Responsibility transfers to cloud provider are:

- Physical Hosts
- Physical Network
- Physical datacenter

<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

upvoted 1 times

□  **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

□  **Kelsi999** 11 months ago

NYY is correct.

I had this question on the exam today

upvoted 7 times

□  **walkaway** 1 year, 3 months ago

N Y Y.

For those who still think 3rd is a YES, read the following statement from Microsoft Docs

For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type).

Regardless of the type of deployment, the following responsibilities are always retained by you:

- Data
- Endpoints
- Account
- Access management

Ref: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility#division-of-responsibility>

upvoted 9 times

□  **mikcs** 1 year, 3 months ago

on exam 12/12/22

upvoted 1 times

□  **yogur83** 1 year, 4 months ago

NYY is correct

upvoted 2 times

□  **Mooooosa** 1 year, 5 months ago

Please understand and review question

Assume we take this services SAAS , IaaS or

1 : In SaaS - system updates - Cloud Provider

2 : We take IaaS : Physical Network - Cloud Provider

3. We take cloud services which provides IAAS, SaaS Paas from provider , We give data and information - organization

upvoted 3 times

□  **Mrpython** 1 year, 6 months ago

N Y Y is correct

upvoted 2 times

□  **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected N Y Y

<https://docs.microsoft.com/en-us/learn/modules/describe-security-concepts-methodologies/2-describe-shared-responsibility-model>

upvoted 4 times

□  **be9z** 1 year, 7 months ago

The third question is No: Answer is NYN: See reference: <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>. Confirm and upvote

upvoted 6 times

□  **AdityaGupta** 1 year, 7 months ago

NYY is correct answer. Physical security of Network Infra is always a responsibility of Cloud service provider.

upvoted 1 times

□  **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 5 times

Question #20

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	<input type="radio"/>	<input type="radio"/>
Hybrid identity requires the implementation of two Microsoft 365 tenants.	<input type="radio"/>	<input type="radio"/>
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	<input checked="" type="radio"/>	<input type="radio"/>
Hybrid identity requires the implementation of two Microsoft 365 tenants.	<input type="radio"/>	<input checked="" type="radio"/>
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	<input checked="" type="radio"/>	<input type="radio"/>

✉  **User_Mowgli**  1 year, 6 months ago

Correct

upvoted 13 times

✉  **fko8**  4 months, 2 weeks ago

AD Connect is now called Entra Connect

upvoted 5 times

✉  **pifpaff**  1 year ago

the answer is correct

upvoted 3 times

✉  **me2023** 1 year, 2 months ago

Answer is YNY

upvoted 3 times

✉  **cris_exam** 1 year, 2 months ago

YNY is correct

upvoted 3 times

✉  **jsl101669** 1 year, 4 months ago

ADDs is a cloud service. On-Prem is what is required for AADConnect. I think the answer is YNN.

upvoted 1 times

✉  **luckyiki** 1 year, 4 months ago

Actually Active Directory Domain Services is a service within the AD and is not a cloud service

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

upvoted 3 times

✉  **walkaway** 1 year, 3 months ago

Azure ADDS is different from ADDS. The name says it all.

upvoted 5 times

✉  **FBrabble** 1 year, 4 months ago

Y N Y = correct

upvoted 3 times

✉  **abilioneto** 1 year, 5 months ago

YNY are the correct ones

upvoted 4 times

 **Mrpython** 1 year, 6 months ago

Correct Answer

upvoted 4 times

Question #21

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

▼	provides benchmark recommendations and guidance for protecting Azure services.
Azure Application Insights	
Azure Network Watcher	
Log Analytics workspaces	
Security baselines for Azure	

Correct Answer:**Answer Area**

▼	provides benchmark recommendations and guidance for protecting Azure services.
Azure Application Insights	
Azure Network Watcher	
Log Analytics workspaces	
Security baselines for Azure	

Reference:

<https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cloud-services-security-baseline>

 **eddie_network_jedi** Highly Voted 2 years, 5 months ago

Correct, "guidance" here is the keyword.

guidance:baselines

upvoted 38 times

 **TheSwedishGuy** Highly Voted 2 years, 5 months ago

Correct.

"Security baselines for Azure help you strengthen security through improved tooling, tracking, and security features. They also provide you a consistent experience when securing your environment."

upvoted 14 times

 **user_666** Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 2 times

 **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 2 times

 **Nicochet** 1 year, 1 month ago

Security baselines for Azure

upvoted 2 times

 **Lizzylizzy** 1 year, 3 months ago

Security baseline for azure helps strengthen security

upvoted 1 times

 **AdityaGupta** 1 year, 7 months ago

D is correct answer

upvoted 2 times

 **cormorant** 1 year, 8 months ago

baselines provide benchmarks

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 2 times

 **Ravikant84** 1 year, 9 months ago

Benchmark = Baseline

upvoted 4 times

- ✉ **atanuforu** 1 year, 9 months ago
Security baselines for Azure
upvoted 1 times
- ✉ **Siddheshz** 1 year, 9 months ago
look for keyword 'benchmark' = baseline
upvoted 2 times
- ✉ **Ralgh** 1 year, 10 months ago
security=protection keyword
upvoted 2 times
- ✉ **Tommo** 1 year, 11 months ago
Correct
upvoted 1 times
- ✉ **BlackdaRipper** 2 years ago
CORRECT ANSWER
upvoted 3 times
- ✉ **Contactfornitish** 2 years, 1 month ago
Appeared in exam on 12/02/2022
upvoted 6 times
- ✉ **gamerongam** 2 years, 1 month ago
Correct,
<https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/security-center-security-baseline>
upvoted 2 times

Question #22

Topic 1

What is an example of encryption at rest?

- A. encrypting communications by using a site-to-site VPN
- B. encrypting a virtual machine disk
- C. accessing a website by using an encrypted HTTPS connection
- D. sending an encrypted email

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest>

Community vote distribution

B (100%)

 [Removed]  2 years, 4 months ago

Encryption at rest for PaaS customers

Platform as a Service (PaaS) customer's data typically resides in a storage service such as Blob Storage but may also be cached or stored in the application execution environment, such as a virtual machine. To see the encryption at rest options available to you, examine the Data encryption models: supporting services table for the storage and application platforms that you use.

upvoted 26 times

 walkaway  1 year, 3 months ago

A is Encryption in Transit

B is Encryption at Rest

C is Encryption in Transit

D is Encryption in Transit (it's still in transit because both senders and recipients need a key to read the content. This helps protect the content during mail sending transit)

upvoted 17 times

 Crucius  7 months, 1 week ago

Selected Answer: B

Correct.

upvoted 1 times

 furq2904 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

 Molota 10 months ago

B - is Encryption at Rest

upvoted 1 times

 Nicochet 1 year, 1 month ago

Option B

upvoted 1 times

 ricardo_27_04_1978 1 year, 3 months ago

at rest - not a communication. So, it must be VM Disk.

upvoted 1 times

 Indy429 1 year, 5 months ago

Key-word is "at-rest" - the only thing considered at-rest in the line-up is the VM disk

upvoted 3 times

 AdityaGupta 1 year, 7 months ago

Selected Answer: B

encrypting a virtual machine disk

upvoted 2 times

 Oeffnen 1 year, 8 months ago

Selected Answer: B

Correct

upvoted 2 times

 Yelad 1 year, 8 months ago

On the exam 10/07/2022

upvoted 5 times

 **jmartingnlz** 1 year, 9 months ago

Selected Answer: B

Correct

upvoted 4 times

 **atanuforu** 1 year, 9 months ago

B. encrypting a virtual machine disk

upvoted 2 times

 **Abrar_Ajmal** 1 year, 9 months ago

B is the correct answer here, quick question are all the other questions on SC-900 on the real exam as well please?

upvoted 2 times

 **gekkehenekie84** 1 year, 9 months ago

Selected Answer: B

VM disc is at rest once stored

upvoted 1 times

 **babai_02** 1 year, 9 months ago

Selected Answer: B

Correct

upvoted 2 times

 **Atpie** 1 year, 10 months ago

Selected Answer: B

Others are sending

upvoted 1 times

Question #23

Topic 1

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/>

Community vote distribution

BCD (100%)

✉  **indecisivez**  1 year, 11 months ago

BCD is correct

upvoted 20 times

✉  **Clouddog**  1 year, 11 months ago

Correct, Zero Trust is a security strategy. It is not a product or a service, but an approach in designing and implementing the following set of security principles:

Verify explicitly
Use least privilege access
Assume breach

upvoted 13 times

✉  **Clouddog** 1 year, 11 months ago

For more information: <https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-overview>

upvoted 3 times

✉  **Francielle**  2 months, 1 week ago

Selected Answer: BCD

C and D are Zero Trust principles, while B can also be explained by having the least possible privileges for an user (identity), thus being the primary security boundary.

upvoted 1 times

✉  **Crucius** 7 months, 1 week ago

Selected Answer: BCD

Correct.

upvoted 1 times

✉  **Molota** 10 months ago

B. Use identity as the primary security boundary. Most Voted
C. Always verify the permissions of a user explicitly. Most Voted
D. Always assume that the user system can be breached.

upvoted 1 times

✉  **ismalo** 1 year, 1 month ago

BCD is my answer

upvoted 1 times

✉  **walkaway** 1 year, 3 months ago

Selected Answer: BCD

Just use the exclusion method to answer this question. A and E violate Zero Trust principles.

BCD = Correct answer

upvoted 2 times

✉  **mikcs** 1 year, 3 months ago

Selected Answer: BCD

on exam 12/12/22

upvoted 2 times

✉ **yogur83** 1 year, 4 months ago

Selected Answer: BCD

<https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-overview>

upvoted 2 times

✉ **Zeus009** 1 year, 6 months ago

Correct

upvoted 3 times

✉ **cantbeme** 1 year, 7 months ago

on exam today

upvoted 4 times

✉ **simonseztech** 1 year, 7 months ago

Selected Answer: BCD

BCD is correct

upvoted 2 times

✉ **AdityaGupta** 1 year, 7 months ago

Selected Answer: BCD

B. Use identity as the primary security boundary. Most Voted

C. Always verify the permissions of a user explicitly. Most Voted

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

upvoted 1 times

✉ **tomtmario** 1 year, 8 months ago

Selected Answer: BCD

Correct answer

upvoted 1 times

✉ **choquedi** 1 year, 8 months ago

Selected Answer: BCD

Correct

upvoted 1 times

✉ **bercules** 1 year, 9 months ago

BCD is correct

upvoted 1 times

✉ **atanuforu** 1 year, 9 months ago

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.

upvoted 1 times

Question #24

Topic 1

HOTSPOT -

Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.

Hot Area:

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and a user profile icon. Below the bar, the heading 'Azure services' is displayed. There are several tiles representing different services: 'Create a resource' (plus sign icon), 'Alerts' (exclamation mark icon), 'Application Insights' (lightbulb icon), 'Subscriptions' (key icon), 'Policy' (hexagon icon), 'Azure AD Connect Health' (blue cube with heart icon), 'Security Center' (shield with lock icon), 'Advisor' (cloud with sun icon), 'Monitor' (speedometer icon), and a large blue arrow pointing right labeled 'More services'.

Correct Answer:

This screenshot is identical to the one above, but the 'Security Center' tile is highlighted with a green background, indicating it is the correct answer.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track>

advillella Highly Voted 1 year, 11 months ago

Azure Security Center and Azure Defender are now called Microsoft Defender for Cloud
upvoted 40 times

cormorant Highly Voted 1 year, 8 months ago

Which service should you use to view your Azure secure score?

sssssssecurity centre
upvoted 26 times

Crucius Most Recent 7 months, 1 week ago

Security Center
upvoted 1 times

□  **Darkfire** 8 months ago

It's Security Center in this example.
But it is now called Microsoft Defender for Cloud.

<https://learn.microsoft.com/nl-nl/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide>
upvoted 2 times

□  **Dhamus** 8 months, 2 weeks ago

It is now called Microsoft Defender for Cloud.
upvoted 1 times

□  **Dhamus** 10 months, 2 weeks ago

It is now called Microsoft Defender for Cloud.
upvoted 2 times

□  **Nicochet** 1 year, 1 month ago

Microsoft Defender for Cloud
upvoted 4 times

□  **yonie** 1 year, 3 months ago

=Microsoft Defender for Cloud
upvoted 3 times

□  **Lizzylizzy** 1 year, 3 months ago

Security center
upvoted 1 times

□  **abilioneto** 1 year, 5 months ago

correct
upvoted 2 times

□  **AdityaGupta** 1 year, 7 months ago

Azure Security Center
upvoted 2 times

□  **cormorant** 1 year, 8 months ago

security center for viewing your security score
upvoted 3 times

□  **clem24** 1 year, 10 months ago

correct
upvoted 2 times

□  **[Removed]** 1 year, 11 months ago

Correct
upvoted 3 times

Question #25

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	Answer Area
Corrective	Action subcategory Encrypt data at rest.
Detective	Action subcategory Perform a system access audit.
Preventative	Action subcategory Make configuration changes in response to a security incident.

Correct Answer:

Action Subcategories	Answer Area
Corrective	Preventative Encrypt data at rest.
Detective	Detective Perform a system access audit.
Preventative	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.

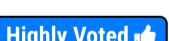
Box 3: Corrective -

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>

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证
微信添加 hello231119

✉  **Luanee**  1 year, 6 months ago

It's correct

upvoted 9 times

✉  **Zeus009**  1 year, 6 months ago

Aligned

upvoted 9 times

✉  **user_666**  1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 3 times

✉  **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023, but had only 2 boxes

upvoted 2 times

 **Kelsi999** 11 months ago

On the exam today. The answer is correct

upvoted 2 times

 **Nicochet** 1 year, 1 month ago

Correct

upvoted 2 times

 **mikcs** 1 year, 3 months ago

on exam 12/12/22

upvoted 3 times

 **rama161** 1 year, 4 months ago

All correct

upvoted 4 times

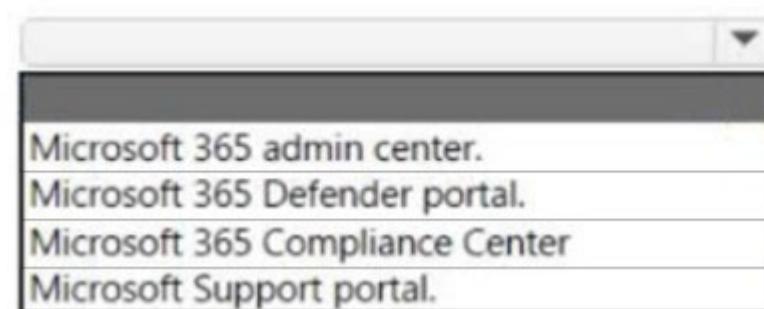
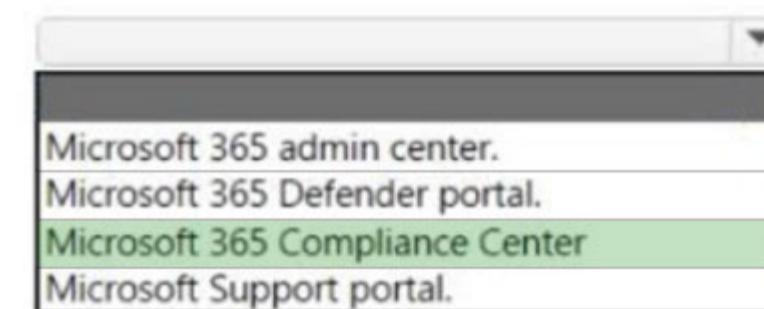
Question #26

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Compliance Manager can be directly accessed from the**Correct Answer:****Compliance Manager can be directly accessed from the**

Sign in to Compliance Manager -

1. Go to the Microsoft Purview compliance portal and sign in with your Microsoft 365 global administrator account.
2. Select Compliance Manager on the left navigation pane. You'll arrive at your Compliance Manager dashboard.

The direct link to access Compliance Manager is <https://compliance.microsoft.com/compliancemanager>

Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup>

Jeff_84 Highly Voted 1 year, 6 months ago

Compliance Centre is now known as Microsoft Purview
upvoted 32 times

Ola189 Highly Voted 1 year, 4 months ago

Correct but it's now called Microsoft Purview, not Microdoft 365 Compliance Centre.
upvoted 11 times

Molota Most Recent 10 months ago

Microdft 365 Compliance Centre IS Microsoft Purview
upvoted 2 times

XtraWest 11 months, 2 weeks ago

Microsoft Purview is correct
upvoted 2 times

yonie 1 year, 3 months ago

it's now called Microsoft Purview
upvoted 2 times

Lizzylizzy 1 year, 3 months ago

Compliance center now called purview
upvoted 2 times

yogur83 1 year, 4 months ago

In this case compliance center but MS has changed it to Microsoft Purview
upvoted 4 times

[Removed] 1 year, 5 months ago

Correct
upvoted 1 times

User_Mowgli 1 year, 6 months ago

Correct
upvoted 3 times

Question #27

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	<input type="radio"/>	<input type="radio"/>
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	<input type="radio"/>	<input type="radio"/>
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	<input checked="" type="radio"/>	<input type="radio"/>
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

Microsoft Secure Score has updated improvement actions to support security defaults in Azure Active Directory, which make it easier to help protect your organization with pre-configured security settings for common attacks.

If you turn on security defaults, you'll be awarded full points for the following improvement actions:

Ensure all users can complete multi-factor authentication for secure access (9 points)

Require MFA for administrative roles (10 points)

Enable policy to block legacy authentication (7 points)

Box 2: Yes -

Each improvement action is worth 10 points or less, and most are scored in a binary fashion. If you implement the improvement action, like create a new policy or turn on a specific setting, you get 100% of the points. For other improvement actions, points are given as a percentage of the total configuration.

Note: Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Box 3: Yes -

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score>

 **vorter** Highly Voted  1 year, 6 months ago

Wouldn't #3 be no, because that's the compliance score, not Secure Score?

upvoted 49 times

 **darkpangel** Highly Voted  1 year, 6 months ago

YN. Compliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide>

upvoted 20 times

 **jg_85** Most Recent  3 months, 3 weeks ago

YNN

3 Should be No, because that's the compliance score, not the Secure Score

upvoted 1 times

□ **RahulX** 6 months, 4 weeks ago

Yes
Yes
NO
upvoted 1 times

□ **Curious76** 7 months ago

YYN
For #3 be No, because that's the compliance score, not the Secure Score
upvoted 2 times

□ **jaaake** 9 months ago

YYN is correct. This is done by the Compliance Score
upvoted 2 times

□ **manofsteel9** 10 months ago

#3 should be "N".

Compliance Score, which is a separate feature in Microsoft 365, specifically focuses on assessing an organization's adherence to key regulations and standards for data protection and governance. Compliance Score evaluates actions and configurations related to compliance requirements, industry regulations, and data protection standards. It provides a score based on the completion of recommended actions related to compliance.

You can access the Microsoft 365 Security documentation at:
<https://docs.microsoft.com/en-us/microsoft-365/security/>

You can access the Microsoft 365 Compliance documentation at:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/>

These resources should provide you with comprehensive information about Microsoft Secure Score, Compliance Score, and their respective functionalities within the Microsoft 365 environment.

upvoted 2 times

□ **Micha338el** 10 months ago

Security Center assessments have been mapped to compliance regulations, such that each applicable regulation control has some assessments associated with it.
You can view your compliance relative to the supported controls of a regulation based on the passing vs. failing assessments that align with that regulation.
As you remediate more assessments, your compliance posture improves.
upvoted 1 times

□ **hululolo** 1 year ago

Appeared in exam on 3rd March
upvoted 4 times

□ **FiScorp_81** 1 year, 1 month ago

Correct answer YYN
3# is the Compliance Score
upvoted 5 times

□ **PinkUnicorns** 1 year, 2 months ago

YYN - Please correct
upvoted 7 times

□ **Charly0710** 1 year, 3 months ago

queda entonces YYN
upvoted 3 times

□ **walkaway** 1 year, 3 months ago

3 is a NO. The hint is the regulation and standards in the statement.

Compliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance.

upvoted 4 times

□ **Ajkom** 1 year, 4 months ago

YYN ,
<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-secure-score-across-the-microsoft-security-stack/ba-p/1938977>
upvoted 4 times

□ **FBrabble** 1 year, 4 months ago

YYN - "Compliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance. This baseline draws elements primarily from NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) and ISO (International Organization for Standardization), as well as from FedRAMP (Federal Risk and Authorization Management Program) and GDPR (General Data Protection Regulation of the European Union)." source: <https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide>

upvoted 6 times

FBabble 1 year, 4 months ago

agree - YYN is what I came up with prior to looking at this Q&A, so glad this community is here to help us learn!!!!

upvoted 4 times

palito1980 1 year, 4 months ago

YYN. "Regulations, standards for data protection and governance" is Compliance not secure score.

upvoted 2 times

Question #28

Topic 1

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: D

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common>

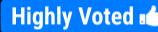
Community vote distribution

A (99%)

✉️  extrankie  2 years, 8 months ago

PIM is the correct answer A

upvoted 195 times

✉️  gills  2 years, 9 months ago

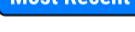
Provided answer is wrong. Should be A.

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

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

upvoted 95 times

✉️  AaronMedrano  1 month, 3 weeks ago

Selected Answer: A

Should be A.

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

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.

upvoted 1 times

✉️  mohamed.ali.elmasry 2 months, 1 week ago

PIM is the correct answer A

upvoted 1 times

✉️  frych 3 months, 1 week ago

Selected Answer: A

PIM is correct for short time access

upvoted 1 times

✉️  Jeroenexams 3 months, 3 weeks ago

Answer A, PIM relates to the Azure tasks

C seems incorrect because it says POLICY, not control

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-session>

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Defender for Cloud Apps portal to refine filters and set actions to take.

upvoted 1 times

✉️  chanc2023 4 months, 2 weeks ago

Most people vote for A and the answer provided by this site is D. So which one is the correct?

upvoted 1 times

✉️  geggio 5 months ago

Selected Answer: A

A right
upvoted 1 times

 **BrkyUlukn** 5 months ago

Correct answer is A:
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure> 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

upvoted 1 times

 **stewbiee** 6 months ago

Selected Answer: A
PIM is the correct answer A
upvoted 2 times

 **xRiot007** 6 months, 2 weeks ago

A - PIM because you give timed access
upvoted 3 times

 **Tahamaffia** 6 months, 2 weeks ago

Got this question on my exam 05/09/2023
upvoted 3 times

 **Tomix** 6 months, 3 weeks ago

A:
Azure Active Directory (Azure AD) Privileged Identity Management (PIM) allows you to grant temporary administrative roles to users for a specified duration, which can be set for two hours or any desired time frame. This ensures that users have elevated privileges only when needed and for a limited period.
upvoted 1 times

 **RahulX** 6 months, 4 weeks ago

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
upvoted 1 times

 **Mixxy1010** 7 months ago

PIM (A) - Conditional access is a sign on policies (allow / deny) - however you could enforce a 2 hour re-sign in policy, but it would not be fit for purpose of the question.
upvoted 1 times

 **theptr** 7 months ago

Selected Answer: A

A is correct
upvoted 1 times

 **Crucius** 7 months, 1 week ago

Selected Answer: A

Correct.
upvoted 1 times

Question #29

Topic 1

In a hybrid identity model, what can you use to sync identities between Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD)?

- A. Active Directory Federation Services (AD FS)
- B. Microsoft Sentinel
- C. Azure AD Connect
- D. Azure AD Privileged Identity Management (PIM)

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect>

Community vote distribution

C (100%)

✉  **frych** 3 months, 1 week ago

Selected Answer: C

AD Connect is called Entra Connect now
upvoted 1 times

✉  **fko8** 4 months, 2 weeks ago

AD Connect now is called Entra Connect
upvoted 1 times

✉  **Tahamaffia** 6 months, 2 weeks ago

Got this question on my exam 05/09/2023
upvoted 2 times

✉  **RahulX** 6 months, 4 weeks ago

C. Azure AD Connect
upvoted 1 times

✉  **Crucius** 7 months, 1 week ago

Selected Answer: C
Correct.
upvoted 1 times

✉  **manofsteel9** 10 months ago

Selected Answer: C
Correct answer
upvoted 2 times

✉  **hululolo** 1 year ago

Answer C
Appeared in exam on 3rd March
upvoted 4 times

✉  **RahulX** 1 year, 1 month ago

Yes Correct Ans is Azure AD connect.
upvoted 2 times

✉  **Skillplayer** 1 year, 1 month ago

Correct connect
upvoted 1 times

✉  **Lizzylizzy** 1 year, 3 months ago

Azure AD connect
upvoted 2 times

✉  **Mcelona** 1 year, 3 months ago

Selected Answer: C
C is Correct
upvoted 4 times

 **FBrabble** 1 year, 4 months ago

C correct

upvoted 3 times

 **[Removed]** 1 year, 5 months ago

Selected Answer: C

Coorect

upvoted 4 times

 **ruank** 1 year, 6 months ago

Selected Answer: C

Correct

upvoted 4 times

 **Derag** 1 year, 6 months ago

Azure AD Connect Sync Server, therefore, the answer is correct.

upvoted 3 times

 **Zeus009** 1 year, 6 months ago

Correct

upvoted 3 times

Question #30

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	<input type="radio"/>	<input type="radio"/>
Global administrator is a role in Azure Active Directory (Azure AD).	<input type="radio"/>	<input type="radio"/>
An Azure Active Directory (Azure AD) user can be assigned only one role.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	<input checked="" type="radio"/>	<input type="radio"/>
Global administrator is a role in Azure Active Directory (Azure AD).	<input checked="" type="radio"/>	<input type="radio"/>
An Azure Active Directory (Azure AD) user can be assigned only one role.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

Azure AD supports custom roles.

Box 2: Yes -

Global Administrator has access to all administrative features in Azure Active Directory.

Box 3: No -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles> <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

 **Melwin86** Highly Voted 2 years, 8 months ago

correct

1. <https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create>
 - 2,3 <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>
- upvoted 35 times

 **cantbeme** Highly Voted 1 year, 7 months ago

on exam today
upvoted 10 times

 **geggio** Most Recent 5 months ago

y-y-n right
upvoted 1 times

 **RahulX** 6 months, 4 weeks ago

YES
YES
NO
upvoted 1 times

 **bigelmo_elmo** 9 months ago

This is a question from AZ-900 exam as well
upvoted 1 times

zellck 11 months ago

Got this in Apr 2023 exam.

upvoted 3 times

hululolo 1 year ago

Appeared in exam on 3rd March

upvoted 7 times

RahulX 1 year, 1 month ago

Yes

Yes

No

upvoted 4 times

Nicochet 1 year, 1 month ago

Y,Y,N is the correct answer

upvoted 2 times

Mcelona 1 year, 3 months ago

Y,Y,N is the answer

upvoted 3 times

FBrabble 1 year, 4 months ago

Y, Y, N is correct for sure

upvoted 4 times

IXone 1 year, 5 months ago

Correct

upvoted 3 times

Zeus009 1 year, 6 months ago

Aligned

upvoted 3 times

AdityaGupta 1 year, 7 months ago

YYN is correct, multiple roles can be assigned to any user, including custom roles.

upvoted 3 times

AbhilAM 1 year, 8 months ago

In exam today

upvoted 3 times

I3ul3u 1 year, 8 months ago

Correct

upvoted 2 times

idhashi 1 year, 10 months ago

Correct

upvoted 2 times

Question #31

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) is an identity and access management service.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	<input type="radio"/>	<input checked="" type="radio"/>
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) is an identity and access management service.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No -

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Box 2: Yes -

Microsoft 365 uses Azure Active Directory (Azure AD). Azure Active Directory (Azure AD) is included with your Microsoft 365 subscription.

Box 3: Yes -

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide>

✉  **gchauhanabay**  2 years, 7 months ago

Correct is

False

True

True

upvoted 35 times

✉  **dynamicJames**  2 years, 7 months ago

Guys, of course you need/get an Azure AD when you license/buy a M365 tenant. Whenever you create Users via the admin.microsoft.com page, the users are created in the AAD "above".

So I go with:

False

True

True

upvoted 18 times

✉  **farcity** 2 years, 4 months ago

agreed

upvoted 2 times

✉  **RahulX**  6 months, 4 weeks ago

NO

YES

YES

upvoted 1 times

□ **manofsteel9** 10 months ago

The answer is F,T,T

Azure AD serves as the cloud-based identity and access management solution for Microsoft 365. It enables organizations to manage user identities, control access to resources, and secure applications and data in the Microsoft 365 environment. Azure AD is tightly integrated with Microsoft 365 services and provides the foundation for authentication and authorization across the suite of Microsoft cloud services.

You can access the Microsoft 365 documentation at:

URL: <https://docs.microsoft.com/en-us/microsoft-365/>

upvoted 1 times

□ **abilioneto** 1 year, 5 months ago

My guess is NYY

upvoted 7 times

□ **smartin2010** 1 year, 5 months ago

NYY, is correct.

upvoted 4 times

□ **cantbeme** 1 year, 7 months ago

on exam today

upvoted 4 times

□ **AdityaGupta** 1 year, 7 months ago

NYY, is correct.

upvoted 2 times

□ **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 4 times

□ **cormorant** 1 year, 8 months ago

azure AD is deployed to a cloud environment

upvoted 3 times

□ **bharatpatoliya** 1 year, 10 months ago

No, YES, YES..

upvoted 3 times

□ **Tommo** 1 year, 11 months ago

Correct

upvoted 1 times

□ **BlackdaRipper** 2 years ago

NO YES YES is the answer

upvoted 3 times

□ **G_unit_19** 2 years, 1 month ago

N,Y,Y is correct

upvoted 2 times

□ **Ronald88** 2 years, 3 months ago

Correct

false

true

true

upvoted 2 times

□ **Adil251** 2 years, 3 months ago

CORRECT

upvoted 2 times

□ **faricity** 2 years, 4 months ago

Answer is correct

upvoted 1 times

Question #32

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

With Windows Hello for Business, a user's biometric data used for authentication

- | |
|--|
| is stored on an external device. |
| is stored on a local device only. |
| is stored in Azure Active Directory (Azure AD). |
| is replicated to all the devices designated by the user. |

Correct Answer:**Answer Area**

With Windows Hello for Business, a user's biometric data used for authentication

- | |
|--|
| is stored on an external device. |
| is stored on a local device only. |
| is stored in Azure Active Directory (Azure AD). |
| is replicated to all the devices designated by the user. |

Biometrics templates are stored locally on a device.

Reference:

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

 **Jebli071** Highly Voted 2 years, 4 months ago

Correct !

upvoted 25 times

 **draadloos1973** Highly Voted 2 years ago

Correct, data is stored in the tpm chip

upvoted 13 times

 **Lipseal** 1 year, 9 months ago

I can't find where it says the biometric data is stored on the tpm chip. Are you sure?

upvoted 1 times

 **OG_Diablo** 1 year, 3 months ago

The thing that is saved on the TPM chip (if present) is the secure key. If a TPM chip is not available, software-based techniques are used to secure the key. (see <https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm#windows-hello-for-business>)

I also couldn't find a source that explains where specifically the biometric data is stored. Microsoft just says, "on the device":
<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#where-is-windows-hello-biometrics-data-stored>

upvoted 2 times

 **Tahamaffia** Most Recent 6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 3 times

 **RahulX** 6 months, 4 weeks ago

With Windows Hello for Business, as user's biometric data used for authentication is stored on a local device only.

upvoted 1 times

 **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

 **hululolo** 1 year ago

Answer: Local device

Appeared in exam on 3rd March

upvoted 4 times

 **RahulX** 1 year, 1 month ago

Is Stored in local Device Only.

upvoted 2 times

 **Nicochet** 1 year, 1 month ago

Only in local device

upvoted 1 times

✉ **globy118** 1 year, 2 months ago

Appeared in exam on 21/01/2023

upvoted 1 times

✉ **Lizzylizzy** 1 year, 3 months ago

Stored on a local device

upvoted 1 times

✉ **abilioneto** 1 year, 5 months ago

Correct

upvoted 3 times

✉ **Zeus009** 1 year, 6 months ago

Aligned

upvoted 2 times

✉ **AdityaGupta** 1 year, 7 months ago

Correct, data is stored locally.

upvoted 3 times

✉ **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 5 times

✉ **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

✉ **Olakunle24** 1 year, 10 months ago

The Windows Hello authenticator works to authenticate and allow employees onto your enterprise network. Authentication doesn't roam among devices, isn't shared with a server, and can't easily be extracted from a device. If multiple employees share a device, each employee will use his or her own biometric data on the device.

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise>

upvoted 4 times

✉ **imjoe** 1 year, 9 months ago

Here is the statement from your link:

The biometric data used to support Windows Hello is stored on the local device only. It doesn't roam and is never sent to external devices or servers.

upvoted 2 times

✉ **sensa** 1 year, 11 months ago

appeared on my exam today

upvoted 3 times

Question #33

Topic 1

What is the purpose of Azure Active Directory (Azure AD) Password Protection?

- A. to control how often users must change their passwords
- B. to identify devices to which users can sign in without using multi-factor authentication (MFA)
- C. to encrypt a password by using globally recognized encryption standards
- D. to prevent users from using specific words in their passwords

Correct Answer: D

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

Community vote distribution

D (100%)

✉ **Melwin86** Highly Voted 2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>
upvoted 30 times

✉ **jjrodriguezbriz** Highly Voted 2 years ago

Selected Answer: D

Correct

upvoted 12 times

✉ **Peace4ever** Most Recent 4 months, 2 weeks ago

I just passed my exam today, and this was one of the questions.
To prevent users from using specific words in their passwords
upvoted 1 times

✉ **RahulX** 6 months, 4 weeks ago

D. to prevent users from using specific words in their passwords
upvoted 1 times

✉ **Nemish71** 6 months, 4 weeks ago

correct
upvoted 1 times

✉ **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023, options were shuffled
upvoted 1 times

✉ **XtraWest** 11 months, 2 weeks ago

The purpose of Azure Active Directory (Azure AD) Password Protection is to help prevent common passwords and weak passwords from being used in Azure AD.
upvoted 2 times

✉ **MeisAdriano** 11 months, 2 weeks ago

why not A too?
upvoted 1 times

✉ **RahulX** 1 year, 1 month ago

D is correct ans.
upvoted 1 times

✉ **Nicochet** 1 year, 1 month ago

Correct
upvoted 1 times

✉ **mitchduck** 1 year, 4 months ago

Selected Answer: D

Correct

upvoted 2 times

  **JulianDres5845** 1 year, 5 months ago**Selected Answer: D**

Correct

upvoted 2 times

  **[Removed]** 1 year, 5 months ago**Selected Answer: D**

Correct

upvoted 2 times

  **abilioneto** 1 year, 5 months ago

correct

upvoted 2 times

  **Emmuyah** 1 year, 5 months ago

Correct

upvoted 1 times

  **AdityaGupta** 1 year, 7 months ago**Selected Answer: D**

Correct, to prevent from using already breached or common passwords.

upvoted 1 times

  **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

Question #34

Topic 1

Which Azure Active Directory (Azure AD) feature can you use to evaluate group membership and automatically remove users that no longer require membership in a group?

- A. access reviews
- B. managed identities
- C. conditional access policies
- D. Azure AD Identity Protection

Correct Answer: A

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

Community vote distribution

 A (100%)

✉  **Melwin86**  2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

upvoted 36 times

✉  **[Removed]**  1 year, 11 months ago

A is correct. But the description offered is not fully adequate for what access reviews do: there is no capability to AUTOMATICALLY remove user access rights. The whole point of (manual user-driven) access reviews is that in some cases automation isn't possible. (See the link already provided here: <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>)

upvoted 9 times

✉  **PC75**  5 months, 1 week ago

Selected Answer: A

Correct.

upvoted 1 times

✉  **RahulX** 6 months, 4 weeks ago

A. access reviews

upvoted 1 times

✉  **manofsteel9** 10 months ago

Selected Answer: A

A-Correct answer

upvoted 1 times

✉  **nobrainatall** 1 year, 1 month ago

Selected Answer: A

as suggested by Barbados

<https://youtu.be/kDRjQQ22Wkk>

upvoted 1 times

✉  **Whyest** 1 year, 2 months ago

Why there is no "dynamics groups" in the option ? I think it's an error :

Dynamic groups are used to automate the management of Azure Active Directory (AAD) group membership. They allow you to define rules to automatically add or remove users from a group based on certain criteria such as their job title or department.

Access reviews, on the other hand, are used to periodically review the access permissions of users to Azure resources. They allow you to identify and revoke unnecessary access, ensuring that only the right people have the right level of access to your resources. Access reviews can be done on role assignments, group memberships, and application assignments.

In summary, Dynamic groups are used to automatically manage group membership in AAD, while access reviews are used to periodically review and revoke unnecessary access to Azure resources, so here it must be Dynamic Groups or maybe I'm wrong ?

upvoted 5 times

✉  **Barbados** 1 year, 1 month ago

You're overthinking it. The key word in this question is "evaluate". You are given the option to set up recurring reviews and apply the decisions "automatically".

Check out this video and look at the slide around the 1:30 mark.

<https://youtu.be/kDRjQQ22Wkk>

upvoted 5 times

 **Lizzylizzy** 1 year, 3 months ago

Access review is the correct answer

upvoted 1 times

 **dd9396** 1 year, 3 months ago

A is correct, When the review is complete, access reviews can be set to manually or automatically remove access from the group membership or application assignment except for a dynamic group or originates from on-premises AD.

upvoted 2 times

 **InformacionFalsa** 1 year, 3 months ago

That would be wrong. Dynamic groups are the ones that do it AUTOMATICALLY. If that word wouldn't appear, then the right answer would be "A"

upvoted 1 times

 **mitchduck** 1 year, 4 months ago

Selected Answer: A

A is correct

upvoted 2 times

 **Lone_Wolf** 1 year, 5 months ago

KEYWORD

evaluate:review

Answer is A

upvoted 3 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 1 times

 **Zeus009** 1 year, 6 months ago

correct

upvoted 2 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 2 times

 **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 2 times

 **cormorant** 1 year, 8 months ago

ACCESS reviews - remove ACCESS rights

upvoted 1 times

Question #35

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Multi-factor authentication (MFA)
Pass-through authentication
Password writeback
Single sign-on (SSO)

requires additional verification, such as a verification code sent to a mobile phone.

Answer Area**Correct Answer:**

Multi-factor authentication (MFA)
Pass-through authentication
Password writeback
Single sign-on (SSO)

requires additional verification, such as a verification code sent to a mobile phone.

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

-  **Emmanski08** Highly Voted 1 year, 8 months ago
if you don't know this you shouldn't be taking the exam
upvoted 29 times
-  **Melwin86** Highly Voted 2 years, 8 months ago
correct

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa>
upvoted 20 times
-  **Peace4ever** Most Recent 4 months, 2 weeks ago
I just passed my exam today, and this was one of the questions: MFA.
upvoted 1 times
-  **RahulX** 6 months, 4 weeks ago
Multi-factor authentication (MFA)
upvoted 1 times
-  **manofsteel9** 10 months ago
Correct
upvoted 1 times
-  **RahulX** 1 year, 1 month ago
MFA is correct ans.
upvoted 2 times
-  **Zeus009** 1 year, 6 months ago
Correct
upvoted 1 times
-  **AbhilAM** 1 year, 8 months ago
In exam today
upvoted 3 times
-  **Tommo** 1 year, 11 months ago
CORRECT
upvoted 1 times

✉  **bikewun** 2 years ago

CORRECT

upvoted 1 times

✉  **BlackdaRipper** 2 years ago

MFA IS CORRECT

upvoted 1 times

✉  **Moddybaba** 2 years, 1 month ago

Correct answer selected (MFA)

upvoted 1 times

✉  **Contactfornitish** 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 3 times

✉  **qdam** 2 years, 2 months ago

correct answer

upvoted 3 times

✉  **Ronald88** 2 years, 3 months ago

Correct MFA

upvoted 2 times

✉  **Jitusrit** 2 years, 4 months ago

Correct ...mda response can be done via call, sms code, and auth app

upvoted 2 times

✉  **DALGMCI** 2 years, 4 months ago

correct!

upvoted 2 times

Question #36

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	<input type="radio"/>	<input type="radio"/>
Conditional access policies apply before first-factor authentication is complete.	<input type="radio"/>	<input type="radio"/>
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	<input type="radio"/>	<input type="radio"/>

Answer Area**Correct Answer:**

Statements	Yes	No
Conditional access policies can use the device state as a signal.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies apply before first-factor authentication is complete.	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

Box 2: No -

Conditional Access policies are enforced after first-factor authentication is completed.

Box 3: Yes -

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>✉  **Melwin86**  2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies>
upvoted 36 times✉  **Whyiest**  1 year, 2 months agoYNY Correct
upvoted 5 times✉  **user_666**  1 month, 3 weeks agohad this question on my exam today (01 feb 2024)
upvoted 1 times✉  **RahulX** 6 months, 4 weeks agoYES
NO
YES
upvoted 2 times✉  **Kelsi999** 11 months agoThe answer is correct.
I had this question on the exam today
upvoted 4 times✉  **cris_exam** 1 year, 2 months ago

YNY is correct.

upvoted 4 times

 **yonie** 1 year, 3 months ago

Question needs to be updated:

Device state (deprecated)

This preview feature has been deprecated. Customers should use the Filter for devices condition in the Conditional Access policy, to satisfy scenarios previously achieved using device state (preview) condition.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-deprecated>

upvoted 5 times

 **OG_Diablo** 1 year, 3 months ago

The answers are sort of correct. 'Device state' has since been deprecated. You can use 'Filter for devices' to achieve the same results (and much more).

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-deprecated>

upvoted 2 times

 **mikcs** 1 year, 3 months ago

on exam 12/12/22

upvoted 2 times

 **Mcelona** 1 year, 3 months ago

Correct

upvoted 1 times

 **IXone** 1 year, 5 months ago

Correct

upvoted 3 times

 **abilioneto** 1 year, 5 months ago

My guess is YNY

upvoted 2 times

 **AdityaGupta** 1 year, 7 months ago

Answer is correct:

YNY

upvoted 1 times

 **GetulioJr** 1 year, 8 months ago

Answer is correct:

YNY

upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

 **bouti** 1 year, 9 months ago

B1: Y

A Conditional Access policy brings signals together, to make decisions, and enforce organizational policies.

upvoted 1 times

 **sensa** 1 year, 11 months ago

appeared on my exam today

upvoted 3 times

Question #37

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Correct Answer:**Answer Area**

Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

 **RamazanInce** Highly Voted 2 years, 5 months ago

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

upvoted 41 times

 **Melwin86** Highly Voted 2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

upvoted 30 times

 **Ramye** Most Recent 3 months ago

Given answer is correct.

Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization.

Source: <https://learn.microsoft.com/en-us/defender-for-identity/what-is>

upvoted 1 times

 **RahulX** 6 months, 4 weeks ago

Microsoft Defender for Identity

upvoted 1 times

 **Drinn** 1 year ago

Keyword is Identity

upvoted 2 times

 **IXone** 1 year, 5 months ago

Correct

upvoted 5 times

 **cormorant** 1 year, 8 months ago

Microsoft Defender for IDENTITY (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to IDENTIFY, detect, and investigate advanced threats, compromised IDENTITIES, and malicious insider actions directed at your organization.

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

upvoted 10 times

 **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 6 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

✉ **jimmysplash** 1 year, 9 months ago

correct actice directory-identity

upvoted 2 times

✉ **tnagy** 1 year, 10 months ago

Wrong Answer. The answer is Microsoft Defender for End Point.

"Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats."

The question is not asking about "Compromised Identities" or threats related to Identities in specific. So the answer is NOT MD for Identity.
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide>

upvoted 5 times

✉ **yaza85** 1 year, 10 months ago

How does MDE leverage onpremise active directory signals??? Furthermore it says identify, detect and investiagte. MDE would als be able to respond. So MDI is the correct answer

upvoted 4 times

✉ **sasasach** 1 year, 5 months ago

wrong. It should be MDI. MDI topic is also on sc200.

upvoted 1 times

✉ **sensa** 1 year, 11 months ago

appeared on my exam today

upvoted 4 times

✉ **Clouddog** 2 years ago

Provided answer is correct:

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization

upvoted 6 times

✉ **Jebli071** 2 years, 4 months ago

Correct answer and refference !

upvoted 3 times

✉ **Jitusrit** 2 years, 4 months ago

Absolutely correct..

upvoted 2 times

✉ **eddie_network_jedi** 2 years, 5 months ago

Correct, "identify" here is the keyword.

upvoted 5 times

✉ **Cryptomike87** 2 years, 2 months ago

No, the keyword is "Active Directory" and the answer is correct.

upvoted 8 times

✉ **P_2311** 2 years, 8 months ago

Correct

upvoted 5 times

Question #38

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Microsoft Defender for Identity can identify advanced threats from

signals.
Azure Active Directory (Azure AD)
Azure AD Connect
on-premises Active Directory Domain Services (AD DS)

Correct Answer:**Answer Area**

Microsoft Defender for Identity can identify advanced threats from

signals.
Azure Active Directory (Azure AD)
Azure AD Connect
on-premises Active Directory Domain Services (AD DS)

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

 **Melwin86** Highly Voted 2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

upvoted 23 times

 **johnegil** Highly Voted 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 11 times

 **user_666** Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 2 times

 **RahulX** 6 months, 4 weeks ago

Microsoft Defender for Identity can identify advanced threats from on-premises active directory domain services.

upvoted 1 times

 **Kelsi999** 11 months ago

Correct

On the exam today

upvoted 2 times

 **Nicochet** 1 year, 1 month ago

Correct

upvoted 4 times

 **mikcs** 1 year, 3 months ago

on exam 12/12/22

upvoted 2 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 2 times

 **smartin2010** 1 year, 6 months ago

correct

upvoted 1 times

 **sensa** 1 year, 11 months ago

appeared on my exam today

upvoted 4 times

 **Tommo** 1 year, 11 months ago

correct

upvoted 1 times

Clouddog 2 years ago

Provided answer is correct:

Defender for Identity protects the AD FS in your environment by detecting on-premises attacks on the AD FS and providing visibility into authentication events generated by the AD FS.

upvoted 5 times

Alessandro_L 2 years, 1 month ago

Correct

upvoted 3 times

Adil251 2 years, 3 months ago

CORRECT

upvoted 5 times

Sachuu97 2 years, 6 months ago

Correct

upvoted 4 times

Nic1234 2 years, 6 months ago

correct

upvoted 4 times

P_2311 2 years, 8 months ago

correct

upvoted 6 times

Question #39

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Active Directory (Azure AD) is

used for authentication and authorization.

- | |
|---|
| an extended detection and response (XDR) system |
| an identity provider |
| a management group |
| a security information and event management (SIEM) system |

Answer Area

Azure Active Directory (Azure AD) is

Correct Answer: used for authentication and authorization.

- | |
|---|
| an extended detection and response (XDR) system |
| an identity provider |
| a management group |
| a security information and event management (SIEM) system |

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide>

 **Mk1331** Highly Voted  2 years, 7 months ago

Correct answer

upvoted 28 times

 **Melwin86** Highly Voted  2 years, 8 months ago

correct

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>

upvoted 20 times

 **RahulX** Most Recent  6 months, 4 weeks ago

Azure AD is an identity provider used for authentication and authorization.

upvoted 1 times

 **Whyiest** 1 year, 2 months ago

It's the right answer

upvoted 3 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 4 times

 **Emmuyah** 1 year, 5 months ago

Correct Answer

upvoted 2 times

 **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected => Identity Provider

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>

upvoted 4 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 2 times

 **andion** 1 year, 7 months ago

An identity provider

upvoted 2 times

✉ **cormorant** 1 year, 8 months ago

Active directory is an identity provider to grant users the access rights according to their assigned roles
upvoted 1 times

✉ **sensa** 1 year, 11 months ago

appeared on my exam today
upvoted 3 times

✉ **Tommo** 1 year, 11 months ago

correct
upvoted 2 times

✉ **Alessandro_L** 2 years, 1 month ago

Correct!
upvoted 2 times

✉ **Jitusrit** 2 years, 4 months ago

AAD IS cloud based identity provider..
upvoted 1 times

✉ **GuruPandian** 2 years, 8 months ago

Correct
upvoted 2 times

✉ **P_2311** 2 years, 8 months ago

correct
upvoted 2 times

Question #40

Topic 1

Which Azure Active Directory (Azure AD) feature can you use to provide just-in-time (JIT) access to manage Azure resources?

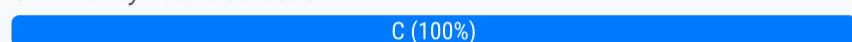
- A. conditional access policies
- B. Azure AD Identity Protection
- C. Azure AD Privileged Identity Management (PIM)
- D. authentication method policies

Correct Answer: C

Azure AD Privileged Identity Management (PIM) provides just-in-time privileged access to Azure AD and Azure resources

Reference:

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

Community vote distribution

 C (100%)

✉  **Matic_Prime**  2 years, 7 months ago

correct

upvoted 21 times

✉  **OlaCharles**  2 years, 6 months ago

I agree. PIM is used for Just In Time and Just Enough Access

upvoted 12 times

✉  **shahmitu**  6 months, 2 weeks ago

Correct!

upvoted 1 times

✉  **RahulX** 6 months, 4 weeks ago

C. Azure AD Privileged Identity Management (PIM)

upvoted 1 times

✉  **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

✉  **manofsteel9** 10 months ago

Selected Answer: C

Correct Answer.

upvoted 1 times

✉  **obaali1990** 1 year, 1 month ago

I wrote today Feb 24, 2023. I had 976/1000. This site is great

upvoted 8 times

✉  **RahulX** 1 year, 1 month ago

PIM is correct ans.

upvoted 1 times

✉  **nobrainataall** 1 year, 1 month ago

Selected Answer: C

that's exactly what PIM does

upvoted 1 times

✉  **Nicochet** 1 year, 1 month ago

PIM correct

upvoted 1 times

✉  **Whyiest** 1 year, 2 months ago

It's the correct answer.

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

upvoted 2 times

✉  **Rahul9802** 1 year, 2 months ago

Correct Answer is PIM

upvoted 2 times

 **jcabello7** 1 year, 3 months ago

PIM is the correct answer

upvoted 1 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 2 times

 **andion** 1 year, 7 months ago

Hi, please how to make difference between PIM and PAM?

upvoted 2 times

 **AdityaGupta** 1 year, 7 months ago

Selected Answer: C

C. Azure AD Privileged Identity Management (PIM)

upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 3 times

Question #41

Topic 1

Which three authentication methods can be used by Azure Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

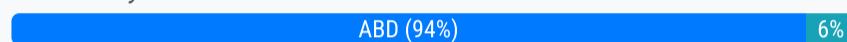
- A. text message (SMS)
- B. Microsoft Authenticator app
- C. email verification
- D. phone call
- E. security question

Correct Answer: ABD

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

Community vote distribution



✉ **Jillis** Highly Voted 2 years, 7 months ago

Correct

upvoted 29 times

✉ **HK010** Highly Voted 1 year, 12 months ago

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 app

Windows Hello for Business

FIDO2 security key

OATH hardware token (preview)

OATH software token

SMS

Voice call

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

upvoted 22 times

✉ **Illaadsf** Most Recent 6 months, 1 week ago

Selected Answer: ABD

correct

upvoted 1 times

✉ **Tahamaffia** 6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 1 times

✉ **RahulX** 6 months, 4 weeks ago

A. text message (SMS)

B. Microsoft Authenticator app

D. phone call

upvoted 1 times

✉ **Crucius** 7 months, 1 week ago

Selected Answer: ABD

Correct.

upvoted 1 times

✉ **User1208** 9 months, 3 weeks ago

I agree the answer can be verified with the Learning materials, but in reality, I do set up my personal email as a component of the MFA for my working email. Is that empowered by other tech?

upvoted 2 times

✉ **studytontight** 10 months ago

This was on the May 2023 exam.

upvoted 1 times

□ **King_Lam** 12 months ago

In Exam 31st March

upvoted 3 times

□ **hululolo** 1 year ago

Appeared in exam on 3rd March

upvoted 3 times

□ **Nicochet** 1 year, 1 month ago

Correct

upvoted 1 times

□ **ehallak** 1 year, 1 month ago

Selected Answer: ABD

Correct. For more details:

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

upvoted 2 times

□ **Whyiest** 1 year, 2 months ago

Azure AD Multi-Factor Authentication supports :

- Microsoft Authenticator app
- Windows Hello for Business
- FIDO2 security key
- OATH hardware token (preview)
- OATH software token
- SMS
- Voice call

upvoted 2 times

□ **2cent2** 1 year, 2 months ago

Selected Answer: ABD

verified via the given links.

upvoted 2 times

□ **Lizzylizzy** 1 year, 3 months ago

Mfa does not include email and security questions

upvoted 2 times

□ **Mcelona** 1 year, 3 months ago

Selected Answer: ABD

A,B,D is the answer

upvoted 3 times

□ **IZone** 1 year, 5 months ago

Correct

upvoted 1 times

Question #42

Topic 1

Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your organization?

- A. sensitivity label policies
- B. Customer Lockbox
- C. information barriers
- D. Privileged Access Management (PAM)

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers>

Community vote distribution

C (100%)

✉️  **Vinny2019**  2 years, 4 months ago

Information Barrier is the correct choice, ignore the typo :-)
upvoted 63 times

✉️  **ThomasDehottay**  2 years, 5 months ago

Correct but better with "Barriers" rather than "Batteries" :D
upvoted 40 times

✉️  **Tahamaffia**  6 months, 2 weeks ago

Got this question on my exam 05/09/2023
upvoted 2 times

✉️  **RahulX** 6 months, 4 weeks ago

Correct ans is A.
You can use sensitivity label policies to restrict communication and the sharing of information between members of two departments at your organization.
upvoted 1 times

✉️  **Crucius** 7 months, 1 week ago

Selected Answer: C

Correct.
upvoted 1 times

✉️  **Itp1120** 9 months, 2 weeks ago

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.
upvoted 2 times

✉️  **Nicochet** 1 year, 1 month ago

Information Barrier
upvoted 3 times

✉️  **Mcelona** 1 year, 3 months ago

Selected Answer: C

C is the answer
upvoted 3 times

✉️  **IXone** 1 year, 5 months ago

Correct : Information Barrier
upvoted 1 times

✉️  **abilioneto** 1 year, 5 months ago

correct
upvoted 1 times

✉️  **Zeus009** 1 year, 6 months ago

Information Barrier is the correct answer
upvoted 1 times

✉️  **88xan** 1 year, 7 months ago

Answer: C Information Barrier
keyword restrict = barrier
upvoted 3 times

✉ **AdityaGupta** 1 year, 7 months ago

Selected Answer: C

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers>

C Information Barriers
upvoted 1 times

✉ **MaryJD** 1 year, 8 months ago

information barriers would be better
upvoted 1 times

✉ **Userer6945** 1 year, 8 months ago

Why is it not PAM?
upvoted 1 times

✉ **PatYeo** 1 year, 2 months ago

I think the answer is not PAMS; reason being PAMS is not a Microsoft 365 feature. Information Barrier is a feature of Microsoft 365.
upvoted 1 times

✉ **ricardo_27_04_1978** 1 year, 3 months ago

I have the same doubt, but if i had to gess, maybe i would say that PAM(access) is related to permissions that users might have accessing apps or resources, not other users. Information barriers, on the other hand, is espicifically about who knows and a way to keep it secure.
upvoted 1 times

✉ **cormorant** 1 year, 8 months ago

INFORMATION BARRIERS are a Microsoft 365 feature which you can use to restrict communication and the sharing of information between members of two departments at your organization
upvoted 2 times

✉ **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022
upvoted 5 times

Question #43

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>
Conditional access policies can be used to block access to an application based on the location of the user.	<input type="radio"/>	<input type="radio"/>
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can be used to block access to an application based on the location of the user.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

 **Jitusrit** Highly Voted 2 years, 4 months ago

Correct..

upvoted 27 times

 **Contactfornitish** Highly Voted 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 12 times

 **RahulX** Most Recent 6 months, 4 weeks ago

NO

YES

NO

upvoted 1 times

 **X98M** 10 months, 1 week ago

It would be nice to have an explanation as to why an answer is correct/incorrect.

upvoted 3 times

 **RahulX** 1 year, 1 month ago

1. No.

2. Yes.

3. Yes (because we can use CA Policy base location, device, IP Add, Azure Registered, Join devices) not only join devices.

upvoted 1 times

 **obaali1990** 1 year, 1 month ago

Read again, Note the word: 'ONLY'

upvoted 9 times

 **Nicochet** 1 year, 1 month ago

Absolutely correct!!

upvoted 2 times

 **JJGsy** 1 year, 1 month ago

The answer to the last question must be "Yes" since it's Azure AD that offers the Conditional Access service in the first place!

upvoted 1 times

 **obaali1990** 1 year, 1 month ago

Read again, Note the word: 'ONLY'

upvoted 2 times

 **Whyiest** 1 year, 2 months ago

NYN Correct

upvoted 1 times

 **Whyiest** 1 year, 2 months ago

Correct

upvoted 1 times

 **Whyiest** 1 year, 2 months ago

Correct

upvoted 2 times

 **IXone** 1 year, 5 months ago

Correct

upvoted 3 times

 **AdityaGupta** 1 year, 7 months ago

NYN is correct

upvoted 3 times

 **MugoKE** 1 year, 8 months ago

Correct

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 5 times

 **clem24** 1 year, 10 months ago

NYN correct

upvoted 1 times

 **bikewun** 2 years ago

CORRECT

upvoted 1 times

 **Alessandro_L** 2 years, 1 month ago

Correct

upvoted 2 times

Question #44

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Conditional access policies can be applied to global administrators.	<input type="radio"/>	<input type="radio"/>
Conditional access policies are evaluated before a user is authenticated.	<input type="radio"/>	<input type="radio"/>
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
Conditional access policies can be applied to global administrators.	<input checked="" type="radio"/>	<input type="radio"/>
Conditional access policies are evaluated before a user is authenticated.	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

Conditional access policies can be applied to all users

Box 2: No -

Conditional access policies are applied after first-factor authentication is completed.

Box 3: Yes -

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

 **Fuji_56** Highly Voted 1 year, 11 months ago

2nd def no, first you are authenticated - then any policies are applied
upvoted 31 times

 **Dhamus** 10 months, 2 weeks ago

You're right, the user must first authenticate for conditional access to be applied to them.
upvoted 2 times

 **M36570** Highly Voted 1 year, 9 months ago

2nd is no, from official exam test preparation
upvoted 11 times

 **user_666** Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)
upvoted 1 times

 **Ramye** 3 months ago

Given answers are correct.

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Source: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/location-condition>
upvoted 1 times

 **RahulX** 6 months, 4 weeks ago

YES

NO

YES

upvoted 1 times

□ **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 2 times

□ **CertAddict69** 9 months, 3 weeks ago

I would say YYY.

For the second one, Yes Conditional Access takes place after first factor authentication, but, a user is not authenticated after first factor authentication. First factor authentication is only part of the authentication process. A user is not fully authenticated until they have completed Conditional Access as well, so Conditional Access takes place BEFORE a user is authenticated as it is part of the authentication process.

upvoted 2 times

□ **manofsteel9** 10 months ago

Correct answer is: YYY

for the 2nd one, Conditional access policies in Azure Active Directory (Azure AD) are evaluated before a user is authenticated. Conditional access allows organizations to enforce additional security requirements and controls based on specific conditions, such as user location, device state, or risk level.

upvoted 2 times

□ **King_Lam** 12 months ago

In Exam 31st March

upvoted 4 times

□ **Nicochet** 1 year, 1 month ago

YNY is correct

upvoted 4 times

□ **Whyiest** 1 year, 2 months ago

YNY Correct

upvoted 3 times

□ **Whyiest** 1 year, 2 months ago

It's no for the 2nd one because Conditional Access starts only after 1st authentication

upvoted 1 times

□ **ricardo_27_04_1978** 1 year, 3 months ago

How is it, that a global administrator could be included in compliance policies? Shouldn't he be in the top of the hierarchy? isn't the one who makes the rules?

upvoted 2 times

□ **OG_Diablo** 1 year, 3 months ago

Global admin accounts are the ones that you need to secure the most. If anything, more conditional access policies should apply to them, not less.

However, it is recommended to set up a break-glass account in case of emergency. Or in case you mess up configuring a conditional access policy and block yourself (and other admins) from reverting it. The emergency account should be excluded from all conditional access policies. But it should therefore be VERY closely monitored and not used for anything else.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access#set-up-emergency-access-accounts>
upvoted 4 times

□ **John316** 1 year, 3 months ago

Those are actually the accounts with more stringent compliance policies because of their admin privileges.

upvoted 3 times

□ **IXone** 1 year, 5 months ago

Correct

upvoted 5 times

□ **abilioneto** 1 year, 5 months ago

correct

upvoted 3 times

□ **88xan** 1 year, 7 months ago

Answers: YNY

Conditional Access policies are enforced AFTER first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

upvoted 3 times

□ **AdityaGupta** 1 year, 7 months ago

YNY is correct

Box 1: Yes -

Conditional access policies can be applied to all users

Box 2: No -

Conditional access policies are applied after first-factor authentication is completed.

Box 3: Yes -

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

upvoted 3 times

Question #45

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

guest account.
managed identity.
service principal.
user account.

Correct Answer:**Answer Area**

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

guest account.
managed identity.
service principal.
user account.

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>✉  thiaybovo  2 years, 3 months ago

CORRECT

upvoted 22 times

✉  Clouddog  2 years ago

Provided answer is correct:

A service principal is created in each tenant where the application is used and references the globally unique app object. The service principal object defines what the app can actually do in the specific tenant, who can access the app, and what resources the app can access.

upvoted 19 times

✉  lukecage5  6 months, 1 week ago

Correct answer is Service Principal.

A service principal is created in each tenant where the application is used and references the globally unique app object. The service principal object defines what the app can actually do in the specific tenant, who can access the app, and what resources the app can access.

upvoted 1 times

✉  RahulX 6 months, 4 weeks ago

Correct Ans.

Service Principal

upvoted 1 times

✉  Kelsi999 11 months ago

Correct

I had this question on the exam

upvoted 2 times

✉  Whyest 1 year, 2 months ago

The answer is correct. Here is more informations if you need :

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

A service principal is a security identity used to represent an application in Azure Active Directory (AAD). It is used to authenticate the application to access resources, and also to assign permissions to those resources.

A service principal is like a user identity (login and password or certificate) for an application.

An application object, on the other hand, is a representation of an application in Azure Active Directory. It contains information about the application, such as its name and URL, as well as its associated service principal.

In summary, a service principal is a security identity used to authenticate an application, while an application object is a representation of the application in Azure Active Directory that contains information about the application and its associated service principal.

upvoted 11 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 3 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 2 times

 **Zeus009** 1 year, 6 months ago

Agreed

upvoted 1 times

 **cormorant** 1 year, 8 months ago

key words for service principle - applications registered

upvoted 3 times

 **Cactus88** 1 year, 9 months ago

Correct

upvoted 1 times

 **rapunzellin** 1 year, 11 months ago

Correct

upvoted 1 times

 **DemekeA** 2 years, 1 month ago

Service Principal

upvoted 4 times

 **Contactfornitish** 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 6 times

 **Ummar26** 2 years, 1 month ago

correct

upvoted 6 times

 **evanow** 2 years, 4 months ago

Correct

upvoted 4 times

Question #46

Topic 1

Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. fingerprint
- B. facial recognition
- C. PIN
- D. email verification
- E. security question

Correct Answer: ABC

Reference:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication>

Community vote distribution

ABC (100%)

✉  **JayHall**  2 years, 5 months ago

correct

Windows Hello in Windows 10 enables users to sign in to their device using a PIN. <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password>

Windows Hello lets your employees use fingerprint or facial recognition as an alternative method to unlocking a device. With Windows Hello, authentication happens when the employee provides his or her unique biometric identifier while accessing the device-specific Windows Hello credentials.

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise>

upvoted 34 times

✉  **Yelad**  1 year, 8 months ago

On the exam 10/07/2022

upvoted 6 times

✉  **RahulX**  6 months, 4 weeks ago

- A. fingerprint
- B. facial recognition
- C. PIN

upvoted 1 times

✉  **joshsz** 7 months, 2 weeks ago

Selected Answer: ABC

Correct

upvoted 1 times

✉  **Molota** 9 months, 3 weeks ago

Selected Answer: ABC

like when logging on the computer ... ABC

upvoted 1 times

✉  **Nicochet** 1 year, 1 month ago

ABC. Correct.

upvoted 3 times

✉  **Whyest** 1 year, 2 months ago

Windows Hello for Business MFA:

- Fingerprint
- Facial recognition
- PIN

upvoted 3 times

✉  **Whyest** 1 year, 2 months ago

Selected Answer: ABC

Correct

upvoted 1 times

✉  **2cent2** 1 year, 2 months ago

Selected Answer: ABC

.....

upvoted 2 times

✉ **Andreeew883** 1 year, 3 months ago

Valid answer is A,b,c

upvoted 2 times

✉ **smartin2010** 1 year, 6 months ago

Correct

upvoted 1 times

✉ **Zeus009** 1 year, 6 months ago

Aligned

upvoted 1 times

✉ **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 3 times

✉ **taky** 1 year, 9 months ago

Selected Answer: ABC

Correct, biometric and number password are supported. Email requires internet connection on the device and security questions are used to recover access account.

upvoted 3 times

✉ **PravinDhote** 1 year, 11 months ago

Selected Answer: ABC

Correct

upvoted 1 times

✉ **Eric02** 1 year, 11 months ago

Selected Answer: ABC

Correct

upvoted 2 times

✉ **bikewun** 2 years ago

CORRECT

upvoted 2 times

Question #47

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

When you enable security defaults in Azure Active Directory (Azure AD),

- | |
|---|
| Azure AD Identity Protection |
| Azure AD Privileged Identity Management (PIM) |
| multi-factor authentication (MFA) |

will be enabled for all Azure AD users.

Answer Area

When you enable security defaults in Azure Active Directory (Azure AD),

Correct Answer:

- | |
|---|
| Azure AD Identity Protection |
| Azure AD Privileged Identity Management (PIM) |
| multi-factor authentication (MFA) |

will be enabled for all Azure AD users.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

✉️  **Cereb7** Highly Voted 2 years, 3 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

Security defaults make it easier to help protect your organization from these attacks with preconfigured security settings:

- Requiring all users to register for Azure AD Multi-Factor Authentication.
 - Requiring administrators to do multi-factor authentication.
 - Blocking legacy authentication protocols.
 - Requiring users to do multi-factor authentication when necessary.
 - Protecting privileged activities like access to the Azure portal.
- upvoted 37 times

✉️  **sensa** Highly Voted 1 year, 11 months ago

appeared on my exam today

upvoted 8 times

✉️  **RahulX** Most Recent 6 months, 4 weeks ago

Correct Ans.

When Security Default is enabled in Azure AD Portal MFA is automatically enabled tenant wide but user can avoid the MFA for 14 grace period.

upvoted 1 times

✉️  **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected => MFA

upvoted 8 times

✉️  **cantbeme** 1 year, 7 months ago

on exam today

upvoted 3 times

✉️  **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 4 times

✉️  **Lazylinux** 1 year, 8 months ago

MFA for sure

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

upvoted 5 times

□ **Lawiwi** 1 year, 9 months ago

correct

upvoted 1 times

□ **jacqs101** 1 year, 11 months ago

Technically the answers on this question are all wrong.

upvoted 3 times

□ **[Removed]** 2 years ago

MFA will be triggered but they are not automatically enabled

upvoted 4 times

□ **Lazylinux** 1 year, 8 months ago

It is in way Enabled bu forcing you to register for it and you have 14 days grace period if NOT activated in 14 days access will be denied until the MFA registration process is completed and hence indirectly enabled!! Enabled may NOT be best word for it, i prefer activated

upvoted 3 times

□ **bikewun** 2 years ago

CORRECT

upvoted 1 times

□ **DemekeA** 2 years, 1 month ago

MFA is answer

upvoted 2 times

□ **Contactfornitish** 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 3 times

□ **yulexam** 2 years, 4 months ago

correct...

to change the "security default" : AAD>properties>manage security defaults

upvoted 4 times

□ **[Removed]** 2 years, 4 months ago

Correct!

upvoted 2 times

Question #48

Topic 1

You have an Azure subscription.

You need to implement approval-based, time-bound role activation.

What should you use?

- A. Windows Hello for Business
- B. Azure Active Directory (Azure AD) Identity Protection
- C. access reviews in Azure Active Directory (Azure AD)
- D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Correct Answer: D

Reference:

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

Community vote distribution

D (100%)

 **Whyiest** Highly Voted 1 year, 2 months ago

Note for your exam :
When you see the key word "time" linked to an access or an authentication, assume that there is high chance that it's PIM.
upvoted 35 times

 **k_jay** Highly Voted 1 year, 11 months ago

Correct answer!
upvoted 11 times

 **RahulX** Most Recent 6 months, 4 weeks ago

Correct.
D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
upvoted 1 times

 **Molota** 9 months, 3 weeks ago

Selected Answer: D
Answer is PIM
upvoted 1 times

 **Nicochet** 1 year, 1 month ago

PIM is the option.
upvoted 3 times

 **Whyiest** 1 year, 2 months ago

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

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is designed specifically for implementing approval-based, time-bound role activation in an Azure subscription. PIM allows you to manage and control access to privileged roles in Azure AD, Azure resources, and Azure AD-integrated SaaS apps. It enables you to elevate access on a just-in-time basis and provides an approval workflow for role activation, which can be restricted to specific time periods. This makes it an ideal choice for implementing the requirements specified in the question.

upvoted 3 times

 **2cent2** 1 year, 2 months ago

Selected Answer: D
d is correct
upvoted 2 times

 **PikaDeUrso** 1 year, 3 months ago

Selected Answer: D
Correct!
upvoted 3 times

 **FBrabble** 1 year, 4 months ago

PIM for sure D
upvoted 1 times

 **IXone** 1 year, 5 months ago

Correct

upvoted 1 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 1 times

 **smartin2010** 1 year, 6 months ago

D correct

upvoted 1 times

 **Benjam** 1 year, 6 months ago

Selected Answer: D

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

upvoted 3 times

 **Zeus009** 1 year, 6 months ago

Agreed

upvoted 1 times

 **dino23** 1 year, 7 months ago

Correct answer!

upvoted 1 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 1 times

 **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 2 times

Question #49

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Global administrators are exempt from conditional access policies	<input type="radio"/>	<input type="radio"/>
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	<input type="radio"/>	<input type="radio"/>
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Global administrators are exempt from conditional access policies	<input type="radio"/>	<input checked="" type="radio"/>
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	<input type="radio"/>	<input checked="" type="radio"/>
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa>

✉ **FBrabble** Highly Voted 1 year, 4 months ago

N N Y correct

upvoted 11 times

✉ **IZone** Highly Voted 1 year, 5 months ago

Correct

upvoted 5 times

✉ **RahulX** Most Recent 6 months, 4 weeks ago

NO

NO

YES

upvoted 1 times

✉ **RahulX** 6 months, 4 weeks ago

You can create a conditional access policy targeted to all users including Global Admin.

upvoted 1 times

✉ **Kelsi999** 11 months ago

On the exam today. Answers are correct

upvoted 3 times

✉ **Daniel_Angelo** 11 months, 1 week ago

NNY:

2°:Use Conditional Access policies to apply the right access controls when needed to keep your organization secure.
can not add users to azure ad roles.

upvoted 1 times

 **King_Lam** 12 months ago

In Exam 31st March

upvoted 4 times

 **hululolo** 1 year ago

Appeared in exam on 3rd March

upvoted 3 times

 **Nicochet** 1 year, 1 month ago

NNI Totally correct

upvoted 1 times

 **Whyiest** 1 year, 2 months ago

NNY I agree with others it's correct

upvoted 4 times

 **abilioneto** 1 year, 5 months ago

correct

upvoted 4 times

 **Zeus009** 1 year, 6 months ago

Aligned

upvoted 4 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 5 times

 **misterperson** 1 year, 10 months ago

correct

upvoted 2 times

 **GPerez73** 1 year, 11 months ago

Correct

upvoted 3 times

 **[Removed]** 1 year, 11 months ago

No No Yes - correct

upvoted 2 times

Question #50

Topic 1

When security defaults are enabled for an Azure Active Directory (Azure AD) tenant, which two requirements are enforced? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. All users must authenticate from a registered device.
- B. Administrators must always use Azure Multi-Factor Authentication (MFA).
- C. Azure Multi-Factor Authentication (MFA) registration is required for all users.
- D. All users must authenticate by using passwordless sign-in.
- E. All users must authenticate by using Windows Hello.

Correct Answer: BC

Security defaults make it easy to protect your organization with the following preconfigured security settings:

- Requiring all users to register for Azure AD Multi-Factor Authentication.
- Requiring administrators to do multi-factor authentication.
- Blocking legacy authentication protocols.
- Requiring users to do multi-factor authentication when necessary.
- Protecting privileged activities like access to the Azure portal.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

Community vote distribution

BC (100%)

 [Removed]  1 year, 11 months ago

Selected Answer: BC

Correct

upvoted 13 times

 JJGsy  1 year, 1 month ago

Misleading question, as if all users require MFA, there's no separate requirement to also require this for admins!

upvoted 10 times

 dawnbringer69 10 months ago

This is wrong. The Users are Required to REGISTER to MFA not use it continuously.

The difference is that Admin will be forced to use MFA ALL THE TIME.

Hence the discrimination.

upvoted 1 times

 dawnbringer69 10 months ago

The Answer Is Correct.

upvoted 1 times

 RahulX  6 months, 4 weeks ago

Correct

B. Administrators must always use Azure Multi-Factor Authentication (MFA)

C. Azure Multi-Factor Authentication (MFA) registration is required for all users

upvoted 1 times

 studytonight 10 months ago

A question that was very similar to this was on the May 2023 exam.

upvoted 1 times

 Whyiest 1 year, 2 months ago

Selected Answer: BC

Correct

upvoted 2 times

 IXOne 1 year, 5 months ago

Correct

upvoted 4 times

abilioneto 1 year, 5 months ago

correct

upvoted 3 times

Zeus009 1 year, 6 months ago

B and C are joined at the hip

upvoted 4 times

Armanas 1 year, 6 months ago

Selected Answer: BC

This Question appeared in Exam today (02 September 2022)

I selected => B, C

upvoted 4 times

cantbeme 1 year, 7 months ago

on exam today

upvoted 3 times

AbhilAM 1 year, 8 months ago

In exam today

upvoted 1 times

Mahaendhiran 1 year, 9 months ago

Selected Answer: BC

Correct

upvoted 1 times

misterperson 1 year, 10 months ago

correct

upvoted 1 times

Siphe 1 year, 10 months ago

Correct

upvoted 1 times

sensa 1 year, 11 months ago

appeared on my exam today

upvoted 3 times

Question #51

Topic 1

Which type of identity is created when you register an application with Active Directory (Azure AD)?

- A. a user account
- B. a user-assigned managed identity
- C. a system-assigned managed identity
- D. a service principal

Correct Answer: D

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

Community vote distribution

D (100%)

✉  **RahulX** 6 months, 4 weeks ago

D. a service principal

upvoted 1 times

✉  **zellck** 11 months ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals#service-principal-object>

Application - The type of service principal is the local representation, or application instance, of a global application object in a single tenant or directory. In this case, a service principal is a concrete instance created from the application object and inherits certain properties from that application object. A service principal is created in each tenant where the application is used and references the globally unique app object. The service principal object defines what the app can actually do in the specific tenant, who can access the app, and what resources the app can access.

upvoted 1 times

✉  **Kelsi999** 11 months ago

On the exam today. Correct answer

upvoted 1 times

✉  **Nicochet** 1 year, 1 month ago

a Service Principal

upvoted 3 times

✉  **o_seun** 1 year, 3 months ago

Correct

service Principal is correct

upvoted 2 times

✉  **ITOPS** 1 year, 3 months ago

Selected Answer: D

Correct

upvoted 2 times

✉  **FBrabble** 1 year, 4 months ago

Yes the answer is D service principal

upvoted 2 times

✉  **Ola189** 1 year, 4 months ago

Selected Answer: D

CORRECT

upvoted 3 times

✉  **IXone** 1 year, 5 months ago

Correct

upvoted 2 times

✉  **abilioneto** 1 year, 5 months ago

correct

upvoted 1 times

 **Mahaendhiran** 1 year, 9 months ago

Selected Answer: D

Correct

upvoted 2 times

 **misterperson** 1 year, 10 months ago

correct

upvoted 2 times

 **Siphe** 1 year, 10 months ago

D - correct answer.

upvoted 1 times

 **GPerez73** 1 year, 11 months ago

Correct

upvoted 3 times

Question #52

Topic 1

Which three tasks can be performed by using Azure Active Directory (Azure AD) Identity Protection? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Configure external access for partner organizations.
- B. Export risk detection to third-party utilities.
- C. Automate the detection and remediation of identity based-risks.
- D. Investigate risks that relate to user authentication.
- E. Create and automatically assign sensitivity labels to data.

Correct Answer: CDE

Community vote distribution

BCD (100%)

 **KoosDuppen**  1 year, 11 months ago

Directly from the SC-900 Fundamentals training slides:

Azure Identity Protection

Enables organizations to accomplish three key tasks:

- Automate the detection and remediation of identity based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third party utilities for further analysis.

upvoted 80 times

 **Roux** 1 year, 10 months ago

please share the slides

upvoted 3 times

 **Suresh13** 1 year, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

upvoted 6 times

 **vskordas** 1 year, 6 months ago

EXPORT RDD TO OTHER TOOLS NOT ORGANIZATIONS

upvoted 1 times

 **Kuliet** 1 year, 6 months ago

"other TOOLS" = "3rd party UTILITIES", same thing, different words mate.

upvoted 7 times

 **JMROFLLOL**  1 year, 11 months ago

Selected Answer: BCD

As other have said, sensitivity labels have nothing to do with it.

upvoted 31 times

 **obaali1990** 1 year, 1 month ago

Exactly

upvoted 2 times

 **Ozzie**  2 months, 4 weeks ago

It is CDE:

Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks. These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation.

The tools that are written down here are available from Microsoft, so not third parties.

Ref:<https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection>

upvoted 1 times

 **Akacokie** 5 months ago

Selected Answer: BCD

B. Export risk detection to third-party utilities. Most Voted

C. Automate the detection and remediation of identity based-risks. Most Voted

D. Investigate risks that relate to user authentication. Most Voted
upvoted 2 times

 **Tomix** 6 months, 3 weeks ago

Selected Answer: BCD

upvoted 2 times

 **RahulX** 6 months, 4 weeks ago

Correct Ans are

- B. Export risk detection to third-party utilities.
- C. Automate the detection and remediation of identity based-risks.
- D. Investigate risks that relate to user authentication.

upvoted 2 times

 **Darkfire** 8 months ago

Selected Answer: BCD

Answer should be BCD

upvoted 2 times

 **manofsteel9** 10 months ago

Selected Answer: BCD

correct answer is BCD.

I verified with the provided link from the guys here.

upvoted 1 times

 **bjobare** 10 months ago

Selected Answer: BCD

Automate the detection and remediation of identity-based risks.

Investigate risks using data in the portal.

Export risk detection data to other tools.

upvoted 1 times

 **MarcioTB** 10 months, 2 weeks ago

Selected Answer: BCD

correct

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: BCD

BCD is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

Identity Protection allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to other tools.

upvoted 1 times

 **Distinctive** 11 months, 1 week ago

Selected Answer: BCD

THE answers are here

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

upvoted 1 times

 **bahik999** 11 months, 1 week ago

its CDE:

- C. Automate the detection and remediation of identity-based risks.
 - D. Investigate risks that relate to user authentication.
 - E. Create and automatically assign sensitivity labels to data.
- A. Azure AD Identity Protection is not used to configure external access for partner organizations. This task is typically performed using Azure AD B2B collaboration.
- B. Azure AD Identity Protection does not export risk detection to third-party utilities. It provides built-in reports and notifications for risk detections.
- C. Azure AD Identity Protection can automate the detection and remediation of identity-based risks by using its machine learning algorithms to detect risky sign-ins and user behavior. It can also take remedial actions such as blocking access or requiring additional authentication.
- D. Azure AD Identity Protection allows investigating risks that relate to user authentication. It provides detailed reports and recommendations for remediation.
- E. Azure AD Identity Protection does not create and automatically assign sensitivity labels to data. This task is typically performed using Azure Information Protection.

upvoted 1 times

 **Mehe323** 8 months, 1 week ago

So it is NOT E (note the NOT in below sentence) it s. It should be BCD, that is also confirmed in the Security, Compliance and Identity fundamentals Learning path.

E. Azure AD Identity Protection does not create and automatically assign sensitivity labels to data. This task is typically performed using Azure Information Protection

upvoted 1 times

 **nobrainatall** 1 year, 1 month ago

Selected Answer: BCD

E is compliance and has nothing to do with Azure Identity Protection

upvoted 2 times

 **Nicochet** 1 year, 1 month ago

Is BCD. E is incorrect.

upvoted 2 times

 **Whyiest** 1 year, 2 months ago

100% sure that is BCD

upvoted 2 times

 **ok22** 1 year, 2 months ago

Selected Answer: BCD

BCD is definitely correct.

upvoted 1 times

Question #53

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

When using multi-factor authentication (MFA), a password is considered something you

are
have
know
share

Correct Answer:**Answer Area**

When using multi-factor authentication (MFA), a password is considered something you

are
have
know
share

Box 1: know -

Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

Reference:

<https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA>

 **Whyiest** Highly Voted  1 year, 2 months ago

Password = know
 Device / code / key = have
 Biometric = you are
 upvoted 27 times

 **Tahamaffia** Most Recent  6 months, 2 weeks ago

Got this question on my exam 05/09/2023
 upvoted 2 times

 **RahulX** 6 months, 4 weeks ago

Password = something you know
 Code = something you have
 Biometric = something you are.
 upvoted 2 times

 **bigelmo_elmo** 8 months, 4 weeks ago

If you don't know this... you shouldn't be taking the exam
 upvoted 2 times

 **hululolo** 1 year ago

Appeared in exam on 3rd March
 upvoted 4 times

 **walkaway** 1 year, 3 months ago

Have is for device. Know is for password.
 upvoted 4 times

 **PoopyPants** 1 year, 3 months ago

Perhaps an MFA token could be considered something you have. However MFA tokens dont contain words. Question states a PassWORD. Lousy question.
 upvoted 2 times

 **Cegep** 1 year, 5 months ago

The question states a password.
 That's something you know.
 upvoted 3 times

 **vskordas** 1 year, 6 months ago

The doc you provide is Know (password), hav (token- mobile), are (fingerprint) so, all of these must be considered as correct, not only A
upvoted 3 times

 **RodrigoAB** 1 year, 6 months ago

Something You Know, Have, or Are

Something you ---->know<---- (eg. a password). This is the most common kind of authentication used for humans.

upvoted 4 times

Question #54

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	<input type="radio"/>	<input type="radio"/>
Windows Hello for Business can use a PIN code as an authentication method.	<input type="radio"/>	<input type="radio"/>
Windows Hello for Business authentication information syncs across all the devices registered by a user.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	<input type="radio"/>	<input checked="" type="radio"/>
Windows Hello for Business can use a PIN code as an authentication method.	<input checked="" type="radio"/>	<input type="radio"/>
Windows Hello for Business authentication information syncs across all the devices registered by a user.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

The Microsoft Authenticator app helps you sign in to your accounts when you're using two-factor verification. Two-factor verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised. Two-factor verification uses a second factor like your phone to make it harder for other people to break in to your account.

Box 2: Yes -

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Box 3: No -

Windows Hello credentials are based on certificate or asymmetrical key pair. Windows Hello credentials can be bound to the device, and the token that is obtained using the credential is also bound to the device.

Reference:

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

 **Anand_Parappurath**  1 year, 5 months ago

I think Windows hello is single factor authentication and MS Authenticator is used a MFA agent or device or tool. for me the ans is N,Y,N
upvoted 6 times

 **OG_Diablo** 1 year, 3 months ago

Windows Hello for Business actually counts as multi-factor authentication. Because it is something you have (the physical computer) and either something you know (PIN) or something you are (biometrics).

You cannot use the MS Authenticator for Windows Hello for Business, as that is something you have on a different device. WHfB is strictly local on the Windows computer.

That doesn't change the correct answers, though. They remain N, Y, N.

upvoted 7 times

 **Ola189**  1 year, 4 months ago

From <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>:

'In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a

new type of user credential that is tied to a device and uses a biometric or PIN.'

Answer is correct. (NYN)

upvoted 5 times

 **user_666** Most Recent 1 month, 3 weeks ago

had this question on my exam today (01 feb 2024)

upvoted 1 times

 **Tomix** 6 months, 3 weeks ago

Yes

Yes

No

upvoted 2 times

 **RahulX** 6 months, 4 weeks ago

No

Yes

No

upvoted 1 times

 **Mehe323** 8 months, 1 week ago

The explanation of the first statement is not very clear. You use the app for accounts that have their credentials stored in the cloud. Windows Hello is tied to the device, the account details to login are stored on the device. You can't use the MA app for such a device.

upvoted 2 times

 **Molota** 9 months, 3 weeks ago

agreed with the given answer

upvoted 1 times

 **StressFree** 12 months ago

e o pior q é verdade....

upvoted 1 times

 **smurferinoatexcel** 1 year ago

Correct.

1) MS authenticator app is not a part of Windows Hello

2) PIN is considered "something you know"

3) Windows Hello stores authentication information only on the local device

upvoted 2 times

 **Neeraj1978** 1 year, 1 month ago

N,Y,N Windows Hello is a more personal, more secure way to get instant access to your Windows 10 devices using a PIN, facial recognition, or fingerprint. You'll need to set up a PIN as part of setting up fingerprint or facial recognition sign-in, but you can also sign in with just your PIN.

upvoted 1 times

 **Nicochet** 1 year, 1 month ago

No Yes No

upvoted 1 times

 **Whyest** 1 year, 2 months ago

Windows Hello for Business MFA:

- Fingerprint
- Facial recognition
- PIN

upvoted 2 times

 **FBrabble** 1 year, 4 months ago

tricky question but N Y N looks correct as WH4B is a different topic than MFA in this case

upvoted 2 times

 **SiDoCiOuS** 1 year, 5 months ago

On the exam 10/18/2022.

upvoted 3 times

 **656823** 1 year, 6 months ago

This should be YYN, right?

upvoted 2 times

 **vskordas** 1 year, 6 months ago

..Then why when I have to login to my bank I use MS Authenticator app at my mobile?

..I think MS Authenticator is MFA option.

upvoted 2 times

 **Mehe323** 8 months ago

The bank is not a Microsoft service, they are referring to login into Microsoft accounts and devices that are included in Windows Hello for Business. Windows HfB has two main authentication options for device and Microsoft account login: something you have (the device) and

something you are (biometric) OR something you know (PIN).
<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/>
upvoted 1 times

 **Zeus009** 1 year, 6 months ago
Agreed
upvoted 1 times

Question #55

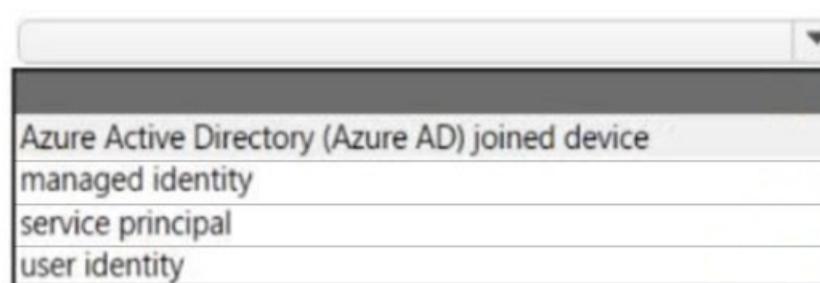
Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

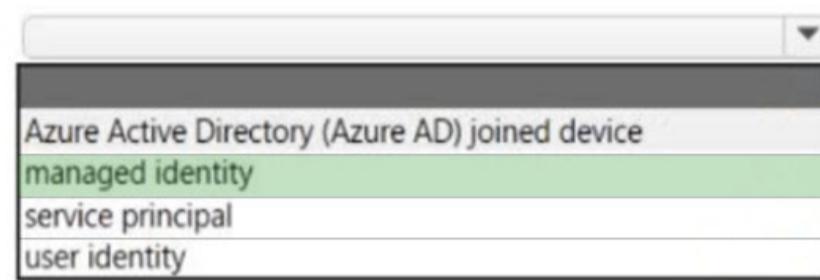
An Azure resource can use a system-assigned



to access Azure services.

Correct Answer:

An Azure resource can use a system-assigned



to access Azure services.

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

Here are some of the benefits of using managed identities:

You don't need to manage credentials. Credentials aren't even accessible to you.

You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

IXOne Highly Voted 1 year, 5 months ago

Correct

upvoted 8 times

RahulX Most Recent 6 months, 4 weeks ago

"managed identity" is the correct answer.

upvoted 1 times

zelick 11 months ago

"managed identity" is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#managed-identity-types>
System-assigned. Some Azure resources, such as virtual machines allow you to enable a managed identity directly on the resource. When you enable a system-assigned managed identity:

- A service principal of a special type is created in Azure AD for the identity. The service principal is tied to the lifecycle of that Azure resource. When the Azure resource is deleted, Azure automatically deletes the service principal for you.
- By design, only that Azure resource can use this identity to request tokens from Azure AD.
- You authorize the managed identity to have access to one or more services.
- The name of the system-assigned service principal is always the same as the name of the Azure resource it is created for. For a deployment slot, the name of its system-assigned identity is <app-name>/slots/<slot-name>.

upvoted 2 times

TATTIF 11 months, 2 weeks ago

managed identity is correct

upvoted 2 times

FBrabble 1 year, 4 months ago

managed identity = correct answer

upvoted 4 times

abilioneto 1 year, 5 months ago

correct

upvoted 2 times

Emmuyah 1 year, 5 months ago

Correct Answer

upvoted 3 times

>User_Mowgli 1 year, 6 months ago

Managed Identity
upvoted 4 times

Question #56

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use

classifications
incidents
policies
Secure score

in the Microsoft 365 Defender portal to identify devices that are affected by an alert.

Correct Answer:

Answer Area

You can use

classifications
incidents
policies
Secure score

in the Microsoft 365 Defender portal to identify devices that are affected by an alert.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide>

User_Mowgli Highly Voted 1 year, 6 months ago

Incident:alert
upvoted 7 times

Yindave Highly Voted 1 year, 5 months ago

its a bit of a strange sentence, but yeah, Incident's the correct awnser
upvoted 5 times

Daniel_Angelo Most Recent 11 months, 1 week ago

Yes, Incident - Alert:
Microsoft 365 Defender automatically aggregates the alerts and their associated information into an incident.
upvoted 3 times

Nicochet 1 year, 1 month ago

Incidents
upvoted 3 times

FBrabble 1 year, 4 months ago

yes Incident since it is a thing that happened triggering an alert
upvoted 4 times

IXone 1 year, 5 months ago

Correct
upvoted 3 times

Zeus009 1 year, 6 months ago

Correct
upvoted 3 times

Question #57

Topic 1

What are two capabilities of Microsoft Defender for Endpoint? Each correct selection presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. automated investigation and remediation
- B. transport encryption
- C. shadow IT detection
- D. attack surface reduction

Correct Answer: AD

Reference:

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

Community vote distribution

AD (100%)

✉ **An_is_here** Highly Voted 2 years, 8 months ago

Answers are CORRECT

Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale. While The attack surface reduction set of capabilities provides the first line of defence in the stack.

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide#microsoft-defender-for-endpoint>

upvoted 35 times

✉ **sensa** Highly Voted 1 year, 11 months ago

appeared on my exam today

upvoted 13 times

✉ **RahulX** Most Recent 6 months, 4 weeks ago

- A. automated investigation and remediation
- D. attack surface reduction

upvoted 1 times

✉ **Darkfire** 8 months ago

Selected Answer: AD

Answers are correct

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

upvoted 1 times

✉ **manofsteel9** 10 months ago

Selected Answer: AD

Correct!

By excluding non-related statements.

upvoted 1 times

✉ **Charly0710** 1 year, 2 months ago

AD

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide>

upvoted 2 times

✉ **yonie** 1 year, 3 months ago

Selected Answer: AD

Voted AD

upvoted 3 times

✉ **IZone** 1 year, 5 months ago

A D CORRECT

upvoted 2 times

✉ **abilioneto** 1 year, 5 months ago

correct

upvoted 2 times

✉ **Siphe** 1 year, 10 months ago

Voted A,D
upvoted 3 times

 **Eric02** 1 year, 11 months ago

Selected Answer: AD

Voted AD
upvoted 3 times

 **Chief** 2 years ago

<https://docs.microsoft.com/en-us/learn/modules/describe-threat-protection-with-microsoft-365-defender/5-describe-defender-endpoint>
upvoted 2 times

 **Baba65Baba** 2 years, 1 month ago

Selected Answer: AD

AD is correct
upvoted 7 times

 **sounakroy** 2 years, 1 month ago

Selected Answer: AD

CORRECT
upvoted 2 times

Question #58

Topic 1

DRAG DROP -

Match the Azure networking service to the appropriate description.

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

NOTE: Each correct match is worth one point.

Select and Place:

Services	Answer Area	
Azure Bastion	Service	Provides Network Address Translation (NAT) services
Azure Firewall	Service	Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Service	Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Correct Answer:

Services	Answer Area	
Azure Bastion	Azure Firewall	Provides Network Address Translation (NAT) services
Azure Firewall	Azure Bastion	Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Network security group (NSG)	Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Box 1: Azure Firewall -

Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.

Box 2: Azure Bastion -

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

Box 3: Network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network.

Reference:

<https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview> <https://docs.microsoft.com/en-us/azure/bastion/bastion-overview> <https://docs.microsoft.com/en-us/azure/firewall/features> <https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

 **Chris2pher** Highly Voted 1 year, 4 months ago

That is correct. Only azure firewall can translate SNAT/DNAT while NSG cannot. But it can filter traffic.

Firewall

Bastion

NSG

upvoted 9 times

 **sensa** Highly Voted 1 year, 11 months ago

appeared on my exam today

upvoted 6 times

 **RahulX** Most Recent 6 months, 4 weeks ago

Correct

Azure Firewall

Bastion

NSG

upvoted 1 times

 **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

 **bigelmo_elmo** 9 months ago

Guys its a trick question don't get confused , the given answers are correct

upvoted 1 times

manofsteel9 10 months ago

answer is correct: Firewall, Bastion, NSG
upvoted 1 times

churkin6 1 year ago

Firewall
Bastion
NSG
upvoted 1 times

manidaredevil 1 year, 1 month ago

it should be NSG
Bastion
Firewall

Because NAT has nothing to do with Firewall.

upvoted 3 times

dinodinobr 1 year, 5 months ago

NSG
Bastion
Firewall
upvoted 2 times

walkaway 1 year, 3 months ago

NSG doesn't provide NAT capabilities bro. This is what Azure Firewall does.

NSG can be applied to NIC or subnet.

The answer is Azure Firewall, Azure Bastion and NSG.

upvoted 2 times

SUBRRA01 1 year, 4 months ago

But the answer says
Firewall
Bastion
NSG

Which is correct?

upvoted 1 times

allwn 1 year, 4 months ago

1st option is very unclear to me
2. Bastion
3. NSG
upvoted 1 times

IZone 1 year, 5 months ago

CORRECT

upvoted 3 times

SiDoCiOuS 1 year, 5 months ago

On the exam 10/18/2022.
upvoted 2 times

Yelad 1 year, 8 months ago

On the exam 10/07/2022
upvoted 3 times

[Removed] 1 year, 11 months ago

Correct
upvoted 5 times

Question #59

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Advisor
Azure Bastion
Azure Monitor
Azure Sentinel

is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Correct Answer:**Answer Area**

Azure Advisor
Azure Bastion
Azure Monitor
Azure Sentinel

is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Reference:

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

 **An_is_here** Highly Voted  2 years, 8 months ago

Answer is CORRECT

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

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

upvoted 29 times

 **sokolsulejmani** Highly Voted  2 years ago

Answer is correct, keep in mind that name has changed to "Microsoft Sentinel"

upvoted 6 times

 **RahulX** Most Recent  6 months, 4 weeks ago

Microsoft Azure Sentinel is Correct Ans.

upvoted 1 times

 **Darkfire** 8 months ago

Answer is correct

Keywords are SIEM / SOAR = Sentinel

upvoted 1 times

 **studyonight** 10 months ago

This was on the May 2023 exam.

upvoted 1 times

 **zellck** 11 months ago

"Azure Sentinel" is the answer.

<https://learn.microsoft.com/en-us/azure/sentinel/overview>

Microsoft Sentinel is a scalable, cloud-native solution that provides:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)

upvoted 2 times

 **MoneyStacking** 1 year, 2 months ago

Microsoft Siemtinel !!

upvoted 1 times

 **Lizzylizzy** 1 year, 3 months ago

Azure sentinel

upvoted 4 times

 **IXone** 1 year, 5 months ago

Microsoft Azure Sentinel CORRECT
upvoted 2 times

□ **abilioneto** 1 year, 5 months ago

correct

upvoted 2 times

□ **Zeus009** 1 year, 6 months ago

Correct

upvoted 1 times

□ **cantbeme** 1 year, 7 months ago

on exam today

upvoted 3 times

□ **jimmysplash** 1 year, 9 months ago

keyword- siem

upvoted 2 times

□ **itelessons** 1 year, 10 months ago

SIEMtinel...

upvoted 4 times

□ **misterperson** 1 year, 10 months ago

correct

upvoted 1 times

□ **Okeythaone** 1 year, 11 months ago

yeah that's the correct answer

upvoted 1 times

□ **Raze** 1 year, 11 months ago

ans is correct

upvoted 1 times

Question #60

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	<input type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	<input checked="" type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

Microsoft Defender for Cloud provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more

Box 2: Yes -

Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes -

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on-premises.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender> <https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction> <https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction>

 **sokolsulejmani** Highly Voted 2 years ago

keep in mind that Azure Security Center and Azure Defender are now called "Microsoft Defender for Cloud"

upvoted 45 times

 **danialonso** Highly Voted 2 years, 6 months ago

All is correct!

upvoted 25 times

 **RahulX** Most Recent 6 months, 4 weeks ago

YES

YES

YES

upvoted 1 times

 **Curious76** 7 months ago

YYY

Azure Security Center, which helps you protect workloads running in Azure against cyber threats, can now also be used to secure workloads running on-premises and in other clouds. Managing security across increasingly distributed infrastructure is complex and can create gaps that are exploited by attackers.

upvoted 2 times

 **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

□ **StressFree** 12 months ago

Microsoft Defender for Cloud its the new name for them
upvoted 2 times

□ **Sorcias25** 1 year ago

Currently, the plan that is enabled by default is "Foundational CSMP", the new "Defender CSPM" isn't enabled... 'cause it will cost after the preview ends.

Next week I present the exam, and if the Question was updated I'll pass my report here...

upvoted 2 times

□ **Lille_89** 1 year, 3 months ago

Correct

upvoted 4 times

□ **RJJz** 1 year, 3 months ago

cORRECT

upvoted 3 times

□ **Yindave** 1 year, 5 months ago

i hate those 'what kind of subscription support this feature' questions, but lucky i've got this one correct, all of them are Yes

upvoted 8 times

□ **obaali1990** 1 year, 1 month ago

I am happy for you.

upvoted 1 times

□ **IXone** 1 year, 5 months ago

CORRECT

upvoted 3 times

□ **SiDoCiOuS** 1 year, 5 months ago

On the exam 10/18/2022.

upvoted 4 times

□ **hihiha** 1 year, 5 months ago

I need all exam

upvoted 1 times

□ **smartin2010** 1 year, 6 months ago

Correct

upvoted 1 times

□ **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 4 times

□ **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

□ **Raze** 1 year, 11 months ago

all correct

upvoted 2 times

Question #61

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use

Reports
Hunting
Attack simulator
Incidents

in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

https://shop335422782.taobao.com 淘宝搜索店铺:黑马专业认证
微信添加 hello231119**Correct Answer:****Answer Area**

You can use

Reports
Hunting
Attack simulator
Incidents

in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide>

 **Breino** Highly Voted 2 years, 8 months ago

Incidents:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide>

upvoted 24 times

 **Contactfornitish** Highly Voted 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 7 times

 **zellck** Most Recent 11 months ago

"Incidents" is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide>

An incident in Microsoft 365 Defender is a collection of correlated alerts and associated data that make up the story of an attack.

upvoted 1 times

 **MoneyStacking** 1 year, 2 months ago

Indicents > alerts

upvoted 4 times

 **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 4 times

 **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 2 times

 **Raze** 1 year, 11 months ago

ans is correct

upvoted 2 times

 **cyber_rip** 1 year, 11 months ago

correct

upvoted 2 times

 **Cereb7** 1 year, 11 months ago

Same link: " A view of threat-related incidents which aggregate alerts into end-to-end attack stories across Microsoft Defender for Endpoint and Microsoft Defender for Office 365 to reduce the work queue, as well as simplify and speed up your investigation."

upvoted 2 times

 **Surjit24** 2 years, 1 month ago

Reports can allow Aggregation

upvoted 3 times

 **Alessandro_L** 2 years, 1 month ago

Incidents - CORRECT

upvoted 5 times

 **Chris_Chen** 2 years, 2 months ago

Correct

upvoted 1 times

 **Melwin86** 2 years, 8 months ago

correct

upvoted 2 times

Question #62

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	<input type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can deny outbound traffic to the internet.	<input type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	<input checked="" type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can deny outbound traffic to the internet.	<input checked="" type="radio"/>	<input type="radio"/>
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	<input checked="" type="radio"/>	<input type="radio"/>

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

 **Art3** Highly Voted 2 years, 6 months ago

correct!

upvoted 29 times

 **Jitusrit** Highly Voted 2 years, 4 months ago

Correct

upvoted 9 times

 **Melvinpisa** Most Recent 2 months ago

So basically NSG can do everything that an Azure Firewall can do with the exception of NAT.

upvoted 1 times

 **RahulX** 6 months, 4 weeks ago

YES

YES

YES

upvoted 1 times

 **zellck** 11 months ago

YYY is the answer.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

upvoted 1 times

 **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 5 times

 **BN7** 1 year, 9 months ago

correct!

upvoted 2 times

 **KikaJ** 1 year, 10 months ago

correct

upvoted 2 times

 **misterperson** 1 year, 10 months ago

correct

upvoted 2 times

 **krnjtSingh** 1 year, 11 months ago

correct

upvoted 1 times

 **maheshwaghmare** 1 year, 11 months ago

Correct!

upvoted 2 times

 **Raze** 1 year, 11 months ago

ans is correct

upvoted 1 times

 **jingling** 1 year, 11 months ago

correct

upvoted 1 times

 **Chris_Chen** 2 years, 2 months ago

Correct

upvoted 2 times

 **Adriamcam** 2 years, 5 months ago

correct

upvoted 3 times

Question #63

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
------------	-----	----

Microsoft Intune can be used to manage Android devices.

Microsoft Intune can be used to provision Azure subscriptions.

Microsoft Intune can be used to manage organization-owned devices and personal devices.

Answer Area

Statements	Yes	No
------------	-----	----

Correct Answer: Microsoft Intune can be used to manage Android devices.

Microsoft Intune can be used to provision Azure subscriptions.

Microsoft Intune can be used to manage organization-owned devices and personal devices.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune> <https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management>

 Igab Highly Voted 2 years, 7 months ago

Correct

upvoted 18 times

 Whyiest Highly Voted 1 year, 2 months ago

Correct. Note that Intune does not have something to deal with provisioning resources.

Intune mainly allows you to manage endpoints.

upvoted 6 times

 jentifelmalti Most Recent 4 months, 1 week ago

Correct!

upvoted 1 times

 RahulX 6 months, 4 weeks ago

YES

NO

YES

upvoted 1 times

 Molota 9 months, 3 weeks ago

Y N Y

So correct answers

upvoted 1 times

 obaali1990 1 year, 1 month ago

The third answer: what type of organizational devices is the question asking?

upvoted 1 times

 Nicochet 1 year, 1 month ago

YNY correct

upvoted 1 times

-  **CAPME22** 1 year, 2 months ago
You can have azure subscription without intune
This is correct - YNY

upvoted 2 times

-  **clem24** 1 year, 10 months ago
Correct
upvoted 1 times

-  **misterperson** 1 year, 10 months ago
correct
upvoted 1 times

-  **fasttony77** 2 years, 2 months ago
Correct
upvoted 1 times

-  **Adil251** 2 years, 3 months ago
CORRECT
upvoted 2 times

Question #64

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can create one Azure Bastion per virtual network.	<input type="radio"/>	<input type="radio"/>
Azure Bastion provides secure user connections by using RDP.	<input type="radio"/>	<input type="radio"/>
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
You can create one Azure Bastion per virtual network.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Bastion provides secure user connections by using RDP.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview> <https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal>

 **mavexamtops** Highly Voted 2 years, 6 months ago

Correct.

<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview>

upvoted 18 times

 **lgab** Highly Voted 2 years, 7 months ago

Correct

upvoted 10 times

 **RahulX** Most Recent 6 months, 4 weeks ago

YES

YES

YES

upvoted 1 times

 **zellck** 11 months ago

YYY is the answer.

<https://learn.microsoft.com/en-us/azure/bastion/bastion-overview>

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal, or via the native SSH or RDP client already installed on your local computer. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

upvoted 3 times

 **zellck** 11 months ago

<https://learn.microsoft.com/en-us/azure/bastion/bastion-overview#architecture>

Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.

upvoted 2 times

✉ **Rispid** 1 year, 1 month ago

Tricky question

upvoted 3 times

✉ **DikSoft** 1 year, 3 months ago

Azure Bastion acts as client using RDP/SSH connection to servers/VMs.

End-User does not use RDP when it connects to Azure Bastion.

YNY

upvoted 8 times

✉ **ezapper2** 1 year, 2 months ago

I believe it still uses RDP however only via the admin portal, not direct.

upvoted 2 times

✉ **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected => YYY

<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview>

upvoted 3 times

✉ **cantbeme** 1 year, 7 months ago

on exam today

upvoted 2 times

✉ **AbhilAM** 1 year, 8 months ago

In exam today

upvoted 1 times

✉ **clem24** 1 year, 10 months ago

YYY is correct

upvoted 1 times

✉ **Cereb7** 1 year, 11 months ago

"Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned." So answer is correct needed to know with exam in 2 days.

upvoted 1 times

✉ **fred2305** 2 years ago

I should say YNY, SSH brings security, not RDP

upvoted 2 times

✉ **Bulldozer** 1 year, 11 months ago

RDP session secured because it is over TLS

upvoted 3 times

✉ **yaza85** 1 year, 10 months ago

RDP is by default encrypted and mutually authenticated so yes it is secure and there is no difference between RDP and SSH from a threat modeling perspective.

upvoted 1 times

✉ **[Removed]** 2 years, 2 months ago

YNY. Azure Bastion uses RDP and SSH together. It does not use RDP by itself. RDP is not a secure connection.

upvoted 4 times

✉ **yaza85** 1 year, 10 months ago

RDP is by default encrypted and mutually authenticated so yes it is secure and there is no difference between RDP and SSH from a threat modeling perspective.

upvoted 1 times

✉ **TJ001** 2 years, 2 months ago

How does SSH matter for Windows servers you are trying to connect via Bastion?

upvoted 2 times

✉ **yaza85** 1 year, 10 months ago

SSH connection is available for Windows since Windows Management Framework 5.1.

Azure Bastion can also be used to connect to Linux servers so SSH is used by default

upvoted 1 times

✉ **itelessons** 2 years ago

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

upvoted 3 times

Question #65

Topic 1

What feature in Microsoft Defender for Endpoint provides the first line of defense against cyberthreats by reducing the attack surface?

- A. automated remediation
- B. automated investigation
- C. advanced hunting
- D. network protection

Correct Answer: D

Network protection helps protect devices from Internet-based events. Network protection is an attack surface reduction capability.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide>

Community vote distribution D (100%)

 [Removed]  2 years, 1 month ago

Selected Answer: D

D is the right answer!

upvoted 11 times

 Contactfornitish  2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 9 times

 czaaa  5 months, 4 weeks ago

It's technically ASR, but I guess D is also correct since it is network protection.

upvoted 1 times

 RahulX 6 months, 4 weeks ago

D is correct ans.

upvoted 1 times

 furq2904 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 1 times

 zellck 11 months ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide#overview-of-network-protection>

Network protection helps protect devices from Internet-based events. Network protection is an attack surface reduction capability. It helps prevent employees from accessing dangerous domains through applications. Domains that host phishing scams, exploits, and other malicious content on the Internet are considered dangerous. Network protection expands the scope of Microsoft Defender SmartScreen to block all outbound HTTP(s) traffic that attempts to connect to low-reputation sources (based on the domain or hostname).

upvoted 1 times

 Yelad 1 year, 8 months ago

On the exam 10/07/2022

upvoted 5 times

 Beng_ali 2 years, 2 months ago

Selected Answer: D

Answer is D

upvoted 5 times

 [Removed] 2 years, 4 months ago

Correct!

upvoted 6 times

Question #66

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area**In Microsoft Sentinel, you can automate common tasks by using**

- deep investigation tools.
- hunting search-and-query tools.
- playbooks.
- workbooks.

Correct Answer:**Answer Area****In Microsoft Sentinel, you can automate common tasks by using**

- deep investigation tools.
- hunting search-and-query tools.
- playbooks.
- workbooks.

Reference:

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

 **Whyiest** Highly Voted  1 year, 2 months ago

Correct answer.

Workbooks in Azure Sentinel are interactive dashboards that allow users to explore and analyze security data. They provide a visual representation of security data, allowing users to quickly identify patterns and trends. Workbooks can be customized to display specific data and can be shared with other users.

Playbooks in Azure Sentinel are automated response capabilities that allow users to take action on security incidents. They provide a set of predefined playbooks and actions to help users respond to security incidents quickly and effectively. Playbooks can be triggered by specific events or conditions, and can be customized to fit the needs of the organization. They also have the capability to integrate with other Azure services and third-party tools, and can be used to automate incident triage, investigations, and remediation tasks.

In summary, Workbooks are for analysis and visualization of security data, whereas Playbooks are for automated incident response.
upvoted 20 times

 **Geolem** Highly Voted  1 year, 6 months ago

<https://learn.microsoft.com/en-us/azure/sentinel/overview#automate-and-orchestrate-common-tasks-by-using-playbooks>
upvoted 11 times

 **RahulX** Most Recent  6 months, 4 weeks ago

Playbooks is the correct ans.
upvoted 1 times

 **Darkfire** 8 months ago

Answer is correct

Keyword = Workbooks = Microsoft Sentinel
upvoted 1 times

 **Darkfire** 8 months ago

Excuse my language

Playbooks
upvoted 1 times

 **StressFree** 12 months ago

the word here is AUTOMATE, to automate must be Playbooks
upvoted 2 times

 **Nicochet** 1 year, 1 month ago

Playbooks
upvoted 2 times

 **TheB** 1 year, 2 months ago

Answer is correct Playbook
upvoted 3 times

Question #67

Which two types of resources can be protected by using Azure Firewall? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Azure virtual machines
- B. Azure Active Directory (Azure AD) users
- C. Microsoft Exchange Online inboxes
- D. Azure virtual networks
- E. Microsoft SharePoint Online sites

Correct Answer: DE

Community vote distribution

AD (97%)



 **Hellboy** Highly Voted 2 years, 5 months ago

A and D
upvoted 58 times

 **Cepul** Highly Voted 2 years, 3 months ago

Selected Answer: AD
A and D are correct
upvoted 23 times

 **zeek_9** Most Recent 2 months ago

Selected Answer: DE
D. Azure virtual networks
E. Microsoft SharePoint Online sites

Azure Firewall is specifically designed to secure and control traffic between Azure virtual networks and the internet (option D). While it can provide protection for certain types of Microsoft 365 services, such as SharePoint Online sites (option E), it is not primarily focused on protecting individual Azure virtual machines (option A). Therefore, the correct selections are D and E.

upvoted 2 times

 **gwbr** 2 months, 2 weeks ago

Selected Answer: DE
it is confusing and not exactly intuitive but I had to agree that D&E are the correct answers since Virtual Machine is not exactly a network resource per se, while Sharepoint is a network application.
"You can use the Azure Firewall built-in Service Tags and FQDN tags to allow outbound communication to Office 365 endpoints and IP addresses."
-- <https://learn.microsoft.com/en-us/azure/firewall/protect-office-365>
upvoted 1 times

 **Paddy71** 3 months ago

Protecting SharePoint Online with an Azure Firewall can provide several benefits. Azure Firewall is a cloud-native stateful firewall as a service that can be deployed in your virtual networks or in Azure Virtual WAN hub deployments for filtering traffic flowing between cloud resources, the Internet, and on-premises. You can create rules or policies specifying allow/deny traffic using layer 3 to layer 7 controls. You can also filter traffic going to the internet using both Azure Firewall and third parties by directing some or all traffic through third-party security providers for advanced filtering and user protection. This can help to improve the security of your SharePoint Online deployment by providing an additional layer of protection against web attacks and simplifying security management without requiring any application changes.

upvoted 1 times

 **schepkev** 3 months, 2 weeks ago

Selected Answer: AD
A and D
upvoted 1 times

 **Wilderness** 4 months, 1 week ago

A and D is correct
upvoted 1 times

 **uikty** 4 months, 3 weeks ago

"E" is an absurd incorrect answer that I don't know where it comes from
A and D
upvoted 1 times

 **Grimz** 5 months, 1 week ago

Selected Answer: AD

A and D

upvoted 1 times

 RahulX 6 months, 4 weeks ago

A and D is correct ans.

Azure VM

Azure Vnet

upvoted 1 times

 theptr 7 months ago**Selected Answer: AD**

Q And D

upvoted 1 times

 Darkfire 8 months ago**Selected Answer: AD**

Should be A & D

upvoted 1 times

 rsb7 9 months, 1 week ago**Selected Answer: AD**

Correct answer AD

upvoted 1 times

 eliomadeit 9 months, 3 weeks ago**Selected Answer: AD**

Network and Vms are two different types of resources, SP online does not need any firewall

upvoted 2 times

 manofsteel9 10 months ago**Selected Answer: AD**

Correct Answer: A & D

upvoted 2 times

 DrHax 10 months, 2 weeks ago**Selected Answer: AD**

A and D are correct

upvoted 1 times

 Ibbxtreme 1 year ago**Selected Answer: AD**

Obvious answers :)

upvoted 3 times

Question #68

Topic 1

You plan to implement a security strategy and place multiple layers of defense throughout a network infrastructure.

Which security methodology does this represent?

- A. threat modeling
- B. identity as the security perimeter
- C. defense in depth
- D. the shared responsibility model

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth>

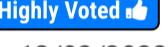
Community vote distribution

C (100%)

✉  **eddie_network_jedi**  2 years, 5 months ago

right, "defense" is the keyword here.

upvoted 10 times

✉  **Contactfornitish**  2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 10 times

✉  **Fabulous_7**  3 months, 3 weeks ago

If someone missed this question; obviously you're not qualified for the exam..... 'DEFENSE INDEPTH'

upvoted 1 times

✉  **RahulX** 6 months, 4 weeks ago

C. defense in depth

upvoted 1 times

✉  **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/3-describe-defense-depth>

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. A defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data.

upvoted 3 times

✉  **LegendZA** 1 year ago

Correct

upvoted 1 times

✉  **churkin6** 1 year ago

Selected Answer: C

C is Correct

upvoted 2 times

✉  **TheB** 1 year, 2 months ago

keyword "multiple layers of defense" = defense In-depth

upvoted 2 times

✉  **amsioso** 1 year, 7 months ago

layers=depth

upvoted 2 times

✉  **Random_Mane** 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 5 times

✉  **[Removed]** 2 years, 1 month ago

Selected Answer: C

Answer is correct

upvoted 1 times

 **TJ001** 2 years, 2 months ago

right answers Defence in depth spanning

Data, Application, Compute, Network , Perimeter , Identity and Access and Physical. Of this physical is more of cloud provider responsibility

upvoted 3 times

Question #69

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	<input type="radio"/>	<input type="radio"/>
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	<input type="radio"/>	<input type="radio"/>
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	<input checked="" type="radio"/>	<input type="radio"/>
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	<input type="radio"/>	<input checked="" type="radio"/>

 [Removed]  2 years, 4 months ago

Correct !

Y
Y
N

upvoted 16 times

 Contactfornitish  2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 14 times

 azhrhsn  2 months, 2 weeks ago

Yes, Yes, No

upvoted 1 times

 Tahamaffia 6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 2 times

 RahulX 6 months, 4 weeks ago

YES

YES

NO

upvoted 1 times

 zellck 11 months ago

YYN is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/non-windows?view=o365-worldwide#microsoft-defender-for-endpoint-on-android>

Microsoft Defender for Endpoint on Android is our mobile threat defense solution for devices running Android 6.0 and higher. Both Android Enterprise (Work Profile) and Device Administrator modes are supported. On Android, we offer web protection, which includes anti-phishing, blocking of unsafe connections, and setting of custom indicators. The solution scans for malware and potentially unwanted applications (PUA) and offers additional breach prevention capabilities through integration with Microsoft Intune and Conditional Access.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/supported-capabilities-by-platform?view=o365-worldwide>
upvoted 1 times

 LegendZA 1 year ago

Correct - Y, Y, N
upvoted 2 times

 **Nicochet** 1 year, 1 month ago

YYN is correct.
upvoted 2 times

 **2cent2** 1 year, 2 months ago

YYN, because "MS Defender for O365" is taking care of Sharepoint Online
upvoted 6 times

 **SleepyBear** 1 year, 2 months ago

shouldn't be all YYY. The Sharepoint is part of Office 365.
upvoted 2 times

 **Eduardo_S** 1 year, 2 months ago

Endpoint is for resources, Sharepoint Online Sites is PaaS
upvoted 2 times

 **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)
I selected => Y Y N
upvoted 2 times

 **cantbeme** 1 year, 7 months ago

on exam today
upvoted 1 times

 **AbhilAM** 1 year, 8 months ago

In exam today
upvoted 2 times

 **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022
upvoted 2 times

 **mmNYC** 2 years, 2 months ago

WHO PROTECTS SHARE POINT?
upvoted 5 times

 **amgfishin** 1 year, 2 months ago

Azure WAF
upvoted 2 times

 **skycrap** 1 year, 3 months ago

Back-ups
upvoted 2 times

 **Hot_156** 2 years, 1 month ago

Microsoft Defender for Office 365
upvoted 22 times

 **Marisasa58** 1 year, 6 months ago

I thought same
upvoted 1 times

 **TJ001** 2 years, 2 months ago

Y, Y, N
upvoted 1 times

 **phatboi** 2 years, 3 months ago

Y,Y,N
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/android-intune?view=o365-worldwide#:~:text=Defender%20for%20Endpoint%20supports%20Device,up%20VPN%20service%20while%20onboarding.>
upvoted 5 times

Question #70

Topic 1

What can you use to scan email attachments and forward the attachments to recipients only if the attachments are free from malware?

- A. Microsoft Defender for Office 365
- B. Microsoft Defender Antivirus
- C. Microsoft Defender for Identity
- D. Microsoft Defender for Endpoint

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description>

Community vote distribution

A (100%)

 [Removed]  2 years, 4 months ago

Correct

upvoted 18 times

 Contactfornitish  2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 8 times

 RahulX  6 months, 4 weeks ago

A. Microsoft Defender for Office 365

upvoted 1 times

 zellck 11 months ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365?view=o365-worldwide>

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.

upvoted 1 times

 LegendZA 1 year ago

Selected Answer: A

Correct

upvoted 1 times

 Nicochet 1 year, 1 month ago

A Defender for O365 is the correct answer.

upvoted 2 times

 TheB 1 year, 2 months ago

Selected Answer: A

Defender for O365 is the correct answer

upvoted 3 times

 Mcelona 1 year, 3 months ago

Selected Answer: A

Correct

upvoted 2 times

 yonie 1 year, 3 months ago

Selected Answer: A

Easy A

upvoted 1 times

 Mcelona 1 year, 3 months ago

Selected Answer: A

A is the right answer

upvoted 1 times

□  **pinda** 1 year, 4 months ago

Selected Answer: A

Correct

upvoted 1 times

□  **cantbeme** 1 year, 7 months ago

on exam today

upvoted 1 times

□  **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 2 times

□  **Kamoshika** 1 year, 10 months ago

Selected Answer: A

Answer is A

upvoted 1 times

□  **Beng_ali** 2 years, 2 months ago

Answer is A

upvoted 1 times

Question #71

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>

Community vote distribution

C (100%)

 **JayHall** Highly Voted 2 years, 5 months ago

Correct

The Microsoft 365 Defender connector for Azure Sentinel (preview) sends all Microsoft 365 Defender incidents and alerts information to Azure Sentinel and keeps the incidents synchronized.

Once you add the connector, Microsoft 365 Defender incidents—which include all associated alerts, entities, and relevant information received from Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Cloud App Security—are streamed to Azure Sentinel as security information and event management (SIEM) data, providing you with context to perform triage and incident response with Azure Sentinel.

Once in Azure Sentinel, incidents remain bi-directionally synchronized with Microsoft 365 Defender, allowing you to take advantage of the benefits of both the Microsoft 365 Defender portal and Azure Sentinel in the Azure portal for incident investigation and response.

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender-integration-with-azure-sentinel?view=o365-worldwide>
upvoted 37 times

 **Contactfornitish** Highly Voted 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 8 times

 **RahulX** Most Recent 6 months, 4 weeks ago

C. integration with Microsoft 365 Defender.

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/security/operations/siem-xdr-overview>

Microsoft 365 Defender is an XDR solution that automatically collects, correlates, and analyzes signal, threat, and alert data from across your Microsoft 365 environment.

Microsoft Sentinel is a cloud-native solution that provides security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities. Together, Microsoft Sentinel and Microsoft 365 Defender provide a comprehensive solution to help organizations defend against modern attacks.

upvoted 2 times

 **2cent2** 1 year, 2 months ago

Selected Answer: C

Microsoft Sentinel is a cloud-native SIEM tool; Microsoft 365 Defender provides XDR capabilities for end-user environments (email, documents, identity, apps, and endpoint); and Microsoft Defender for Cloud provides XDR capabilities for infrastructure and multi-cloud platforms including virtual machines, databases, containers, and IoT.

upvoted 6 times

Question #72

Topic 1

What can you use to provide threat detection for Azure SQL Managed Instance?

- A. Microsoft Secure Score
- B. application security groups
- C. Microsoft Defender for Cloud
- D. Azure Bastion

Correct Answer: C

Community vote distribution

C (100%)

 **OrangeSG** Highly Voted 1 year, 3 months ago

Selected Answer: C

Microsoft Defender for SQL is a Defender plan in Microsoft Defender for Cloud. Microsoft Defender for SQL includes functionality for surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database. It provides a single go-to location for enabling and managing these capabilities.

Microsoft Defender for SQL

<https://learn.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql>

upvoted 10 times

 **KingChuang** Highly Voted 1 year, 6 months ago

Correct.

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>

upvoted 6 times

 **RahulX** Most Recent 6 months, 4 weeks ago

C. Microsoft Defender for Cloud

upvoted 1 times

 **beakes** 6 months, 4 weeks ago

threat detection = Defender

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction#advanced-threat-protection>

An advanced threat protection service continuously monitors your SQL servers for threats such as SQL injection, brute-force attacks, and privilege abuse. This service provides action-oriented security alerts in Microsoft Defender for Cloud with details of the suspicious activity, guidance on how to mitigate to the threats, and options for continuing your investigations with Microsoft Sentinel.

upvoted 1 times

 **LegendZA** 1 year ago

Selected Answer: C

Correct

upvoted 1 times

 **Nicochet** 1 year, 1 month ago

Correct. Defender for cloud

upvoted 2 times

 **Whyiest** 1 year, 2 months ago

Selected Answer: C

Correct

upvoted 2 times

 **Qongo** 1 year, 2 months ago

Correct

upvoted 1 times

 **pinda** 1 year, 4 months ago

Selected Answer: C

Correct

upvoted 3 times

 **Burnie** 1 year, 5 months ago

Correct.

upvoted 1 times

Question #73

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area**Statements**

Yes	No
<input type="radio"/>	<input type="radio"/>

Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.

From the Microsoft 365 Defender portal, you can view how your Microsoft Secure Score compares to the score of organizations like yours.

Microsoft Secure Score in the Microsoft 365 Defender portal gives you points if you address the improvement action by using a third-party application or software.

Correct Answer:

Answer Area**Statements**

Yes	No
<input checked="" type="radio"/>	<input type="radio"/>

Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.

From the Microsoft 365 Defender portal, you can view how your Microsoft Secure Score compares to the score of organizations like yours.

Microsoft Secure Score in the Microsoft 365 Defender portal gives you points if you address the improvement action by using a third-party application or software.

 **delight_1** Highly Voted 1 year, 9 months ago

I was confused with the second answer at first... Now, i verified that Microsoft Secure Score is on Microsoft 365 Defender Portal - Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide>

upvoted 8 times

 **Darkfire** 8 months ago

YYY is correct.

I was confused as well.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score-history-metrics-trends?view=o365-worldwide#compare-your-score-to-organizations-like-yours>

upvoted 2 times

 **Tumi21** Highly Voted 1 year, 9 months ago

YYY is correct

upvoted 5 times

 **RahulX** Most Recent 6 months, 4 weeks ago

YES

YES

YES

upvoted 1 times

 **zellck** 11 months ago

YYY is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide#products-included-in-secure-score>

Currently there are recommendations for the following products:

- Microsoft 365 (including Exchange Online)
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps

- Microsoft Teams

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide#how-it-works>

You're given points for the following actions:

- Configuring recommended security features
- Doing security-related tasks
- Addressing the recommended action with a third-party application or software, or an alternate mitigation

upvoted 2 times

 **zellck** 11 months ago

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide>

Organizations gain access to robust visualizations of metrics and trends, integration with other Microsoft products, score comparison with similar organizations, and much more. The score can also reflect when third-party solutions have addressed recommended actions.

upvoted 1 times

 **obaali1990** 1 year, 1 month ago

Y Y Y is correct

upvoted 3 times

 **Dj6668** 1 year, 4 months ago

Organizations gain access to robust visualizations of metrics and trends, integration with other Microsoft products, score comparison with similar organizations, and much more. The score can also reflect when third-party solutions have addressed recommended actions.

upvoted 3 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 3 times

 **amsioso** 1 year, 7 months ago

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/portals?view=o365-worldwide>

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 3 times

 **xprience** 1 year, 11 months ago

Correct

upvoted 4 times

Question #74

Topic 1

Which Azure Active Directory (Azure AD) feature can you use to restrict Microsoft Intune-managed devices from accessing corporate resources?

- A. network security groups (NSGs)
- B. Azure AD Privileged Identity Management (PIM)
- C. conditional access policies
- D. resource locks

Correct Answer: C

Community vote distribution

C (100%)

✉ **Adriamcam** Highly Voted 2 years, 5 months ago
correct
upvoted 17 times

✉ **Anshul10** Most Recent 3 weeks, 6 days ago
Selected Answer: C
Conditional Access Policy
upvoted 1 times

✉ **RahulX** 6 months, 3 weeks ago
C. Conditional Access Policy.
upvoted 1 times

✉ **zellck** 11 months ago
Selected Answer: C
C is the answer.

<https://learn.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use#device-based-conditional-access>
With Intune, you deploy device compliance policies to determine if a device meets your expected configuration and security requirements. The compliance policy evaluation determines the device's compliance status, which is reported to both Intune and Azure AD. It's in Azure AD that Conditional Access policies can use a device's compliance status to make decisions on whether to allow or block access to your organization's resources from that device.

upvoted 3 times

✉ **LegendZA** 1 year ago
Selected Answer: C
Correct
upvoted 1 times

✉ **obaali1990** 1 year, 1 month ago
Answer is correct
upvoted 2 times

✉ **TheB** 1 year, 2 months ago
Selected Answer: C
C is the answer
upvoted 3 times

✉ **Tanzy360** 1 year, 6 months ago
Selected Answer: C
C is the correct answer
upvoted 3 times

✉ **jim85** 2 years, 1 month ago
This should be Compliance Policy, not conditional access policy, see <https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>
upvoted 2 times

✉ **yaza85** 1 year, 10 months ago
Compliance Policy are also NOT Azure Active Directory (Azure AD) feature
upvoted 3 times

✉ **sokolsulejmani** 2 years ago

Compliance policies have nothing to do with "Access". Conditional access policies is the right answer
upvoted 8 times

✉  **j0rgevasquez** 2 years ago

That's Right

upvoted 3 times

✉  **CatoFong** 2 years ago

this is incorrect. compliance policy isn't one of the available answers and if it were available, it still has nothing to do with access

upvoted 5 times

✉  **luckyiki** 1 year, 2 months ago

This is the correct link but if you read it further it states:

When you use Conditional Access, you can configure your Conditional Access policies to use the results of your device compliance policies to determine which devices can access your organizational resources. This access control is in addition to and separate from the actions for noncompliance that you include in your device compliance policies

So answer C is correct in this case

upvoted 3 times

Question #75

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Azure Defender
Azure Sentinel
Microsoft Cloud App Security

can use conditional access policies to control sessions in real time.

Correct Answer:

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Azure Defender
Azure Sentinel
Microsoft Cloud App Security

can use conditional access policies to control sessions in real time.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security>

An_is_here Highly Voted 2 years, 8 months ago

The answer is CORRECT. Using Conditional Access App Control protection to get real-time visibility and control over access and activities within your cloud apps.

<https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security#architecture>

upvoted 45 times

Randy8 Highly Voted 2 years, 1 month ago

Microsoft Cloud App Security has been renamed to Microsoft Defender for Cloud Apps:

https://techcommunity.microsoft.com/t5/itops-talk-blog/azure-security-product-name-changes-microsoft-ignite-november/ba-p/3004418?WT.mc_id=modinfra-48365-socuff

upvoted 25 times

zellck Most Recent 11 months ago

"Microsoft Cloud App Security" is the answer.

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad#how-it-works>

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Defender for Cloud Apps portal to further refine filters and set actions to be taken on a user.

upvoted 2 times

LegendZA 1 year ago

Correct - Microsoft Cloud App Security which is now Microsoft Defender for Cloud Apps

upvoted 2 times

cantbeme 1 year, 7 months ago

on exam today

upvoted 3 times

Yelad 1 year, 8 months ago

On the exam 10/07/2022

upvoted 3 times

domranmanhu 1 year, 11 months ago

Correct

upvoted 2 times

DemekeA 2 years, 1 month ago

Answer is correct

upvoted 3 times

- abhmala1 2 years, 1 month ago
THIS CAME ON 15.2.22 EXAM
upvoted 7 times
- Alessandro_L 2 years, 1 month ago
CORRECT
upvoted 1 times
- Jitusrit 2 years, 4 months ago
Absolutely right.
upvoted 1 times
- mileytores 2 years, 5 months ago
Es un CASB basicamente
upvoted 1 times
- Nic1234 2 years, 6 months ago
correct
upvoted 1 times
- P_2311 2 years, 8 months ago
correct
upvoted 3 times
- Melwin86 2 years, 8 months ago
corrcrt
<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad>
upvoted 5 times

Question #76

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure DDoS Protection Standard can be used to protect

Azure Active Directory (Azure AD) applications.
Azure Active Directory (Azure AD) users.
resource groups.
virtual networks.

Correct Answer:**Answer Area**

Azure DDoS Protection Standard can be used to protect

Azure Active Directory (Azure AD) applications.
Azure Active Directory (Azure AD) users.
resource groups.
virtual networks.

Reference:

<https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview>

 **An_is_here** Highly Voted 2 years, 8 months ago

Azure DDoS Protection Standard, combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks. It is automatically tuned to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it requires no application or resource changes.

Since Azure Resources is not listed as part of the option, VIRTUAL NETWORK is the correct answer

<https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview>

upvoted 41 times

 **Nepean** Highly Voted 2 years, 2 months ago

Got 1000. Answer is correct.

upvoted 28 times

 **RahulX** Most Recent 6 months, 4 weeks ago

VIRTUAL NETWORK

upvoted 1 times

 **bigelmo_elmo** 9 months ago

Correct answer because DDoS protection is a type of protection that happens in the networking layer.

upvoted 2 times

 **LegendZA** 1 year ago

Correct - Virtual network.

upvoted 2 times

 **ra1paul** 1 year, 1 month ago

Correct Answer.

upvoted 2 times

 **Norasit** 1 year, 11 months ago

I found this question in exam today but it is AZ-900!!!

upvoted 5 times

 **Contactfornitish** 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 5 times

 **Alessandro_L** 2 years, 1 month ago

CORRECT.

upvoted 3 times

 **thiaybovo** 2 years, 3 months ago

CORRECT

upvoted 1 times

 **vakkil** 2 years, 4 months ago

Technically answer should be all resources in a virtual network.

as per the details mentioned in one of the feature i.e. Multi-Layered protection mentioned in the below link, directs the answer to be network layer protection (i.e. virtual network).

<https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview>

upvoted 4 times

 **Jitusrit** 2 years, 4 months ago

DDOS HAPPENS on IP based identity, so virtual network is correct. But what is the purpose then we can say to secure the application or resources.

upvoted 3 times

 **LoremanReturns** 2 years, 5 months ago

"Azure DDoS Protection is enabled at the Virtual Network level"

<https://azure.microsoft.com/en-gb/pricing/details/ddos-protection/>

upvoted 6 times

 **Ender3** 2 years, 5 months ago

IMHO, both A and D are correct. But since only one answer can be given, I am in a quandary on how to answers in a real test. I guess I would take a 50/50 chance with D.

upvoted 1 times

 **Ender3** 2 years, 5 months ago

IMHO, both A and D are correct. But since only one answer can be given, I am in a quandary on how to answers in a real test. I guess I would take a 50/50 chance with D.

upvoted 1 times

 **alopezme** 2 years, 5 months ago

Azure DDoS Protection is enabled at the Virtual Network level. All protected resource types within the Virtual Network will be automatically protected when Azure DDoS Protection is enabled on the Virtual Network.

<https://azure.microsoft.com/en-gb/pricing/details/ddos-protection/>

upvoted 2 times

 **Thabiso786** 2 years, 6 months ago

Please read the 1st line. Azure Firewall protects your Virtual Network, DDOS protects your applications

<https://docs.microsoft.com/en-us/learn/modules/describe-basic-security-capabilities-azure/4-describe-what-azure-firewall>

upvoted 1 times

 **jedboy88** 2 years, 5 months ago

This document doesn't mention anything about DDoS.

upvoted 1 times

Question #77

Topic 1

What should you use in the Microsoft 365 Defender portal to view security trends and track the protection status of identities?

- A. Attack simulator
- B. Reports
- C. Hunting
- D. Incidents

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-and-insights-in-security-and-compliance?view=o365-worldwide>

Community vote distribution

B (100%)

 **Clouddog** Highly Voted 1 year, 11 months ago

Keyword is trends = reports

upvoted 26 times

 **[Removed]** Highly Voted 1 year, 11 months ago

Selected Answer: B

correct

upvoted 7 times

 **RahulX** Most Recent 6 months, 4 weeks ago

B. Reports

upvoted 1 times

 **obaali1990** 1 year, 1 month ago

Report should be the right answer. I was contemplating on incidents, but the correct answer is reports

upvoted 2 times

 **Armanas** 1 year, 6 months ago

Selected Answer: B

This Question appeared in Exam today (02 September 2022)

I selected => B

Keyword is trends = reports

upvoted 7 times

Question #78

Topic 1

You have a Microsoft 365 E3 subscription.

You plan to audit user activity by using the unified audit log and Basic Audit.

For how long will the audit records be retained?

- A. 15 days
- B. 30 days
- C. 90 days
- D. 180 days

Correct Answer: C

Community vote distribution



✉  **bill086**  1 year, 11 months ago

Selected Answer: C

90 days

upvoted 13 times

✉  **Clouddog**  1 year, 11 months ago

Microsoft 365 unified auditing helps to track activities performed in the different Microsoft 365 services by both users and admins. Basic auditing is enabled by default for most Microsoft 365 organizations. In the Basic audit, audit records are retained and searchable for the last 90 days.

<https://o365reports.com/2021/07/07/microsoft-365-retrieve-audit-log-for-1-year-for-all-subscriptions/>

upvoted 10 times

✉  **chimuelo69**  14 hours, 5 minutes ago

Selected Answer: D

It's 180 days now.

upvoted 1 times

✉  **N4RUT2** 1 day, 18 hours ago

Selected Answer: D

from 90 days to 180 days <https://learn.microsoft.com/en-us/purview/audit-log-retention-policies>

upvoted 1 times

✉  **C0mptias_Main_Guy** 1 month ago

Selected Answer: D

It's now 180 Days. See reference: <https://learn.microsoft.com/en-us/purview/audit-log-retention-policies>

The default retention period for Audit (Standard) has changed from 90 days to 180 days. Audit (Standard) logs generated before October 17, 2023 are retained for 90 days. Audit (Standard) logs generated on or after October 17, 2023 follow the new default retention of 180 days.

upvoted 3 times

✉  **MBjmb** 3 weeks ago

YES IT'S 180 DAYS NOW

upvoted 2 times

✉  **stdevops** 1 month, 1 week ago

Selected Answer: D

Has been changed to 180 days

upvoted 1 times

✉  **hacksp1d3r** 1 month, 3 weeks ago

Selected Answer: D

changed to 180 now

upvoted 2 times

✉  **Manny_ez** 2 months, 1 week ago

Selected Answer: D

Its 180 now.

upvoted 3 times

✉  **Melvinpisa** 2 months, 1 week ago

It was 90 days before but now is 180 days.
upvoted 2 times

 **Ansssh** 2 months, 2 weeks ago

180 days
upvoted 2 times

 **MyNameiswhattt** 2 months, 3 weeks ago

For users assigned any other (non-E5) Office 365 or Microsoft 365 license, audit records are retained for 180 days. For a list of Office 365 and Microsoft 365 subscriptions that support unified audit logging, see the subscription requirements for Audit (Standard) and Audit (Premium).
<https://learn.microsoft.com/en-us/purview/audit-new-search>

upvoted 1 times

 **tc_praveen** 3 months ago

180 DAYS NOW.

The default retention period for Audit (Standard) has changed from 90 days to 180 days. Audit (Standard) logs generated before October 17, 2023 are retained for 90 days. Audit (Standard) logs generated on or after October 17, 2023 follow the new default retention of 180 days.

<https://learn.microsoft.com/en-us/purview/audit-log-retention-policies>

upvoted 3 times

 **C0mptias_Main_Guy** 1 month ago

Confirmed. It is now 180 days.
upvoted 1 times

 **frych** 3 months, 1 week ago

Selected Answer: D

180 days now!
upvoted 3 times

 **tc_praveen** 3 months, 1 week ago

any sources for reference?
upvoted 1 times

 **C0mptias_Main_Guy** 1 month ago

<https://learn.microsoft.com/en-us/purview/audit-log-retention-policies>
upvoted 1 times

 **JohnboscoD** 4 months, 3 weeks ago

Correct answer is D 180 days.
<https://learn.microsoft.com/en-us/purview/audit-standard-setup?view=o365-worldwide>
upvoted 4 times

 **marges_stud** 4 months, 3 weeks ago

Selected Answer: D

Answer D is now correct.

per: <https://learn.microsoft.com/en-us/purview/audit-solutions-overview?view=o365-worldwide#licensing-requirements>
"The default retention period for Audit (Standard) has changed from 90 days to 180 days. Audit (Standard) logs generated before October 17, 2023 are retained for 90 days. Audit (Standard) logs generated on or after October 17, 2023 follow the new default retention of 180 days."
upvoted 7 times

 **RahulX** 6 months, 4 weeks ago

C. 90 days

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview?view=o365-worldwide#comparison-of-key-capabilities>
upvoted 1 times

Question #79

Topic 1

To which type of resource can Azure Bastion provide secure access?

- A. Azure Files
- B. Azure SQL Managed Instances
- C. Azure virtual machines
- D. Azure App Service

Correct Answer: C

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

Reference:

<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview>

Community vote distribution

C (100%)

✉  **tigermaq**  1 year, 9 months ago

Selected Answer: C

Correct

upvoted 10 times

✉  **Clouddog**  1 year, 11 months ago

Correct, Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses. Provision the service directly in your local or peered virtual network to get support for all the VMs within it.

<https://azure.microsoft.com/en-us/services/azure-bastion/>

upvoted 6 times

✉  **RahulX**  6 months, 4 weeks ago

C. Azure virtual machines

upvoted 1 times

✉  **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/bastion/bastion-overview>

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal, or via the native SSH or RDP client already installed on your local computer. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

upvoted 1 times

✉  **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 4 times

✉  **[Removed]** 1 year, 11 months ago

Selected Answer: C

correct

upvoted 5 times

Question #80

What are three uses of Microsoft Cloud App Security? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. to discover and control the use of shadow IT
- B. to provide secure connections to Azure virtual machines
- C. to protect sensitive information hosted anywhere in the cloud
- D. to provide pass-through authentication to on-premises applications
- E. to prevent data leaks to noncompliant apps and limit access to regulated data

Correct Answer: ACE

Reference:

<https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps>

Community vote distribution

ACE (100%)

✉️  **CletusMaximus**  1 year, 5 months ago

Correct. A,C,E

The correct answers can be found via <https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps>. Look for the following title in the article "The Defender for Cloud Apps framework"

upvoted 12 times

✉️  **manofsteel9**  10 months ago

Selected Answer: ACE

A. To discover and control the use of shadow IT: Microsoft Cloud App Security helps organizations discover and gain visibility into the cloud applications and services being used within their environment. It allows IT administrators to assess the risk associated with these shadow IT applications and apply policies to control their usage.

C. To protect sensitive information hosted anywhere in the cloud: Microsoft Cloud App Security provides data loss prevention (DLP) capabilities to protect sensitive information and prevent data leaks in cloud applications. It helps organizations enforce policies to ensure that sensitive data is protected, regardless of where it is hosted in the cloud.

E. To prevent data leaks to noncompliant apps and limit access to regulated data: Microsoft Cloud App Security allows organizations to monitor and control the flow of data within cloud applications. It helps prevent data leaks to noncompliant apps by enforcing policies and restrictions. It also enables organizations to limit access to regulated data, ensuring compliance with data protection regulations.

upvoted 5 times

✉️  **RahulX**  6 months, 4 weeks ago

A. to discover and control the use of shadow IT

C. to protect sensitive information hosted anywhere in the cloud

E. to prevent data leaks to noncompliant apps and limit access to regulated data

upvoted 1 times

✉️  **obaali1990** 1 year, 1 month ago

Correct Answers-ACE

upvoted 2 times

✉️  **yonie** 1 year, 3 months ago

Selected Answer: ACE

Hard question

Correct is ACE

upvoted 4 times

Question #81

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

In the Microsoft 365 Defender portal, an incident is a collection of correlated

alerts
events
vulnerabilities
Microsoft Secure Score improvement actions

Correct Answer:**Answer Area**

In the Microsoft 365 Defender portal, an incident is a collection of correlated

alerts
events
vulnerabilities
Microsoft Secure Score improvement actions

Box 1: vulnerabilities -

Microsoft 365 Defender portal is the new home for monitoring and managing security across your identities, data, devices, and apps, you will need to access various portals for certain specialized tasks.

It used to monitor and respond to threat activity and strengthen security posture across your identities, email, data, endpoints, and apps with Microsoft 365

Defender -

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/portals>

 **darkpangel** Highly Voted 1 year, 6 months ago

Alerts Is the Answer

An incident in Microsoft 365 Defender is a collection of correlated alerts and associated data that make up the story of an attack.

<https://learn.microsoft.com/es-es/microsoft-365/security/defender/incidents-overview?view=o365-worldwide>

upvoted 40 times

 **KingChuang** Highly Voted 1 year, 6 months ago

show in exam 09/19

Alerts is the answer

upvoted 17 times

 **rafaseb** Most Recent 1 month, 1 week ago

Answer should be "alerts"

upvoted 1 times

 **Syl0** 2 months, 3 weeks ago

I thought Alerts and Incidents come together?

upvoted 1 times

 **Ramye** 3 months ago

Alerts is the answer.

@Examtopics pls update with the correct answer.

upvoted 4 times

 **Paddy71** 3 months ago

die word vulnerabilities does not even exist on the referenced URL

upvoted 1 times

 **frych** 3 months, 1 week ago

ALERTS

upvoted 2 times

 **TungstonTim** 4 months, 3 weeks ago

An incident in Microsoft 365 Defender is a collection of correlated alerts and associated data that make up the story of an attack.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide>

upvoted 1 times

□ **RahulX** 6 months, 4 weeks ago

in the Microsoft 365 defender portal an incident is a collection of correlated of Alerts.

upvoted 2 times

□ **Crucius** 7 months, 1 week ago

a = ALERTS

upvoted 1 times

□ **Mpumi** 8 months, 1 week ago

Alerts is the answer.

upvoted 2 times

□ **furq2904** 8 months, 4 weeks ago

appeared on July 1st 2023

upvoted 2 times

□ **Molota** 9 months, 1 week ago

Alert is the answer

upvoted 1 times

□ **manofsteel9** 10 months ago

Alerts

In the Microsoft 365 Defender portal, an incident is a collection of correlated alerts. Incidents help security teams understand the scope and impact of potential threats by grouping related alerts together. This grouping enables efficient investigation and response to security incidents.

upvoted 2 times

□ **zellck** 11 months ago

"alerts" is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide>

An incident in Microsoft 365 Defender is a collection of correlated alerts and associated data that make up the story of an attack.

upvoted 2 times

□ **XtraWest** 11 months, 1 week ago

Alert seems correct

upvoted 1 times

□ **YesOpo** 1 year ago

Alerts is the answer.

upvoted 2 times

Question #82

Topic 1

You need to connect to an Azure virtual machine by using Azure Bastion.

What should you use?

- A. PowerShell remoting
- B. the Azure portal
- C. the Remote Desktop Connection client
- D. an SSH client

Correct Answer: C

You can create an RDP connection to a Windows VM using Azure Bastion.

Reference:

<https://docs.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows>

Community vote distribution

B (97%)

 **yonie** Highly Voted 1 year, 3 months ago

Selected Answer: B

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal
upvoted 15 times

 **cris_exam** Highly Voted 1 year, 2 months ago

Selected Answer: B

Azure portal is correct
upvoted 7 times

 **Aalkinani** Most Recent 1 week, 6 days ago

Selected Answer: B

When connecting to an Azure virtual machine using Azure Bastion, you should use:

B. the Azure portal

Azure Bastion provides a web-based RDP and SSH access to your Azure virtual machines directly through the Azure portal, eliminating the need to expose your virtual machines to the public internet. Therefore, you would use the Azure portal to connect securely to your Azure virtual machine via Azure Bastion.

upvoted 1 times

 **AaronMedrano** 1 month, 3 weeks ago

Selected Answer: B

Selected Answer: B
Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal
upvoted 1 times

 **Harry123421313** 2 months, 1 week ago

B is correct

upvoted 1 times

 **gwbr** 2 months, 2 weeks ago

Selected Answer: B

you use Azure Portal to connect to Bastion
<https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows>
upvoted 1 times

 **geggio** 4 months, 3 weeks ago

Selected Answer: C

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. right.. but how I connect to VM? with rdp
upvoted 2 times

 **Vhailor** 6 months, 2 weeks ago

Selected Answer: B

Azure portal is the correct one.
to use RDP you must change bastion license from basic to standard

upvoted 1 times

□ **RahulX** 6 months, 4 weeks ago

C. RDP

upvoted 2 times

□ **dsharp** 8 months, 1 week ago

Azure portal

upvoted 1 times

□ **rawyak** 9 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

□ **mbontoi** 9 months, 3 weeks ago

the recommendation is RDP

upvoted 1 times

□ **manofsteel9** 10 months ago

Selected Answer: B

B: the Azure portal.

Azure Bastion is a service that provides secure and seamless Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Azure virtual machines directly through the Azure portal. It eliminates the need for public IP addresses or exposing virtual machines to the public internet.

upvoted 1 times

□ **zellck** 11 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/bastion/bastion-overview>

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal, or via the native SSH or RDP client already installed on your local computer. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

upvoted 1 times

□ **XtraWest** 11 months, 1 week ago

Azure Portal as per ChatGPT

upvoted 1 times

□ **clauimagagnotti** 1 year, 1 month ago

Selected Answer: B

upvoted 2 times

□ **Mithu94** 1 year, 1 month ago

Selected Answer: B

Azure portal

upvoted 2 times

Question #83

Topic 1

Which service includes the Attack simulation training feature?

- A. Microsoft Defender for Cloud Apps
- B. Microsoft Defender for Identity
- C. Microsoft Defender for SQL
- D. Microsoft Defender for Office 365

Correct Answer: D

Attack simulation training in Microsoft Defender for Office 365 Plan 2 or Microsoft 365 E5 lets you run benign cyberattack simulations in your organization. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training>

Community vote distribution

D (100%)

 **pinda**  1 year, 4 months ago

Selected Answer: D

Correct

upvoted 7 times

 **fdosoli**  1 year, 5 months ago

Correct, the answer is D

upvoted 5 times

 **TungstonTim**  4 months, 3 weeks ago

Selected Answer: D

In organizations with Microsoft Defender for Office 365 Plan 2 (add-on licenses or included in subscriptions like Microsoft 365 E5), you can use Attack simulation training in the Microsoft 365 Defender portal to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide>

upvoted 1 times

 **RahulX** 6 months, 4 weeks ago

D. Microsoft Defender for Office 365

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide>

If your organization has Microsoft 365 E5 or Microsoft Defender for Office 365 Plan 2, which includes Threat Investigation and Response capabilities, you can use Attack simulation training in the Microsoft 365 Defender portal to run realistic attack scenarios in your organization. These simulated attacks can help you identify and find vulnerable users before a real attack impacts your bottom line.

upvoted 1 times

 **LeoDen** 1 year, 6 months ago

Selected Answer: D

Attack simulation training in Microsoft Defender for Office 365 Plan 2 or Microsoft 365 E5 lets you run benign cyberattack simulations in your organization.

upvoted 4 times

Question #84

Topic 1

Which type of alert can you manage from the Microsoft 365 Defender portal?

- A. Microsoft Defender for Storage
- B. Microsoft Defender for SQL
- C. Microsoft Defender for Endpoint
- D. Microsoft Defender for IoT

Correct Answer: C

The Alerts queue shows the current set of alerts. You get to the alerts queue from Incidents & alerts > Alerts on the quick launch of the Microsoft 365 Defender portal.

Alerts from different Microsoft security solutions like Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft 365 Defender appear here.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts>

Community vote distribution

C (100%)

 **RahulX** 6 months, 4 weeks ago

C. Microsoft Defender for Endpoint
upvoted 2 times

 **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender-portal?view=o365-worldwide>

The Microsoft 365 Defender portal combines protection, detection, investigation, and response to email, collaboration, identity, device, and cloud app threats, in a central place. The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes:

- Microsoft Defender for Endpoint delivers preventative protection, post-breach detection, automated investigation, and response for devices in your organization.

upvoted 2 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: C

Alerts from different Microsoft security solutions like Microsoft Defender for Endpoint, Microsoft Defender for Office 365, and Microsoft 365 Defender appear here.

upvoted 4 times

 **Nail** 1 year, 2 months ago

Selected Answer: C

MDI, MDO, MDE, and MDCA (formerly MCAS) are all in the M365 Defender portal.

upvoted 2 times

 **datahop** 1 year, 4 months ago

Correct is C!

Alert sources

Microsoft 365 Defender

Microsoft Defender for Office 365

Microsoft Defender for Endpoint

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Azure Active Directory (AAD) Identity Protection

App Governance

Microsoft Data Loss Prevention

source: <https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

upvoted 3 times

 **fdosoli** 1 year, 5 months ago

The correct answer is C!

upvoted 3 times

 **CletusMaximus** 1 year, 5 months ago

Yep C is the correct answer.

upvoted 3 times

Question #85

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	<input type="radio"/>	<input type="radio"/>
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	<input type="radio"/>	<input type="radio"/>
Hunting provides you with the ability to identify security threats before an alert is triggered.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	<input type="radio"/>	<input checked="" type="radio"/>
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	<input checked="" type="radio"/>	<input type="radio"/>
Hunting provides you with the ability to identify security threats before an alert is triggered.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No -

Microsoft Sentinel data connectors are available for non-Microsoft services like Amazon Web Services.

Box 2: Yes -

Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor

Workbooks, which provides versatility in creating custom dashboards. While the Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Box 3: Yes -

To help security analysts look proactively for new anomalies that weren't detected by your security apps or even by your scheduled analytics rules, Microsoft

Sentinel's built-in hunting queries guide you into asking the right questions to find issues in the data you already have on your network.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/data-connectors-reference> <https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data> <https://docs.microsoft.com/en-us/azure/sentinel/hunting>

 **Mcelona** Highly Voted  1 year, 3 months ago

N Y Y is the right answer

upvoted 8 times

 **Burnie** Highly Voted  1 year, 5 months ago

First. Correct.

upvoted 6 times

 **RahulX** Most Recent  6 months, 4 weeks ago

No

Yes

Yes

upvoted 1 times

✉  **Lorenz1974** 7 months ago

NYY

3) Use queries before, during, and after a compromise to take the following actions:

Before an incident occurs: Waiting on detections is not enough. Take proactive action by running any threat-hunting queries related to the data you're ingesting into your workspace at least once a week.

Results from your proactive hunting provide early insight into events that may confirm that a compromise is in process, or will at least show weaker areas in your environment that are at risk and need attention.

<https://learn.microsoft.com/en-us/azure/sentinel/hunting#use-built-in-queries>

upvoted 1 times

✉  **zellck** 11 months ago

NYY is the answer.

<https://learn.microsoft.com/en-us/azure/sentinel/overview#collect-data-by-using-data-connectors>

Microsoft Sentinel has built-in connectors to the broader security and applications ecosystems for non-Microsoft solutions. You can also use common event format, Syslog, or REST-API to connect your data sources with Microsoft Sentinel.

<https://learn.microsoft.com/en-us/azure/sentinel/overview#create-interactive-reports-by-using-workbooks>

After you onboard to Microsoft Sentinel, monitor your data by using the integration with Azure Monitor workbooks.

upvoted 1 times

✉  **zellck** 11 months ago

<https://learn.microsoft.com/en-us/azure/sentinel/hunting>

As security analysts and investigators, you want to be proactive about looking for security threats, but your various systems and security appliances generate mountains of data that can be difficult to parse and filter into meaningful events. Microsoft Sentinel has powerful hunting search and query tools to hunt for security threats across your organization's data sources. To help security analysts look proactively for new anomalies that weren't detected by your security apps or even by your scheduled analytics rules, Microsoft Sentinel's built-in hunting queries guide you into asking the right questions to find issues in the data you already have on your network.

upvoted 1 times

Question #86

Topic 1

Which two Azure resources can a network security group (NSG) be associated with? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a virtual network subnet
- B. a network interface
- C. a resource group
- D. a virtual network
- E. an Azure App Service web app

Correct Answer: AB

Association of network security groups

You can associate a network security group with virtual machines, NICs, and subnets, depending on the deployment model you use.

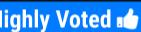
Reference:

<https://aviatrix.com/learn-center/cloud-security/create-network-security-groups-in-azure/>

Community vote distribution



AB (100%)

✉️  **KingChuang**  1 year, 6 months ago

Selected Answer: AB

Correct.

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>
upvoted 7 times

✉️  **Francielle**  1 month ago

Selected Answer: AB

NSG = Virtual Network Subnet and Network Interface.

As per my understanding, D (Virtual Network) is incorrect because the Azure Firewall is deployed there, while the NSG is for subnets.
upvoted 1 times

✉️  **RahulX** 6 months, 3 weeks ago

- A. a virtual network subnet
 - B. a network interface
- upvoted 1 times

✉️  **RahulX** 6 months, 4 weeks ago

- A. a virtual network subnet
 - B. a network interface
- upvoted 1 times

✉️  **Lorenz1974** 7 months ago

Selected Answer: AB

Network security groups (NSGs) let you filter network traffic to and from Azure resources in an Azure virtual network; for example, a virtual machine. An NSG consists of rules that define how the traffic is filtered. YOU CAN ASSOCIATE ONLY ONE NETWORK SECURITY GROUP TO EACH VIRTUAL NETWORK SUBNET AND NETWORK INTERFACE IN A VIRTUAL MACHINE. The same network security group, however, can be associated to as many different subnets and network interfaces as you choose.

<https://learn.microsoft.com/en-us/training/modules/describe-basic-security-capabilities-azure/6-describe-azure-network-security-groups?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-security-solutions>
upvoted 2 times

✉️  **manofsteel9** 10 months ago

Selected Answer: AB

The two Azure resources that a network security group (NSG) can be associated with are:

- A. A virtual network subnet: NSGs can be associated with a virtual network subnet to enforce network security rules on the traffic flowing in and out of that specific subnet. By associating an NSG with a subnet, you can control the inbound and outbound traffic to the resources within that subnet.
 - B. A network interface: NSGs can also be associated with a network interface, which is attached to a virtual machine or other Azure resources. By associating an NSG with a network interface, you can define rules to filter network traffic to and from that specific network interface, providing granular security control at the network level.
- upvoted 1 times

zellck 11 months ago

Selected Answer: AB

AB is the answer.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine. The same network security group can be associated to as many subnets and network interfaces as you choose.

upvoted 1 times

Whyest 1 year, 2 months ago

Correct

upvoted 3 times

yonie 1 year, 3 months ago

Selected Answer: AB

Subnets and NICs

upvoted 3 times

OrangeSG 1 year, 3 months ago

Selected Answer: AB

You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine.

How network security groups filter network traffic

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

upvoted 3 times

osmantaskiran 1 year, 4 months ago

B AND D

a network interface of VM, and Virtual Network

upvoted 1 times

osmantaskiran 1 year, 4 months ago

No No, A and B :)

upvoted 5 times

Question #87

Topic 1

What is a use case for implementing information barrier policies in Microsoft 365?

- A. to restrict unauthenticated access to Microsoft 365
- B. to restrict Microsoft Teams chats between certain groups within an organization
- C. to restrict Microsoft Exchange Online email between certain groups within an organization
- D. to restrict data sharing to external email recipients

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?view=o365-worldwide>

Community vote distribution

B (100%)

 **RiXXX**  2 years, 8 months ago

wrong
is B
C is ethical walls
upvoted 57 times

 **vani009**  2 years, 7 months ago

correct answer is B:Information barriers are supported in Microsoft Teams, SharePoint Online, and OneDrive for Business. A compliance administrator or information barriers administrator can define policies to allow or prevent communications between groups of users in Microsoft Teams. Information barrier policies can be used for situations like these:

upvoted 38 times

 **Arcturus611**  1 month ago

Selected Answer: B
B is the answer
upvoted 2 times

 **frych** 3 months, 1 week ago

Selected Answer: B
only B: Microsoft Teams chats
upvoted 2 times

 **BrkyUlukn** 4 months, 1 week ago

Answer:B
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?view=o365-worldwide>
upvoted 2 times

 **Vaibhavwadhai** 5 months ago

Selected Answer: B
Correct Ans is B
upvoted 1 times

 **Jacktheschreck** 6 months, 2 weeks ago

B is correct....why C?
upvoted 1 times

 **RahulX** 6 months, 4 weeks ago

B. to restrict Microsoft Teams chats between certain groups within an organization
upvoted 1 times

 **Lorenz1974** 7 months ago

Selected Answer: B
With information barriers, the organization can restrict communications among specific groups of users.

MICROSOFT PURVIEW INFORMATION BARRIERS IS SUPPORTED IN MICROSOFT TEAMS, SHAREPOINT ONLINE, AND ONEDRIVE FOR BUSINESS.

Information barriers are policies that admins can configure to prevent individuals or groups from communicating with each other.

<https://learn.microsoft.com/en-us/training/modules/describe-insider-risk-capabilities-microsoft-365/4-describe-information-barriers?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-compliance-solutions>

upvoted 1 times

 **dsharp** 8 months, 1 week ago

B Teams communication

Cannot restrict communication through mails, only Teams, SharePoint, OneDrive

upvoted 1 times

 **Darkfire** 8 months, 1 week ago

Selected Answer: B

B is definitely correct.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide>

upvoted 1 times

 **manofsteel9** 10 months ago

Selected Answer: B

According to the Microsoft Purview documentation¹, information barrier policies are used to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. They can help to avoid conflicts of interest and safeguard internal information between users and organizational areas.

Based on this definition, the best use case for implementing information barrier policies in Microsoft 365 is B. to restrict Microsoft Teams chats between certain groups within an organization. This option matches the scenario of preventing unauthorized communication and collaboration among defined groups and users in Microsoft Teams.

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide>

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. Often used in highly regulated industries, IB can help to avoid conflicts of interest and safeguard internal information between users and organizational areas.

upvoted 1 times

 **SGhani** 11 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **clauimagagnotti** 1 year, 1 month ago

Selected Answer: B

upvoted 1 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: B

Exchange is not supported yet.

upvoted 2 times

 **luckyiki** 1 year, 2 months ago

Selected Answer: B

Microsoft Purview Information Barriers (IB) is supported in Microsoft Teams, SharePoint Online, and OneDrive for Business.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers-solution-overview?view=o365-worldwide>

So not exchange (email)

upvoted 3 times

Question #88

Topic 1

What can you use to deploy Azure resources across multiple subscriptions in a consistent manner?

- A. Microsoft Defender for Cloud
- B. Azure Blueprints
- C. Microsoft Sentinel
- D. Azure Policy

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

Community vote distribution

B (100%)

 **Mcelona** Highly Voted 1 year, 3 months ago

Selected Answer: B

For sure

upvoted 7 times

 **RahulX** Most Recent 6 months, 4 weeks ago

B. Azure Blueprints

upvoted 1 times

 **Lorenz1974** 7 months ago

Selected Answer: B

Azure Blueprints provide a way TO DEFINE A REPEATABLE SET OF AZURE RESOURCES. AZURE BLUEPRINTS ENABLE DEVELOPMENT TEAMS TO RAPIDLY PROVISION AND RUN NEW ENVIRONMENTS, with the knowledge that they're in line with the organization's compliance requirements. TEAMS CAN ALSO PROVISION AZURE RESOURCES ACROSS SEVERAL SUBSCRIPTIONS SIMULTANEOUSLY, meaning they can achieve shorter development times and quicker delivery.

<https://learn.microsoft.com/en-us/training/modules/describe-resource-governance-capabilities-azure/3-describe-use-azure-blueprints?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-compliance-solutions>

upvoted 2 times

 **marst0** 10 months, 2 weeks ago

Selected Answer: B

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide#information-barriers-and-microsoft-teams>

In Microsoft Teams, IB policies determine and prevent the following kinds of unauthorized communication and collaboration:

Searching for a user
 Adding a member to a team
 Starting a chat session with someone
 Starting a group chat
 Inviting someone to join a meeting
 Sharing a screen
 Placing a call
 Sharing a file with another user
 Access to a file through sharing a link

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/azure/governance/blueprints/overview>

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and start up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

upvoted 1 times

 **Armanas** 1 year, 6 months ago

Selected Answer: B

This Question appeared in Exam today (02 September 2022)

I selected => B

upvoted 4 times

Question #89

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	<input type="radio"/>	<input type="radio"/>
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	<input type="radio"/>	<input type="radio"/>
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
With Advanced Audit in Microsoft 365, you can identify when email items were accessed.	<input checked="" type="radio"/>	<input type="radio"/>
Advanced Audit in Microsoft 365 supports the same retention period of audit logs as core auditing.	<input type="radio"/>	<input checked="" type="radio"/>
Advanced Audit in Microsoft 365 allocates customer-dedicated bandwidth for accessing audit data.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

The MailItemsAccessed event is a mailbox auditing action and is triggered when mail data is accessed by mail protocols and mail clients.

Box 2: No -

Basic Audit retains audit records for 90 days.

Advanced Audit retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This is accomplished by a default audit log retention policy that retains any audit record that contains the value of Exchange, SharePoint, or AzureActiveDirectory for the Workload property (which indicates the service in which the activity occurred) for one year.

Box 3: yes -

Advanced Audit in Microsoft 365 provides high-bandwidth access to the Office 365 Management Activity API.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-solutions-overview?view=o365-worldwide#licensing-requirements> <https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/> <https://docs.microsoft.com/en-us/microsoft-365/security-compliance/licensing-guidance#advanced-audit>

 **mavexamtops** Highly Voted 2 years, 6 months ago

Correct!

<https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide>

upvoted 16 times

 **WimTS** Highly Voted 1 year, 6 months ago

Answers are correct, but products are rebranded to:

- Microsoft Purview Audit (Standard)
- Microsoft Purview Audit (Premium)

upvoted 15 times

 **IngeborgAnne** 1 year, 5 months ago

Oh my goodness, thank you! I've been wondering what this Advanced Auditing was supposed to be.

upvoted 4 times

 **Lorenz1974** Most Recent 7 months ago

YNY

Audit (Premium) builds on the capabilities of Audit (Standard). Audit (Premium) provides audit log retention policies and LONGER RETENTION OF AUDIT RECORDS. IT PROVIDES AUDIT RECORDS FOR HIGH-VALUE CRUCIAL EVENTS that can help your organization investigate possible security or compliance breaches and determine the scope of compromise. AUDIT (PREMIUM) ALSO PROVIDES ORGANIZATIONS WITH MORE BANDWIDTH TO ACCESS AUDITING LOGS through the Office 365 Management Activity API.

<https://learn.microsoft.com/en-us/training/modules/describe-ediscovery-capabilities-of-microsoft-365/3-describe-audit-solutions?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-compliance-solutions>

upvoted 1 times

 **zellck** 11 months ago

YNY is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-premium?view=o365-worldwide#mailitemsaccessed>

The MailItemsAccessed event is a mailbox auditing action and is triggered when mail data is accessed by mail protocols and mail clients. This event can help investigators identify data breaches and determine the scope of messages that may have been compromised. If an attacker gained access to email messages, the MailItemsAccessed action will be triggered even if there's no explicit signal that messages were actually read (in other words, the type of access such as a bind or sync is recorded in the audit record).

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview?view=o365-worldwide#comparison-of-key-capabilities>

upvoted 1 times

 **zellck** 11 months ago

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-premium?view=o365-worldwide#high-bandwidth-access-to-the-office-365-management-activity-api>

With the release of Audit (Premium), we're moving from a publisher-level limit to a tenant-level limit. The result is that each organization will get their own fully allocated bandwidth quota to access their auditing data. The bandwidth isn't a static, predefined limit but is modeled on a combination of factors including the number of seats in the organization and that E5/A5/G5 organizations will get more bandwidth than non-E5/A5/G5 organizations.

upvoted 1 times

Question #90

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input checked="" type="radio"/>
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input type="radio"/>	<input type="radio"/>

Box 1: No -

Box 2: Yes -

Leaked Credentials indicates that the user's valid credentials have been leaked.

Box 3: Yes -

Multi-Factor Authentication can be required based on conditions, one of which is user risk.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

 Igab Highly Voted  2 years, 7 months ago

The third question I think is YES

"These risk detections can trigger actions such as requiring users to provide multifactor authentication, reset their password, or block access until an administrator takes action."

<https://docs.microsoft.com/en-us/learn/modules/describe-identity-protection-governance-capabilities/5-describe-azure?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-identity-access-management-solutions>
upvoted 18 times

 RH10 Highly Voted  2 years, 7 months ago

Answer is No, Yes, Yes :<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>
upvoted 11 times

 Lorenz1974 Most Recent  7 months ago

NYY

<https://learn.microsoft.com/en-us/training/modules/describe-identity-protection-governance-capabilities/5-describe-azure?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-identity-access-management-solutions>
upvoted 1 times

 zellck 11 months ago

Same as Question 135.

<https://www.examtopics.com/discussions/microsoft/view/93652-exam-sc-900-topic-1-question-135-discussion>

upvoted 2 times

 **zellck** 11 months ago

NYY is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#nonpremium-user-risk-detections>
- Leaked credentials

This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they're checked against Azure AD users' current valid credentials to find valid matches.

upvoted 1 times

 **zellck** 11 months ago

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#sign-in-risk-based-conditional-access-policy>

During each sign-in, Identity Protection analyzes hundreds of signals in real-time and calculates a sign-in risk level that represents the probability that the given authentication request isn't authorized. This risk level then gets sent to Conditional Access, where the organization's configured policies are evaluated. Administrators can configure sign-in risk-based Conditional Access policies to enforce access controls based on sign-in risk, including requirements such as:

- Block access
- Allow access
- Require multifactor authentication

upvoted 1 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 2 times

 **NawafAli** 2 years, 1 month ago

For third question, I think it should be No.

- Bcoz, 1. I know you can use User risk level condition in CA to enforce MFA but no way i can relate the 3rd point talking about CA.
2. In Azure Identity protection, for User risk (High, medium or Low) we only have 2 options either block access or allow access with password change.
3. User risk indicates Identity is compromised, hence its best reset the password rather than doing MFA.

upvoted 1 times

 **datahop** 1 year, 4 months ago

it is yes, because: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

The following three policies are available in Azure AD Identity Protection to protect users and respond to suspicious activity. You can choose to turn the policy enforcement on or off, select users or groups for the policy to apply to, and decide if you want to block access at sign-in or prompt for additional action.

User risk policy

Identifies and responds to user accounts that may have compromised credentials. Can prompt the user to create a new password.

Sign in risk policy

Identifies and responds to suspicious sign-in attempts. Can prompt the user to provide additional forms of verification using Azure AD Multi-Factor Authentication.

MFA registration policy

Makes sure users are registered for Azure AD Multi-Factor Authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Azure AD Multi-Factor Authentication.

upvoted 4 times

 **sas000** 2 years, 2 months ago

I believe given answer is correct as first one is for protection not adding users creation

NYY

upvoted 5 times

 **CodexFT** 2 years, 2 months ago

Correct. The last on is YES - the user risk can trigger different Conditional Access policies, like MFA, change password, etc. (tested on my tenant)

upvoted 5 times

 **alopezme** 2 years, 5 months ago

"Require MFA for users with medium or high sign-in risk"

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>

So last one is YES

upvoted 3 times

 **hapai** 2 years, 8 months ago

for the third question I feel it is Y : "Organizations can choose to block access when risk is detected. Blocking sometimes stops legitimate users from doing what they need to. A better solution is to allow self-remediation using Azure AD Multi-Factor Authentication (MFA) and self-service password reset (SSPR)."

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

upvoted 3 times

 **Cookiekaikai** 2 years, 8 months ago

Should be N, Y, N

user risk policy access control requires password change

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#user-risk-with-conditional-access>

upvoted 5 times

✉  **Alvaroll** 1 year, 7 months ago

It's a tricky question because like you said it require to change the password, but changing the password needs MFA validation.
I think they want to us to say NO, because is "Sign-in risk" which can invoke MFA.

When a user risk policy triggers:

Administrators can require a secure password reset, requiring Azure AD MFA be done before the user creates a new password with SSPR, resetting the user risk.

When a sign-in risk policy triggers:

Azure AD MFA can be triggered, allowing the user to prove it's them by using one of their registered authentication methods, resetting the sign-in risk.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

upvoted 1 times

Question #91

Topic 1

Which Microsoft 365 compliance center feature can you use to identify all the documents on a Microsoft SharePoint Online site that contain a specific key word?

- A. Audit
- B. Compliance Manager
- C. Content Search
- D. Alerts

Correct Answer: C

The Content Search tool in the Security & Compliance Center can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and

OneDrive locations, and instant messaging conversations in Skype for Business.

The first step is to start using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365-worldwide>

Community vote distribution

C (100%)

 **Ford_658** Highly Voted  2 years, 7 months ago

Correct

upvoted 12 times

 **Breino** Highly Voted  2 years, 8 months ago

Correct

upvoted 6 times

 **Lorenz1974** Most Recent  7 months ago

Selected Answer: C

Content Search. Use the Content search tool TO SEARCH FOR CONTENT ACROSS MICROSOFT 365 DATA SOURCES and then export the search results to a local computer.

<https://learn.microsoft.com/en-us/training/modules/describe-ediscovery-capabilities-of-microsoft-365/2-describe-ediscovery-solutions?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-compliance-solutions>
upvoted 1 times

 **manofsteel9** 10 months ago

Selected Answer: C

correct answer.

upvoted 1 times

 **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/ediscovery-content-search?view=o365-worldwide>
You can use the Content search eDiscovery tool in the Microsoft Purview compliance portal to search for in-place content such as email, documents, and instant messaging conversations in your organization. Use this tool to search for content in these cloud-based Microsoft 365 data sources:

- Exchange Online mailboxes
 - SharePoint Online sites and OneDrive for Business accounts
 - Microsoft Teams
 - Microsoft 365 Groups
 - Yammer Groups
- upvoted 1 times

 **XtraWest** 11 months, 1 week ago

From eDiscovery case, you can create a new content search and add the keyword you want to search for.

upvoted 1 times

 **RDIO** 1 year, 2 months ago

Selected Answer: C

correct

upvoted 3 times

 **yonie** 1 year, 3 months ago

Selected Answer: C

Content Search

upvoted 3 times

 **Tanzy360** 1 year, 6 months ago

Selected Answer: C

Content Search is correct

upvoted 3 times

 **kingrouj** 2 years, 7 months ago

correct

upvoted 4 times

Question #92

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Defender
The Microsoft 365 compliance center
The Microsoft Defender portal
Microsoft Endpoint Manager

provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.

Correct Answer:

Answer Area

Azure Defender
The Microsoft 365 compliance center
The Microsoft Defender portal
Microsoft Endpoint Manager

provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.

Reference:

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

 **Cooljoy7777** Highly Voted  1 year, 4 months ago

They have change the name to Microsoft Purview compliance portal
upvoted 9 times

 **yonie** Highly Voted  1 year, 3 months ago

Microsoft Purview compliance portal
upvoted 8 times

 **frych** Most Recent  3 months, 2 weeks ago

B.
now it is called: Microsoft Purview Compliance Portal
upvoted 1 times

 **Lorenz1974** 7 months ago

Now "Microsoft Purview Compliance Portal"

<https://learn.microsoft.com/en-us/training/modules/describe-compliance-management-capabilities-microsoft-365/2-describe-compliance-portal?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.describe-capabilities-of-microsoft-compliance-solutions>
upvoted 1 times

 **XtraWest** 11 months, 1 week ago

Microsoft Purview (compliance.microsoft.com)
upvoted 1 times

 **Mapz** 1 year, 4 months ago

Microsoft Purview compliance portal
upvoted 5 times

Question #93

Topic 1

Which Microsoft 365 feature can you use to restrict users from sending email messages that contain lists of customers and their associated credit card numbers?

- A. retention policies
- B. data loss prevention (DLP) policies
- C. conditional access policies
- D. information barriers

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

Community vote distribution

B (100%)

✉  **billo86**  1 year, 11 months ago

Selected Answer: B

correct

upvoted 7 times

✉  **manofsteel9**  10 months ago

Selected Answer: B

of course DLP

upvoted 1 times

✉  **zellck** 11 months ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies.

upvoted 1 times

✉  **Tanzy360** 1 year, 6 months ago

Selected Answer: B

DLP is the only answer that makes sense and is correct

upvoted 4 times

✉  **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

✉  **Contactfornitish** 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 4 times

✉  **Aashiq1** 2 years, 3 months ago

correct

upvoted 4 times

✉  **wyindualizer** 2 years, 5 months ago

correct

upvoted 4 times

Question #94

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Customer Lockbox
Information barriers
Privileged Access Management (PAM)
Sensitivity labels

can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Correct Answer:**Answer Area**

Customer Lockbox
Information barriers
Privileged Access Management (PAM)
Sensitivity labels

can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview>

✉  **wyindualiizer**  2 years, 5 months ago

correct

upvoted 12 times

✉  **Contactfornitish**  2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 5 times

✉  **manofsteel9**  10 months ago

Correct.

upvoted 1 times

✉  **zellck** 11 months ago

"Customer Lockbox" is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide>

Customer Lockbox ensures that Microsoft can't access your content to do service operations without your explicit approval. Customer Lockbox brings you into the approval workflow process that Microsoft uses to ensure only authorized requests allow access to your content.

upvoted 2 times

✉  **IZone** 1 year, 5 months ago

correct!

upvoted 4 times

✉  **Endi99** 1 year, 11 months ago

correct

upvoted 4 times

Question #95

Topic 1

In a Core eDiscovery workflow, what should you do before you can search for content?

- A. Create an eDiscovery hold.
- B. Run Express Analysis.
- C. Configure attorney-client privilege detection.
- D. Export and download results.

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide>

Community vote distributionA (100%)

✉️  **Contactfornitish**  2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 9 times

✉️  **JayBee65**  2 years, 2 months ago

From <https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide>:
Create an eDiscovery hold. The first step after creating a case is placing a hold (also called an eDiscovery hold) on the content locations of the people of interest in your investigation. ... While this step is optional,...

upvoted 9 times

✉️  **rafaseb**  1 month, 1 week ago

As per some external sources Answer should be A: Create an eDiscovery hold: While placing a hold might be part of your overall data preservation strategy, it's not directly required before running searches in Core eDiscovery. Holds typically aim to prevent data deletion during the discovery process.

upvoted 1 times

✉️  **zellck** 11 months ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/ediscovery-standard-get-started?view=o365-worldwide#explore-the-ediscovery-standard-workflow>

upvoted 1 times

✉️  **palito1980** 1 year, 4 months ago

Selected Answer: A

Not exactly true. Content search can be run without the hold in place but it is the best answer you can provide

upvoted 4 times

✉️  **dendep** 9 months, 1 week ago

eDiscovery differs from Content search. eDiscovery search feature is generally used to identify content (including content on hold) to be exported and presented to a legal counsel as potential evidence. A content search tool, however, does not provide any legal or administrative capabilities like eDiscovery

upvoted 2 times

✉️  **Tanzy360** 1 year, 6 months ago

Selected Answer: A

Create an eDiscovery Hold is the correct answer

upvoted 5 times

✉️  **riyaza** 1 year, 10 months ago

eDiscovery Hold is the right answer

upvoted 2 times

✉️  **sandeep86** 1 year, 10 months ago

Create an eDiscovery Hold.

upvoted 2 times

✉️  **wyindualizer** 2 years, 5 months ago

correct

upvoted 4 times

Question #96

Topic 1

Which Microsoft portal provides information about how Microsoft manages privacy, compliance, and security?

- A. Microsoft Service Trust Portal
- B. Compliance Manager
- C. Microsoft 365 compliance center
- D. Microsoft Support

Correct Answer: A

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide>

Community vote distribution

A (100%)

 **Contactfornitish** Highly Voted 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 7 times

 **sas000** Highly Voted 2 years, 2 months ago

key word is portal, trust as well , answer is correct

upvoted 6 times

 **zellck** Most Recent 11 months ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide>

The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

upvoted 1 times

 **obaali1990** 1 year, 1 month ago

What is the basic differences between the Trust portal and the Purview (Ms 365 compliance) portal?

upvoted 3 times

 **Nail** 1 year, 2 months ago

Selected Answer: A

Correct

upvoted 2 times

 **Tanzy360** 1 year, 6 months ago

Trust portal is the correct answer, privacy:trust

upvoted 4 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 1 times

 **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 2 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 3 times

 **ShamimKamar** 1 year, 9 months ago

The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about Microsoft security, privacy, and compliance practices.

upvoted 4 times

 **aims123456** 2 years, 4 months ago

keyword is privacy = Trust

upvoted 4 times

wyindualiizer 2 years, 5 months ago
correct
upvoted 2 times

Question #97

Topic 1

What can you protect by using the information protection solution in the Microsoft 365 compliance center?

- A. computers from zero-day exploits
- B. users from phishing attempts
- C. files from malware and viruses
- D. sensitive data from being exposed to unauthorized users

Correct Answer: D

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide>

Community vote distribution

D (100%)

wyindualiizer **Highly Voted** 2 years, 5 months ago
correct
upvoted 14 times

Contactfornitish **Highly Voted** 2 years, 1 month ago
Appeared in exam on 12/02/2022
upvoted 8 times

zellck **Most Recent** 11 months ago
Selected Answer: D
D is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide>
upvoted 1 times

cris_exam 1 year, 2 months ago
Selected Answer: D
D is correct
upvoted 4 times

Tanzy360 1 year, 6 months ago
Selected Answer: D
Information protection so those who don't need the information won't have it
D is correct
upvoted 3 times

johnegil 1 year, 8 months ago
Appeared on exam 12/07/2022
upvoted 2 times

Question #98

Topic 1

What can you specify in Microsoft 365 sensitivity labels?

- A. how long files must be preserved
- B. when to archive an email message
- C. which watermark to add to files
- D. where to store files

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

Community vote distribution

C (100%)

✉️  **Contactfornitish**  2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 9 times

✉️  **[Removed]**  2 years, 4 months ago

Correct

upvoted 9 times

✉️  **manofsteel9**  10 months ago

This is a tricky question for me.

Both A and C should be the right answer, not only C.

Part of the labels functions is to specify when this content cannot be available anymore. which is option A. I am missing something here!

upvoted 2 times

✉️  **jaaake** 9 months, 1 week ago

Yes, part of the label's function is to specify as you have explained correctly. However, when the question asks about labels themselves, I would associate that to a watermark, instead of a consequence of that watermark being applied. Hence I would go with C.

upvoted 1 times

✉️  **zellck** 11 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

You can use sensitivity labels to:

- Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

upvoted 1 times

✉️  **Tanzy360** 1 year, 6 months ago

Selected Answer: C

Creating classification for sensitive information/data

C is correct

upvoted 5 times

✉️  **NishanthTech90** 1 year, 6 months ago

This question came on 04/09/2022

upvoted 1 times

Question #99

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	<input type="radio"/>	<input type="radio"/>
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	<input type="radio"/>	<input type="radio"/>
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	<input type="radio"/>	<input checked="" type="radio"/>
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	<input type="radio"/>	<input checked="" type="radio"/>
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No -

Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention.

Box 2: No -

Box 3: Yes -

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide>

 **JohnnyBas** Highly Voted 2 years ago

NNY is correct
upvoted 11 times

 **zellck** Most Recent 11 months ago

NNY

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-premium?view=o365-worldwide#send>
Investigators can use the Send event to identify email sent from a compromised account. The audit record for a Send event contains information about the message, such as when the message was sent, the InternetMessage ID, the subject line, and if the message contained attachments. This auditing information can help investigators identify information about email messages sent from a compromised account or sent by an attacker. Additionally, investigators can use a Microsoft 365 eDiscovery tool to search for the message (by using the subject line or message ID) to identify the recipients the message was sent to and the actual contents of the sent message.

upvoted 1 times

 **zellck** 11 months ago

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-premium?view=o365-worldwide#searchqueryinitiatedexchange>
Investigators can use the SearchQueryInitiatedExchange event to determine if an attacker who may have compromised an account looked for or tried to access sensitive information in the mailbox. The audit record for a SearchQueryInitiatedExchange event contains information such as the actual text of the search query. The audit record also indicates the Outlook environment the search was performed in. By looking at the search queries that an attacker may have performed, an investigator can better understand the intent of the email data that was searched for.

upvoted 1 times

 **JA2018** 2 years, 2 months ago

Shouldn't the answer to part 2 be "Yes"?
upvoted 2 times

 **Randy8** 2 years, 1 month ago

No, "The actual content of the message is not displayed."

<https://docs.microsoft.com/en-ca/learn/modules/describe-ediscovery-capabilities-of-microsoft-365/5b-describe-purpose-value-advanced-auditing>

upvoted 3 times

✉ **jaaake** 9 months, 1 week ago

I am confused about this "Content Explorer Content viewer: Membership in this role group allows you to view the contents of each item in the list. The data classification content viewer role has been pre-assigned to this role group." There is also an alert on that page "Important: These permissions supercede permissions that are locally assigned to the items, which allows viewing of the content."

upvoted 1 times

✉ **jaaake** 9 months, 1 week ago

In other words, without viewing the content how can you express an audit opinion?

upvoted 1 times

✉ **JA2018** 2 years, 2 months ago

<https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide>

upvoted 1 times

✉ **JA2018** 2 years, 2 months ago

Send

The Send event is also a mailbox auditing action and is triggered when a user performs one of the following actions:

Sends an email message

Replies to an email message

Forwards an email message

Investigators can use the Send event to identify email sent from a compromised account. The audit record for a Send event contains information about the message, such as when the message was sent, the InternetMessage ID, the subject line, and if the message contained attachments. This auditing information can help investigators identify information about email messages sent from a compromised account or sent by an attacker. Additionally, investigators can use a Microsoft 365 eDiscovery tool to search for the message (by using the subject line or message ID) to identify the recipients the message was sent to and the actual contents of the sent message.

upvoted 4 times

✉ **[Removed]** 2 years, 4 months ago

Correct

upvoted 2 times

Question #100

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can add a resource lock to an Azure subscription.	<input type="radio"/>	<input type="radio"/>
You can add only one resource lock to an Azure resource.	<input type="radio"/>	<input type="radio"/>
You can delete a resource group containing resources that have resource locks.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
You can add a resource lock to an Azure subscription.	<input checked="" type="radio"/>	<input type="radio"/>
You can add only one resource lock to an Azure resource.	<input type="radio"/>	<input checked="" type="radio"/>
You can delete a resource group containing resources that have resource locks.	<input checked="" type="radio"/>	<input type="radio"/>

 **Aunehwet79** Highly Voted  2 years, 4 months ago

I believe it is YNN

You can't delete a resource group containing locked resources

upvoted 68 times

 **Contactfornitish** Highly Voted  2 years, 1 month ago

Appeared in exam on 12/02/2022

YNN is correct, I scored 1000

upvoted 57 times

 **azhrhsn** Most Recent  2 months, 2 weeks ago

YNN.

In Azure, a resource lock is a setting that can be applied to Azure resources to prevent accidental deletion or modification. It's a feature designed to provide an extra layer of protection, ensuring that critical resources remain safe from unintended changes.

upvoted 1 times

 **TomG** 7 months, 1 week ago

It should be YNN since we can't delete a resource group with resource lock

upvoted 1 times

 **manofsteel9** 10 months ago

YNN.

You can add more than one resource lock to an Azure resource. According to the Microsoft Learn article1, "You can set locks that prevent either deletions or modifications. In the portal, these locks are called Delete and Read-only. In the command line, these locks are called CanNotDelete and ReadOnly." Therefore, you can apply both a Delete and a Read-only lock to a resource if you want to prevent any changes to it.

You cannot delete a resource group containing resources that have resource locks. According to the Microsoft Learn article1, "If you have a Delete lock on a resource and attempt to delete its resource group, the feature blocks the whole delete operation. Even if the resource group or other resources in the resource group are unlocked, the deletion doesn't happen. You never have a partial deletion."

upvoted 2 times

 **zellck** 11 months, 1 week ago

YNN is the answer.

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

upvoted 1 times

 **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#lock-inheritance>
If you have a Delete lock on a resource and attempt to delete its resource group, the feature blocks the whole delete operation. Even if the resource group or other resources in the resource group are unlocked, the deletion doesn't happen. You never have a partial deletion.
upvoted 1 times

✉ **jqatar** 1 year, 1 month ago

You can't delete a resource group containing locked resources
upvoted 1 times

✉ **luckyiki** 1 year, 2 months ago

YNN is the correct answer
upvoted 1 times

✉ **yonie** 1 year, 3 months ago

YNN is the correct answer
upvoted 3 times

✉ **TomGray1989** 1 year, 3 months ago

A couple of months ago I tried to delete a resource group with a resource lock in it. It would not allow this action. YNN is correct.
upvoted 4 times

✉ **Tanzy360** 1 year, 6 months ago

YNN, can't delete a locked resource
upvoted 1 times

✉ **cantbeme** 1 year, 7 months ago

on exam today
upvoted 1 times

✉ **Yelad** 1 year, 8 months ago

On the exam 10/07/2022
upvoted 5 times

✉ **kah1** 1 year, 11 months ago

YNN. Proof :
"If you have a Delete lock on a resource and attempt to delete its resource group, the whole delete operation is blocked. Even if the resource group or other resources in the resource group aren't locked, the deletion doesn't happen. You never have a partial deletion."
source : <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>
upvoted 8 times

✉ **billo86** 1 year, 11 months ago

YNN is the answer. How can you delete a group with a lock on it?
upvoted 5 times

the lock is not on the group but rather on a resource in a resource group.

upvoted 1 times

✉ **Contactfornitish** 2 years, 1 month ago

Why would someone select YES for third one? You can't delete a resource group without deleting resources inside it and you can't delete a resource with a lock (otherwise what's purpose)
upvoted 1 times

✉ **AnujN** 2 years, 1 month ago

Y N N is the correct answer.
upvoted 2 times

Question #101

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Users can apply sensitivity labels manually.	<input type="radio"/>	<input type="radio"/>
Multiple sensitivity labels can be applied to the same file.	<input type="radio"/>	<input type="radio"/>
A sensitivity label can apply a watermark to a Microsoft Word document.	<input type="radio"/>	<input type="radio"/>

Correct Answer:**Answer Area**

Statements	Yes	No
Users can apply sensitivity labels manually.	<input checked="" type="radio"/>	<input type="radio"/>
Multiple sensitivity labels can be applied to the same file.	<input type="radio"/>	<input checked="" type="radio"/>
A sensitivity label can apply a watermark to a Microsoft Word document.	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide>

✉  **wyindualiizer** Highly Voted 2 years, 5 months ago

correct

upvoted 22 times

✉  **Contactfornitish** Highly Voted 2 years, 1 month ago

Appeared in exam on 12/02/2022

upvoted 10 times

✉  **manofsteel9** Most Recent 10 months ago

Correct answer. YNY

You can apply only one sensitivity label to a file. According to the Microsoft Learn article1, "You can apply a sensitivity label to a file or email, but not more than one label. If you try to apply a second label, you're prompted to replace the existing label." Sensitivity labels are used to classify and protect your organization's data based on its sensitivity level.

upvoted 1 times

✉  **zellck** 11 months, 1 week ago

YNY is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-label-policies-can-do>

For documents and emails, a label can be assigned manually by the user, automatically as a result of a condition that you configure, or be assigned by default (the default label option previously described).

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

You can use sensitivity labels to:

- Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

upvoted 1 times

✉  **Lidruj** 11 months, 2 weeks ago

YNY is correct

upvoted 1 times

✉  **Lidruj** 11 months, 2 weeks ago

I Mean YNY ..Sorry
upvoted 1 times

 **StressFree** 12 months ago

Each item that supports sensitivity labels can have a single sensitivity label applied to it. Documents and emails can have both a sensitivity label and a retention label applied to them.

don't confuse SENSITIVE label with RETENTION label. The question says sensitive, and it's only one per item.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

upvoted 2 times

 **Tanzy360** 1 year, 6 months ago

Correct answer, data classification for sensitivity can add watermarks

upvoted 3 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 4 times

 **sas000** 2 years, 2 months ago

correct I passed today above 900 almost same questions

upvoted 6 times

 **sas000** 2 years, 2 months ago

correct answer

upvoted 4 times

 **JayBee65** 2 years, 2 months ago

"Each item that supports sensitivity labels can have a single sensitivity label applied to it. " From: <https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

upvoted 5 times

 **Khumo** 2 years, 4 months ago

Correcto

upvoted 3 times

 **yulexam** 2 years, 4 months ago

yes...correct...

upvoted 3 times

 **dadageer** 2 years, 4 months ago

Correct

upvoted 3 times

Question #102

Topic 1

Which two tasks can you implement by using data loss prevention (DLP) policies in Microsoft 365? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Display policy tips to users who are about to violate your organization's policies.
- B. Enable disk encryption on endpoints.
- C. Protect documents in Microsoft OneDrive that contain sensitive information.
- D. Apply security baselines to devices.

Correct Answer: AC

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

Community vote distribution

AC (100%)

 **Melwin86** Highly Voted 2 years, 8 months ago

correct

upvoted 16 times

 **Tanzy360** Highly Voted 1 year, 6 months ago

Selected Answer: AC

AC are both correct

upvoted 6 times

 **manofsteel9** Most Recent 10 months ago

Selected Answer: AC

Correct.

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: AC

AC is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide#protective-actions-of-dlp-policies>
DLP policies are how you monitor the activities that users take on sensitive items at rest, sensitive items in transit, or sensitive items in use and take protective actions. For example, when a user attempts to take a prohibited action, like copying a sensitive item to an unapproved location or sharing medical information in an email or other conditions laid out in a policy, DLP can:

- show a pop-up policy tip to the user that warns them that they may be trying to share a sensitive item inappropriately

upvoted 1 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: AC

AC Correct

upvoted 2 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 1 times

 **Tumi21** 1 year, 9 months ago

AC - correct

upvoted 1 times

 **devilcried** 1 year, 9 months ago

Selected Answer: AC

correct

upvoted 3 times

 **devilcried** 1 year, 10 months ago

Selected Answer: AC

Correct

upvoted 3 times

□  **TJ001** 2 years, 2 months ago

DLP is more on apps we are using on devices ; hence correct answers
upvoted 3 times

Question #103

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Compliance Manager assesses compliance data for an organization.

continually
monthly
on-demand
quarterly

Answer Area

Compliance Manager assesses compliance data for an organization.

Correct Answer:

continually
monthly
on-demand
quarterly

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide#how-compliance-manager-continuously-assesses-controls>

□  **Melwin86**  2 years, 8 months ago

correct

upvoted 14 times

□  **zellck**  11 months, 1 week ago

"continually" is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide#how-compliance-manager-continuously-assesses-controls>

upvoted 2 times

□  **ant_man** 1 year, 7 months ago

Appeared last week (July)-Correct

upvoted 2 times

□  **Cereb7** 1 year, 11 months ago

Viewing last no provided it is correct.

upvoted 1 times

□  **Gringusss** 2 years, 1 month ago

I Agree

upvoted 2 times

Question #104

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	<input type="radio"/>	<input type="radio"/>
Sensitivity labels can add headers and footers to documents.	<input type="radio"/>	<input type="radio"/>
Sensitivity labels can apply watermarks to emails.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity labels can add headers and footers to documents.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity labels can apply watermarks to emails.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

You can use sensitivity labels to provide protection settings that include encryption of emails and documents to prevent unauthorized people from accessing this data.

Box 2: Yes -

You can use sensitivity labels to mark the content when you use Office apps, by adding watermarks, headers, or footers to documents that have the label applied.

Box 3: Yes -

You can use sensitivity labels to mark the content when you use Office apps, by adding headers, or footers to email that have the label applied.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

 **FableFa** Highly Voted 2 years, 8 months ago

For me, wrong Answer. Correct answer is YES-YES-NO because you can't apply water mark to an email, only to documents in Word, Excel and Powerpoint. <https://docs.microsoft.com/en-us/information-protection/deploy-use/configure-policy-markings>

upvoted 67 times

 **ant_man** 1 year, 7 months ago

Appeared last week (July)-Correct

upvoted 2 times

 **najwa** Highly Voted 2 years, 8 months ago

yes yes no ,

Watermarks can be applied to documents but not to email.

upvoted 31 times

 **Clouddog** 1 year, 11 months ago

correct: Watermarks can be applied to documents but not email.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

upvoted 3 times

 **Ramye** Most Recent 3 months ago

Answer is YYN

Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label

applied. Watermarks can be applied to documents but not email or meeting invites. Example header and watermark:

Source: <https://learn.microsoft.com/en-us/purview/sensitivity-labels>

upvoted 1 times

tc_praveen 3 months, 1 week ago

YYY

You can configure a sensitivity label to:

Encrypt emails, meeting invites, and documents to prevent unauthorized people from accessing this data. ...

Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied.

...•15 Nov 2023

upvoted 1 times

Akacokie 5 months ago

YYN

"Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied. Watermarks can be applied to documents but not email or meeting invites. Example header and watermark:"

<https://learn.microsoft.com/en-us/purview/sensitivity-labels?view=o365-worldwide>

upvoted 1 times

Tarnum 5 months ago

To me all are correct so Y-Y-Y

<https://support.microsoft.com/en-us/office/apply-sensitivity-labels-to-your-files-and-email-2f96e7cd-d5a4-403b-8bd7-4cc636bae0f9>

upvoted 1 times

Curious76 7 months ago

Y

sensitivity labels can potentially be used to apply watermarks to emails, depending on the capabilities of the software or system you are using.

upvoted 2 times

dsharp 8 months, 1 week ago

YYN

You cannot apply watermarks to emails

upvoted 1 times

lilou123 9 months ago

You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark

upvoted 2 times

manofsteel9 10 months ago

Wrong, correct answer is YYN:

<https://docs.microsoft.com/en-us/information-protection/deploy-use/configure-policy-markings>

"In Word and PowerPoint, the label applies the watermark text "This content is Confidential". In Excel, the label applies the watermark text "Confidential". In Outlook, the label doesn't apply any watermark text because watermarks as visual markings are not supported for Outlook."

upvoted 1 times

zellck 11 months, 1 week ago

YYN is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

You can use sensitivity labels to:

- Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

upvoted 1 times

zellck 11 months, 1 week ago

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-a-sensitivity-label-is>

Each item that supports sensitivity labels can have a single sensitivity label applied to it. Documents and emails can have both a sensitivity label and a retention label applied to them.

upvoted 2 times

Lidruj 11 months, 2 weeks ago

answer is YYN

upvoted 1 times

ARM360 11 months, 3 weeks ago

Yes, Yes, Yes

Its now Microsoft Purview Information Protection

You can use sensitivity labels to:

Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

upvoted 7 times

 **luckyiki** 1 year, 2 months ago

From:

<https://docs.microsoft.com/en-us/information-protection/deploy-use/configure-policy-markings>

"Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied. Watermarks can be applied to documents but not email or meeting invites."

upvoted 1 times

 **palito1980** 1 year, 4 months ago

Y,Y,N

Sensitivity labels cannot watermark emails.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-sensitivity-labels-can-do>

upvoted 2 times

 **Tanzy360** 1 year, 6 months ago

Watermarks are for documents not emails

YYN is correct

upvoted 4 times

 **kb95** 1 year, 7 months ago

Mark the content when you use Office apps, by adding watermarks, headers, or footers to email or documents that have the label applied.

Watermarks can be applied to documents but not email. Yes, Yes, No

upvoted 1 times

Question #105

Topic 1

Which Microsoft 365 compliance feature can you use to encrypt content automatically based on specific conditions?

- A. Content Search
- B. sensitivity labels
- C. retention policies
- D. eDiscovery

Correct Answer: B

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide>

Community vote distribution

 B (100%)

 **Andrephv**  2 years, 8 months ago

Correcto

upvoted 19 times

 **Beng_ali**  2 years, 2 months ago

Selected Answer: B

Correct Answer is B

upvoted 6 times

 **Tahamaffia**  6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 2 times

 **manofsteel9** 10 months ago

Selected Answer: B

B is the answer.

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

You can use sensitivity labels to:

- Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content.

upvoted 1 times

 **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-sensitivity-labels-can-do>

- Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied. Watermarks can be applied to documents but not email or meeting invites.

upvoted 1 times

 **IZone** 1 year, 5 months ago

correct

upvoted 3 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 1 times

 **ant_man** 1 year, 7 months ago

Selected Answer: B

Appear last week.

upvoted 2 times

 **MorningStar74** 1 year, 8 months ago

Selected Answer: B

yes, correct

upvoted 3 times

 **Yelad** 1 year, 8 months ago

On the exam 10/07/2022

upvoted 3 times

 **Endi99** 1 year, 11 months ago

Selected Answer: B

Correct

upvoted 4 times

Question #106

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls.	<input type="radio"/>	<input type="radio"/>
Compliance Manager provides predefined templates for creating assessments.	<input type="radio"/>	<input type="radio"/>
Compliance Manager can help you assess whether data adheres to specific data protection standards.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls.	<input type="radio"/>	<input checked="" type="radio"/>
Compliance Manager provides predefined templates for creating assessments.	<input checked="" type="radio"/>	<input type="radio"/>
Compliance Manager can help you assess whether data adheres to specific data protection standards.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No -

Compliance Manager tracks Microsoft managed controls, customer-managed controls, and shared controls.

Box 2: Yes -

Box 3: Yes -

Reference:

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

 [Removed]  2 years, 4 months ago

Correct!

upvoted 15 times

 Yelad  1 year, 8 months ago

On the exam 10/07/2022

upvoted 5 times

 zellck  11 months, 1 week ago

NYY is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide#controls>

Compliance Manager tracks the following types of controls:

- Microsoft managed controls: controls for Microsoft cloud services, which Microsoft is responsible for implementing
- Your controls: sometimes referred to as customer managed controls, these are controls implemented and managed by your organization
- Shared controls: these are controls that both your organization and Microsoft share responsibility for implementing

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide#templates>

Compliance Manager provides over 350 templates to help you quickly create assessments.

upvoted 1 times

 zellck 11 months, 1 week ago

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide#understanding-your-compliance-score>

Compliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance.

upvoted 1 times

 **IZone** 1 year, 5 months ago

Correct!

upvoted 4 times

 **cantbeme** 1 year, 7 months ago

on exam today

upvoted 2 times

 **Dcsam** 2 years ago

Correct

upvoted 4 times

Question #107

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can use the insider risk management solution to detect phishing scams.	<input type="radio"/>	<input type="radio"/>
You can access the insider risk management solution from the Microsoft 365 compliance center.	<input type="radio"/>	<input type="radio"/>
You can use the insider risk management solution to detect data leaks by unhappy employees.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
You can use the insider risk management solution to detect phishing scams.	<input type="radio"/>	<input checked="" type="radio"/>
You can access the insider risk management solution from the Microsoft 365 compliance center.	<input checked="" type="radio"/>	<input type="radio"/>
You can use the insider risk management solution to detect data leaks by unhappy employees.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No -

Phishing scams are external threats.

Box 2: Yes -

Insider risk management is a compliance solution in Microsoft 365.

Box 3: Yes -

Insider risk management helps minimize internal risks from users. These include:

- ⇒ Leaks of sensitive data and data spillage
- ⇒ Confidentiality violations
- ⇒ Intellectual property (IP) theft
- ⇒ Fraud
- ⇒ Insider trading
- ⇒ Regulatory compliance violations

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide>

✉  **xperience**  1 year, 11 months ago

Correct

upvoted 6 times

✉  **BurningIce6699**  1 year, 7 months ago

I only see 95 questions even though it said there is 104?

upvoted 5 times

✉  **jrenz** 1 year, 7 months ago

me too

upvoted 1 times

✉  **zellick**  11 months, 1 week ago

NYY is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide>

upvoted 1 times

✉  **IXone** 1 year, 5 months ago

Correct

upvoted 3 times

✉  **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected => N Y Y

upvoted 4 times

✉  **cantbeme** 1 year, 7 months ago

on exam today

upvoted 2 times

✉  **ant_man** 1 year, 7 months ago

Appeared last week (July)-Correct

upvoted 1 times

Question #108

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证
微信添加 hello231119

Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	<input type="radio"/>	<input type="radio"/>
Azure Policy can be used to ensure that new resources adhere to corporate standards.	<input type="radio"/>	<input type="radio"/>
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Policy can be used to ensure that new resources adhere to corporate standards.	<input checked="" type="radio"/>	<input type="radio"/>
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

 **Juancho** Highly Voted 2 years, 6 months ago

(Y, Y, N) - Correct

1.- Azure Policy supports automatic remediation (Y) R/=

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity. If the managed identity is missing roles, an error is displayed during the assignment of the policy or an initiative. When using the portal, Azure Policy automatically grants the managed identity the listed roles once assignment starts. When using SDK, the roles must manually be granted to the managed identity. The location of the managed identity doesn't impact its operation with Azure Policy.

upvoted 22 times

 **nipsey** Highly Voted 2 years, 4 months ago

3. N

Understand evaluation outcomes

Resources are evaluated at specific times during the resource lifecycle, the policy assignment lifecycle, and for regular ongoing compliance evaluation. The following are the times or events that cause a resource to be evaluated:

A resource is created, updated, or deleted in a scope with a policy assignment.

A policy or initiative is newly assigned to a scope.

A policy or initiative already assigned to a scope is updated.

During the standard compliance evaluation cycle, which occurs once every 24 hours.

For detailed information about when and how policy evaluation happens, see Evaluation triggers.

upvoted 12 times

 **zellck** Most Recent 11 months, 1 week ago

YYN is the answer.

<https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal>

Resources that are non-compliant to policies with deployIfNotExists or modify effects can be put into a compliant state through Remediation. Remediation is accomplished through remediation tasks that deploy the deployIfNotExists template or the modify operations of the assigned policy on your existing resources and subscriptions, whether that assignment is on a management group, subscription, resource group, or individual resource.

<https://learn.microsoft.com/en-us/azure/governance/policy/overview>

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 1 times

□  **MoneyStacking** 1 year, 2 months ago

Only > is always no

upvoted 4 times

□  **johnegil** 1 year, 8 months ago

Appeared on exam 12/07/2022

upvoted 4 times

□  **AbhiM** 2 years ago

I think answer is correct as per the link given as well.

upvoted 4 times

Question #109

DRAG DROP -

Match the Microsoft 365 insider risk management workflow step to the appropriate task.

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

NOTE: Each correct match is worth one point.

Select and Place:

Steps	Answer Area
Action	Review and filter alerts
Investigate	Create cases in the Case dashboard
Triage	Send a reminder of corporate policies to users

Correct Answer:

Steps	Answer Area
Action	Review and filter alerts
Investigate	Create cases in the Case dashboard
Triage	Send a reminder of corporate policies to users

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide>

 **palito1980** Highly Voted 1 year, 4 months ago

Looks correct following the docs.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide#workflow>

upvoted 5 times

 **zellck** Most Recent 11 months, 1 week ago

Same as Question 155.

<https://www.examtopics.com/discussions/microsoft/view/93683-exam-sc-900-topic-1-question-155-discussion>

upvoted 1 times

 **zellck** 11 months, 1 week ago

1. Triage
2. Investigate
3. Action

<https://learn.microsoft.com/en-us/training/modules/describe-insider-risk-capabilities-microsoft-365/2-management-solution>

Triage - New activities that need investigation automatically generate alerts that are assigned a Needs review status. Reviewers in the organization can quickly identify these alerts and scroll through each to evaluate and triage. As part of the triage process, reviewers can view alert details for the policy match, view user activity associated with the match, see the severity of the alert, and review user profile information.

Investigate - Cases are created for alerts that require deeper review and investigation of the details and circumstances around the policy match. The Case dashboard provides an all-up view of all active cases, open cases over time, and case statistics for the organization.

Action - After cases are investigated, reviewers can quickly act to resolve the case or collaborate with other risk stakeholders in the organization.

upvoted 2 times

 **KingChuang** 1 year, 6 months ago

Correct.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide>

upvoted 4 times

Question #110

Topic 1

Which two cards are available in the Microsoft 365 Defender portal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Devices at risk
- B. Compliance Score
- C. Service Health
- D. User Management
- E. Users at risk

Correct Answer: AE

A: The Devices at risk card includes a View details button. Selecting that button takes us to the Device inventory page, as shown in the following image

Device ...	Domain	Risk level	Exposure level	OS platform	Windows 10 versions	Health state	Onboarding sta...
device2	Workgroup	High	Low	Windows 10	Future	Active	Onboarded
smbprod...	Workgroup	Informational	Medium	Windows 10	Future	Inactive	Onboarded
smbprod...	Workgroup	Informational	Low	Windows 10	Future	Active	Onboarded

E: The Microsoft 365 Defender portal cards fall into these categories:

Identities- Monitor the identities in your organization and keep track of suspicious or risky behaviors. Here you can find the Users at risk card.

Data - Help track user activity that could lead to unauthorized data disclosure.

Devices - Get up-to-date information on alerts, breach activity, and other threats on your devices.

Apps - Gain insight into how cloud apps are being used in your organization.

Incorrect:

Not C: The Service Health card can be reached from the Microsoft 365 admin center.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-respond-mitigate-threats>

Community vote distribution

AE (100%)

Woli 1 year, 6 months ago

Selected Answer: AE

AE looks like correct answer.

Notice cards on the Home page. Cards tell you at a glance how many threats were detected, along with how many user accounts, endpoints (devices), and other assets were affected. The following image is an example of cards you might see:

From: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-respond-mitigate-threats?view=o365-worldwide>
upvoted 7 times

k_16 10 months ago

Correct! AE

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: AE

AE is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-respond-mitigate-threats?view=o365-worldwide>

Notice cards on the Home page. Cards tell you at a glance how many threats were detected, along with how many user accounts, endpoints (devices), and other assets were affected.

upvoted 1 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: AE

AE Correct

upvoted 2 times

 **Klown** 1 year, 2 months ago

AE is correct

upvoted 2 times

Question #111

Topic 1

What should you use to ensure that the members of an Azure Active Directory group use multi-factor authentication (MFA) when they sign in?

- A. Azure role-based access control (Azure RBAC)
- B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- C. Azure Active Directory (Azure AD) Identity Protection
- D. a conditional access policy

Correct Answer: D

Community vote distribution

D (100%)

 **manofsteel9** 10 months ago

Selected Answer: D

D is the answer.
upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>
upvoted 3 times

 **AAsif098** 1 year, 2 months ago

Selected Answer: D

Conditional Access is a feature in Azure AD that allows you to create policies that are used to control access to Azure AD-connected resources. These policies can be based on a variety of factors, such as the user's location, device state, and sign-in risk.
upvoted 4 times

 **ETU69** 1 year, 3 months ago

Selected Answer: D

For more granular controls, you can use Conditional Access policies to define events or applications that require MFA.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks#how-to-enable-and-use-azure-ad-multi-factor-authentication>
upvoted 4 times

 **RodrigoAB** 1 year, 6 months ago

Selected Answer: D

The recommended way to enable and use Azure AD Multi-Factor Authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign-in events and that request additional actions before a user is granted access to an application or service.

Information: Microsoft Site!

upvoted 3 times

Question #112

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection generates risk detections once a user is authenticated.	<input type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	<input type="radio"/>	<input type="radio"/>
A user risk in Azure Active Directory (Azure AD) Identity Protection represents the probability that a given identity or account is compromised.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection generates risk detections once a user is authenticated.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Active Directory (Azure AD) Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	<input checked="" type="radio"/>	<input type="radio"/>
A user risk in Azure Active Directory (Azure AD) Identity Protection represents the probability that a given identity or account is compromised.	<input checked="" type="radio"/>	<input type="radio"/>

 OrangeSG Highly Voted  1 year, 3 months ago

Box 1: Yes

Identity Protection generates risk detections only when the correct credentials are used. If incorrect credentials are used on a sign-in, it does not represent risk of credential compromise.

Box 2: Yes

Identity Protection categorizes risk into three tiers: low, medium, and high. When configuring Identity protection policies, you can also configure it to trigger upon No risk level. No Risk means there's no active indication that the user's identity has been compromised.

Box 3: Yes

Each level of risk brings higher confidence that the user or sign-in is compromised. For example, something like one instance of unfamiliar sign-in properties for a user might not be as threatening as leaked credentials for another user.

Reference

What is risk?

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 12 times

 zellck Most Recent  11 months, 1 week ago

YYY is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#risk-levels>
Identity Protection categorizes risk into tiers: low, medium, and high.

Microsoft doesn't provide specific details about how risk is calculated. Each level of risk brings higher confidence that the user or sign-in is compromised. For example, something like one instance of unfamiliar sign-in properties for a user might not be as threatening as leaked credentials for another user.

upvoted 1 times

 zellck 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/describe-identity-protection-governance-capabilities/5-describe-azure>

Identity Protection only generates risk detections when correct credentials are used in the authentication request. If a user uses incorrect credentials, it will not be flagged by Identity Protection since there isn't a risk of credential compromise unless a bad actor uses the correct credentials.

Identity Protection categorizes risk into three tiers: low, medium, and high. It can also calculate the sign-in risk, and user identity risk.

A user risk represents the probability that a given identity or account is compromised. These risks are calculated offline using Microsoft's internal and external threat intelligence sources.

upvoted 2 times

 **jellybiscuit** 1 year, 6 months ago

Correct

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 4 times

Question #113

Topic 1

You need to keep a copy of all files in a Microsoft SharePoint site for one year, even if users delete the files from the site.

What should you apply to the site?

- A. a retention policy
- B. an insider risk policy
- C. a data loss prevention (DLP) policy
- D. a sensitivity label policy

Correct Answer: A

Community vote distribution

A (100%)

 **jellybiscuit** Highly Voted 1 year, 6 months ago

Selected Answer: A

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide#how-retention-works-for-sharepoint-and-onedrive>

upvoted 6 times

 **deep11596** Most Recent 7 months, 2 weeks ago

are these questions are enough to pass the exam? please suggest thanks.

upvoted 1 times

 **manofsteel9** 10 months ago

Selected Answer: A

A. Retention policy.

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide&tabs=teams-retention>

Use a retention policy to manage the data for your organization by deciding proactively whether to retain content, delete content, or retain and then delete the content.

upvoted 1 times

 **AArif098** 1 year, 2 months ago

Selected Answer: A

In order to keep a copy of all files in a Microsoft SharePoint site for one year, even if users delete the files from the site, you should enable the Recycle Bin feature in SharePoint and set the retention period to one year.

upvoted 3 times

 **PinkUnicorns** 1 year, 2 months ago

Selected Answer: A

It is retention - Cheers

upvoted 4 times

 **User_Mowgli** 1 year, 6 months ago

Selected Answer: A

Correct

upvoted 3 times

Question #114

Topic 1

You need to create a data loss prevention (DLP) policy.

What should you use?

- A. the Microsoft 365 Compliance center
- B. the Microsoft Endpoint Manager admin center
- C. the Microsoft 365 admin center
- D. the Microsoft 365 Defender portal

Correct Answer: C

Community vote distribution

A (100%)

 **jellybiscuit**  1 year, 6 months ago

Selected Answer: A

"you can configure DLP policies for all workloads through the Microsoft Purview compliance portal,"

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy>

upvoted 15 times

 **PinkUnicorns**  1 year, 2 months ago

Selected Answer: A

It has been renamed to Purview. So the Answer is A.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/create-a-dlp-policy-from-a-template?view=o365-worldwide>

upvoted 7 times

 **ramonroy**  4 months ago

en examen

upvoted 1 times

 **Darkfire** 8 months, 1 week ago

Selected Answer: A

Defenitely A. the Microsoft 365 Compliance center (Microsoft Purview Compliance Portal)

upvoted 1 times

 **dsharp** 8 months, 1 week ago

Selected Answer: A

The Compliance portal has been rebranded as Microsoft Purview compliance portal and that's where you set up DLP policies

upvoted 1 times

 **dunget** 9 months, 2 weeks ago

Selected Answer: A

To create a data loss prevention (DLP) policy, you can use the Microsoft 365 compliance center or the Microsoft Purview compliance portal. In the Microsoft 365 compliance center, you can navigate to Data loss prevention and then select Policy. From there, you can either create a new policy or edit an existing one. You can then customize the policy settings, such as defining which connectors to include in the Business data group and which connectors to block1. You can also use PowerShell commands to create and manage DLP policies2.

upvoted 2 times

 **Micha338el** 10 months ago

How DLP works between the Compliance portal and Exchange admin center.

In Microsoft Purview, you can create a data loss prevention (DLP) policy in two different admin centers:

In the Microsoft Purview compliance portal, you can create a single DLP policy to help protect content in SharePoint, OneDrive, Exchange, Teams, and now Endpoint Devices. We recommend that you create a DLP policy here. For more information, see Create and Deploy data loss prevention policies.

In the Exchange admin center, you can create a DLP policy to help protect content only in Exchange. This policy can use Exchange mail flow rules (also known as transport rules), so it has more options specific to handling email. For more information, see DLP in the Exchange admin center.

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>
In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies.

upvoted 1 times

 **StressFree** 12 months ago

Microsoft Purview Compliance Portal

upvoted 2 times

 **zxmax01** 1 year, 2 months ago

Selected Answer: A

DLP is a question of Governance and Compliance --> Purview Compliance Center (Answer A)

upvoted 4 times

 **yonie** 1 year, 3 months ago

Selected Answer: A

you can configure DLP policies for all workloads through the Microsoft Purview compliance portal

upvoted 2 times

 **yonie** 1 year, 3 months ago

Selected Answer: A

Microsoft Purview compliance

upvoted 2 times

 **RodrigoAB** 1 year, 5 months ago

Selected Answer: A

DLP = Compliance

upvoted 3 times

 **murrutia** 1 year, 6 months ago

Answer A is the correct answer.

upvoted 1 times

 **Ady_72** 1 year, 6 months ago

"In the Microsoft Purview compliance portal, you'll find the DLP policies under Data loss prevention > Policy. Choose Create a policy to start."

Seems to be A

upvoted 2 times

 **randyruchira** 1 year, 6 months ago

It's A.

upvoted 2 times

 **azeem0077** 1 year, 6 months ago

Selected Answer: A

Which portal do you use to create a DLP?

The easiest, most common way to get started with DLP policies is to use one of the templates included in the Microsoft Purview compliance portal

upvoted 3 times

Question #115

Topic 1

What is an assessment in Compliance Manager?

- A. A policy initiative that includes multiple policies.
- B. A dictionary of words that are not allowed in company documents.
- C. A grouping of controls from a specific regulation, standard or policy.
- D. Recommended guidance to help organizations align with their corporate standards.

Correct Answer: C

Community vote distribution

C (100%)

✉  **palito1980**  1 year, 4 months ago

Selected Answer: C

Definitely C

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide#assessments>
upvoted 7 times

✉  **jellybiscuit**  1 year, 6 months ago

Selected Answer: C

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments>
upvoted 5 times

✉  **Tahamaffia**  6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 1 times

✉  **zellck** 11 months, 1 week ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365-worldwide#introduction-to-assessments>

Compliance Manager helps you create assessments that evaluate your compliance with industry and regional regulations that apply to your organization. Assessments are built upon the framework of assessment templates, which contain the necessary controls, improvement actions, and, where applicable, Microsoft actions for completing the assessment. Setting up the most relevant assessments for your organization can help you implement policies and operational procedures to limit your compliance risk.

upvoted 1 times

✉  **MoneyStacking** 1 year, 2 months ago

Regulation > Compliance

upvoted 5 times

✉  **yonie** 1 year, 3 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide#assessments>

An assessment is grouping of controls from a specific regulation, standard, or policy.

upvoted 4 times

✉  **IZone** 1 year, 5 months ago

Correct

upvoted 3 times

✉  **Goddev** 1 year, 6 months ago

Selected Answer: C

Correct!

upvoted 3 times

Question #116

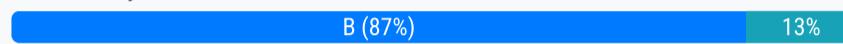
Topic 1

What can you use to view the Microsoft Secure Score for Devices?

- A. Microsoft Defender for Cloud Apps
- B. Microsoft Defender for Endpoint
- C. Microsoft Defender for Identity
- D. Microsoft Defender for Office 365

Correct Answer: B

Community vote distribution



✉ **alashi** 1 year, 4 months ago

Selected Answer: B

DEVICES - endpoint...
upvoted 16 times

✉ **Bartin8tor** 1 year, 3 months ago

Selected Answer: B

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. Forward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture.

So:

MS Defender for Endpoint, and MS 365 defender (if forwarded).
But NOT Defender for O365
upvoted 7 times

✉ **claudioiosa** 2 months, 1 week ago

Selected Answer: B

Endpoint too!!
upvoted 1 times

✉ **CPTeam** 8 months, 1 week ago

Selected Answer: B

DEVICES - endpoint...
upvoted 1 times

✉ **manofsteel9** 10 months ago

Selected Answer: B

B. Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides the capability to view the Microsoft Secure Score for Devices. The Microsoft Secure Score is a measurement of the overall security posture and configuration of devices within an organization. It assesses various security settings, configurations, and best practices to provide a score that represents the level of security and compliance.

upvoted 2 times

✉ **zellck** 11 months, 1 week ago

Selected Answer: B

B is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide>
- Microsoft Secure Score for Devices

Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization.

upvoted 1 times

✉ **XtraWest** 11 months, 1 week ago

Selected Answer: B

Endpoint for Devices
upvoted 1 times

✉ **nikolaost** 1 year, 1 month ago

Selected Answer: B

Defender for Endpoint as it is referring to devices=endpoints

upvoted 3 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: B

"Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal". Microsoft Defender for Endpoint is part of M 365 defender. so B is correct.

upvoted 2 times

 **pviolenta** 1 year, 2 months ago

Selected Answer: B

It is B. I should know as I am the administrator.

upvoted 5 times

 **cris_exam** 1 year, 2 months ago

Selected Answer: B

This one is tricky but the correct answer is B.

Since this is regarding devices, it refers to Endpoints, hence Microsoft Defender for Endpoint, NOT MS Defender for O365.

The below link documentation also confirms in what portals the secure score can be found.

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide#products-included-in-secure-score>

upvoted 5 times

 **yonie** 1 year, 3 months ago

Selected Answer: B

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. == Microsoft Defender for Endpoint

upvoted 1 times

 **oludare** 1 year, 4 months ago

Looks like folks selecting D are confusing Microsoft 365 Defender portal to Microsoft Defender for office 365 (for email etc). They are two separate things. Answer is B.

upvoted 3 times

 **IPERSONIC** 1 year, 4 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-microsoft-secure-score-devices?view=o365-worldwide>

upvoted 1 times

 **BTL_Happy** 1 year, 5 months ago

One will need either 1. Microsoft Defender for Endpoint P2 or M365 E3 and above in order to be able to view Devices and under Microsoft Secure Score.

upvoted 1 times

 **Alitahir** 1 year, 5 months ago

Devices = Endpoint

upvoted 3 times

 **RodrigoAB** 1 year, 5 months ago

Selected Answer: D

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal.

upvoted 4 times

Question #117

Topic 1

DRAG DROP -

Match the Microsoft Defender for Office 365 feature to the correct description.

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

NOTE: Each correct match is worth one point.

Select and Place:

Features	Answer Area
Threat Explorer	Provides intelligence on prevailing cybersecurity issues
Threat Trackers	Provides real-time reports to identify and analyze recent threats
Anti-phishing protection	Detects impersonation attempts

Correct Answer:

Features	Answer Area
Threat Explorer	Provides intelligence on prevailing cybersecurity issues
Threat Trackers	Provides real-time reports to identify and analyze recent threats
Anti-phishing protection	Detects impersonation attempts

louval357 Highly Voted 1 year, 3 months ago

Keywords:

Prevailing = Trackers

Real-time = Explorer

Impersonation = Anti-phishing

upvoted 23 times

yonie 1 year, 3 months ago

Good one

upvoted 6 times

jellybiscuit Highly Voted 1 year, 6 months ago

Correct

Threat tracker

<https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-defender-for-office-365-features#threat-trackers>

Threat Explorer

<https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-defender-for-office-365-features#threat-explorer>

upvoted 7 times

zellck Most Recent 11 months, 1 week ago

1. Threat Trackers

2. Threat Explorer

3. Anti-phishing protection

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/threat-trackers?view=o365-worldwide#what-are-threat-trackers>

Threat Trackers are informative widgets and views that provide you with intelligence on different cybersecurity issues that might impact your company. For example, you can view information about trending malware campaigns using Threat Trackers.

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/threat-explorer-views?view=o365-worldwide>

Threat Explorer (and the real-time detections report) is a powerful, near real-time tool to help Security Operations teams investigate and respond to threats in the Microsoft 365 Defender portal. Explorer (and the real-time detections report) displays information about suspected malware and phish in email and files in Office 365, as well as other security threats and risks to your organization.

upvoted 2 times

zellck 11 months, 1 week ago

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-about?view=o365-worldwide#anti-phishing-protection-in-eop>

EOP (that is, Microsoft 365 organizations without Microsoft Defender for Office 365) contains features that can help protect your organization from phishing threats:

- Spoof intelligence: Use the spoof intelligence insight to review detected spoofed senders in messages from external and internal domains, and manually allow or block those detected senders.

upvoted 1 times

Question #118

Topic 1

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Each network security group (NSG) rule must have a unique name.	<input type="radio"/>	<input type="radio"/>
Network security group (NSG) default rules can be deleted.	<input type="radio"/>	<input type="radio"/>
Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Each network security group (NSG) rule must have a unique name.	<input checked="" type="radio"/>	<input type="radio"/>
Network security group (NSG) default rules can be deleted.	<input type="radio"/>	<input checked="" type="radio"/>
Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types.	<input checked="" type="radio"/>	<input type="radio"/>

✉ **OrangeSG** Highly Voted 1 year, 3 months ago

Box 1: Yes

Security rules must have a unique name within the network security group (NSG)

Box 2: No

You can't remove the default rules, but you can override them by creating rules with higher priorities.

Box 3: Yes

Reference

Network security groups

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

upvoted 10 times

✉ **zellck** Most Recent 11 months, 1 week ago

YNY is the answer.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules>

Name

- A unique name within the network security group. The name can be up to 80 characters long. It must begin with a word character, and it must end with a word character or with '_'. The name may contain word characters or '.', '-', '_'.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules>

You can't remove the default rules, but you can override them by creating rules with higher priorities.

upvoted 1 times

✉ **zellck** 11 months, 1 week ago<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules>

Protocol

- TCP, UDP, ICMP, ESP, AH, or Any. The ESP and AH protocols aren't currently available via the Azure portal but can be used via ARM templates.

upvoted 1 times

✉ **MRCSPD2865** 1 year, 3 months ago

You can delete a custom security rule. You aren't allowed to delete a default security rule.

<https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-security-group?tabs=network-security-group-portal#delete-a-security-rule>

upvoted 4 times

✉ **MRCSPD2865** 1 year, 3 months ago

NSG default rules can be customised but not deleted
upvoted 3 times

 **IZone** 1 year, 5 months ago

Correct

upvoted 1 times

 **jellybiscuit** 1 year, 6 months ago

Correct

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>
upvoted 1 times

Question #119

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

When users attempt to access an application or a service,

administration
auditing
authentication
authorization

controls their level of access.

Correct Answer:

Answer Area

When users attempt to access an application or a service,

administration
auditing
authentication
authorization

controls their level of access.

 **paprda** Highly Voted  1 year, 3 months ago

you can simply memorize:

authENTication = ENTER = can i go in?

authoRization = RIGHTS = where i can then go?

upvoted 22 times

 **zellck** Most Recent  11 months, 1 week ago

"authorisation" is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/2-define-authentication-authorization>

In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to AuthZ.

upvoted 2 times

 **Whyiest** 1 year, 2 months ago

Correct

upvoted 3 times

 **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected => authorization

upvoted 3 times

Question #120

Topic 1

What are customers responsible for when evaluating security in a software as a service (SaaS) cloud services model?

- A. operating systems
- B. network controls
- C. applications
- D. accounts and identities

Correct Answer: C

Community vote distribution

D (98%)

 **Jeebsn**  1 year, 2 months ago

Selected Answer: D

D is the ans
upvoted 5 times

 **zellck**  11 months, 1 week ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/2-describe-shared-responsibility-model>
In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

upvoted 5 times

 **Aalkinani**  1 week, 5 days ago

Selected Answer: D

D. Accounts and identities.

While the SaaS provider manages the underlying infrastructure, including operating systems, network controls, and applications, customers are typically responsible for managing access to the service, including user accounts, identities, and permissions. This includes tasks such as ensuring secure authentication, managing user roles and permissions, and monitoring user activity to detect and prevent unauthorized access.

upvoted 1 times

 **Soniadlg** 3 weeks ago

D es la correcta
upvoted 1 times

 **claudiosousa** 2 months, 1 week ago

Selected Answer: D

Letter D!
upvoted 2 times

 **Darkfire** 8 months, 1 week ago

Selected Answer: D

D = Correct

- A. Operating systems = Responsibility for the hoster (SaaS)
- B. Network controls = Responsibility for the hoster (SaaS)
- C. Applications = Responsibility for the hoster (SaaS)
- D. Accounts and identities = Responsibility for the Customer

upvoted 4 times

 **wborquez** 9 months, 3 weeks ago

La D es la correcta
upvoted 4 times

 **SGhani** 11 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 2 times

✉ **Mithu94** 1 year, 1 month ago

Selected Answer: D

D Correct

upvoted 4 times

✉ **Mithu94** 1 year, 1 month ago

D Correct

upvoted 4 times

✉ **Nokuthula** 1 year, 1 month ago

D is correct

upvoted 3 times

✉ **vhogstad** 1 year, 1 month ago

D is Correct

upvoted 3 times

✉ **Gireesha** 1 year, 2 months ago

It's D, " Accounts and Identities"; Since it's a SaaS

upvoted 3 times

✉ **yonie** 1 year, 3 months ago

Selected Answer: D

correct answer is D - SaaS.

Not PaaS

upvoted 4 times

✉ **MRCSPD2865** 1 year, 3 months ago

correct answer id D - <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility> - answer in the list has to be corrected
upvoted 3 times

✉ **marribas** 1 year, 4 months ago

<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

D is the correct

upvoted 3 times

✉ **Cooljoy7777** 1 year, 4 months ago

Selected Answer: D

It's (SaaS) cloud services model so the company is only responsible for the accounts and ID

upvoted 4 times

✉ **zxmaz01** 1 year, 2 months ago

...and data

upvoted 1 times

Question #121

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

A domain controller
Active Directory Domain Services (AD DS)
Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
Federation

provides single sign-on (SSO) capabilities across multiple identity providers.

Correct Answer:**Answer Area**

A domain controller
Active Directory Domain Services (AD DS)
Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
Federation

provides single sign-on (SSO) capabilities across multiple identity providers.

 IXOne Highly Voted  1 year, 5 months ago

Correct

upvoted 6 times

 Armanas Highly Voted  1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected => Federation

upvoted 5 times

 jalvarinoabad Most Recent  7 months ago

Federation - When you set up SSO to work between multiple identity providers, it's called federation. An SSO implementation based on federation protocols improves security, reliability, end-user experiences, and implementation.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on>

upvoted 1 times

 MacDanorld 1 year, 5 months ago

the question was in my exams today 03/10/22 and I choose Federation

upvoted 4 times

Question #122

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

In an environment that has on-premises resources and cloud resources,

should be the primary security perimeter.

- the cloud
- a firewall
- identity
- Microsoft Defender for Cloud

Correct Answer:

Answer Area

In an environment that has on-premises resources and cloud resources,

should be the primary security perimeter.

- the cloud
- a firewall
- identity
- Microsoft Defender for Cloud

 OrangeSG Highly Voted 1 year, 3 months ago

Answer: Identity

Many consider identity to be the primary perimeter for security. This is a shift from the traditional focus on network security.

Best practice: Center security controls and detections around user and service identities.

Detail: Use Azure AD to collocate controls and identities.

Reference

Azure Identity Management and access control security best practices

<https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices>

upvoted 6 times

 masterb911 Most Recent 8 months ago

Correct

upvoted 1 times

 zellck 11 months, 1 week ago

"identity" is the answer.

<https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices#treat-identity-as-the-primary-security-perimeter>

Many consider identity to be the primary perimeter for security. This is a shift from the traditional focus on network security. Network perimeters keep getting more porous, and that perimeter defense can't be as effective as it was before the explosion of BYOD devices and cloud applications.

upvoted 1 times

 MacDanorld 1 year, 5 months ago

Identity is the correct answer, came out in my exams today

upvoted 3 times

 darkpangel 1 year, 6 months ago

Identity

<https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices>

upvoted 2 times

 **Armanas** 1 year, 6 months ago

This Question appeared in Exam today (02 September 2022)

I selected => identity

upvoted 2 times

Question #123

Topic 1

What does Conditional Access evaluate by using Azure Active Directory (Azure AD) Identity Protection?

- A. user actions
- B. group membership
- C. device compliance
- D. user risk

Correct Answer: C

Community vote distribution

D (100%)

 **cris_exam**  1 year, 2 months ago

Selected Answer: D

Correct is D - User risk.

For customers with access to Identity Protection, user risk can be evaluated as part of a Conditional Access policy.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#user-risk>
upvoted 14 times

 **yonie**  1 year, 3 months ago

Selected Answer: D

D is correct. Identity

upvoted 8 times

 **claudiosousa**  2 months, 1 week ago

Selected Answer: D

D. user risk

upvoted 1 times

 **BrkyUlukn** 3 months, 1 week ago

Answer: D

Explanation:

It's user risk including the below:

Anonymous IP address use

Atypical travel

Malware linked IP address

Unfamiliar sign-in properties

Leaked credentials

Password spray

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identityprotection>

upvoted 1 times

 **rollying** 11 months ago

id.. is user at risk and device is endpoint at risk

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#migrate-risk-policies-from-identity-protection-to-conditional-access>
upvoted 1 times

 **KJUHIF** 1 year, 2 months ago

Selected Answer: D

User risk

upvoted 6 times

 **xeni66** 1 year, 4 months ago

Selected Answer: D

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

upvoted 5 times

etinosaHendrix 1 year, 5 months ago

It's D

upvoted 1 times

Indy429 1 year, 5 months ago

Selected Answer: D

User risk

upvoted 4 times

fdosoli 1 year, 5 months ago

Selected Answer: D

It's D

upvoted 3 times

Kev_NZ 1 year, 6 months ago

Selected Answer: D

It's D

upvoted 4 times

randyruchira 1 year, 6 months ago

It's D

upvoted 1 times

jellybiscuit 1 year, 6 months ago

Selected Answer: D

D. user risk

upvoted 1 times

azeem0077 1 year, 6 months ago

Selected Answer: D

Its's user risk including the below:

Anonymous IP address use

Atypical travel

Malware linked IP address

Unfamiliar sign-in properties

Leaked credentials

Password spray

upvoted 5 times

gaijin101 1 year, 6 months ago

Should be D

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

Its about Identity Protection

upvoted 5 times

Question #124

Which statement represents a Microsoft privacy principle?

- A. Microsoft manages privacy settings for its customers.
- B. Microsoft respects the local privacy laws that are applicable to its customers.
- C. Microsoft uses hosted customer email and chat data for targeted advertising.
- D. Microsoft does not collect any customer data.

Correct Answer: A

Community vote distribution

B (98%)

 **jellybiscuit** Highly Voted 1 year, 6 months ago

Selected Answer: B

<https://privacy.microsoft.com/en-US/#whatinformationwecollectmodule>
upvoted 11 times

 **shaochilee888** Highly Voted 1 year, 6 months ago

Selected Answer: B

Should be B
Then, Strong legal protections. Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.
upvoted 9 times

 **jaaake** Most Recent 9 months, 1 week ago

It can't be A. That would be against the Shared Responsibility Model.
upvoted 3 times

 **manofsteel9** 10 months ago

Selected Answer: B

The correct answer is:

B. Microsoft respects the local privacy laws that are applicable to its customers.

Microsoft respects the local privacy laws that are applicable to its customers. This is a fundamental privacy principle for Microsoft, indicating their commitment to comply with applicable privacy regulations and laws governing the collection, use, and protection of customer data in different regions and jurisdictions.

Option A is incorrect because Microsoft does not manage privacy settings for its customers, but rather provides tools and controls for customers to manage their own privacy settings within Microsoft products and services.

Option C is incorrect because Microsoft does not use hosted customer email and chat data for targeted advertising. Microsoft has specific policies and practices in place to protect customer data and maintain customer trust.

Option D is incorrect because Microsoft does collect customer data, but they do so with a commitment to safeguarding customer privacy and using the data in accordance with applicable privacy laws and regulations.

upvoted 4 times

 **zellck** 11 months, 1 week ago

Selected Answer: B

B is the answer.

<https://www.microsoft.com/en-us/trustcenter/privacy/%E2%80%AF#section3>

- Strong legal protections
We will respect your local privacy laws and fight for legal protection of your privacy as a right.
upvoted 1 times

 **ARM360** 11 months, 3 weeks ago

Selected Answer: B

Answer is B

Our primary privacy principles

Control
We will put you in control of your privacy with easy-to-use tools and clear choices.

Transparency
We will be transparent about data collection and use so you can make informed decisions.

Security

We protect your data with strong security and encryption. To learn more, visit Microsoft Security.

Strong legal protections

We will respect your local privacy laws and fight for legal protection of your privacy as a right.

No content-based targeting

We will not use your email, chat, files, or other personal content to target ads to you.

Benefit to you

When we do collect data, we will use it to benefit you and to make your experiences better.

<https://www.microsoft.com/en-us/trustcenter/privacy/%E2%80%AF#:~:text=Microsoft%20believes%20privacy%20is%20a,data%20is%20collected%20and%20used.>

upvoted 1 times

 **Nokuthula** 1 year, 1 month ago

should be B

upvoted 2 times

 **Tined** 1 year, 1 month ago

Selected Answer: B

<https://privacy.microsoft.com/en-US/#whatinformationwecollectmodule>

upvoted 2 times

 **RDIO** 1 year, 2 months ago

Selected Answer: B

B is correct

upvoted 4 times

 **yonie** 1 year, 3 months ago

Selected Answer: B

Microsoft respects the local privacy laws that are applicable to its customers

upvoted 4 times

 **Creamie** 1 year, 5 months ago

Should be B

upvoted 3 times

 **Indy429** 1 year, 5 months ago

Selected Answer: B

How is it A? It should really be B

upvoted 3 times

 **fdosoli** 1 year, 5 months ago

Selected Answer: B

Should be B!

upvoted 2 times

 **murrutia** 1 year, 6 months ago

This should be Answer B.

upvoted 2 times

 **jnni** 1 year, 6 months ago

Selected Answer: B

Should be B

<https://www.microsoft.com/en-us/trustcenter/privacy/%E2%80%AF>

upvoted 3 times

 **Goddev** 1 year, 6 months ago

Selected Answer: D

Should be be

upvoted 1 times

 **gaijin101** 1 year, 6 months ago

Should be B

upvoted 2 times

Question #125

Topic 1

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

A security information and event management (SIEM)
A security orchestration automated response (SOAR)
A Trusted Automated eXchange of Indicator Information (TAXII)
An attack surface reduction (ASR)

system is a tool that collects data from multiple systems, identifies correlations or anomalies, and generates alerts and incidents.

Correct Answer:**Answer Area**

A security information and event management (SIEM)
A security orchestration automated response (SOAR)
A Trusted Automated eXchange of Indicator Information (TAXII)
An attack surface reduction (ASR)

system is a tool that collects data from multiple systems, identifies correlations or anomalies, and generates alerts and incidents.

✉  **Chanel_n5**  1 year, 1 month ago

Correct.

"A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents."

<https://learn.microsoft.com/en-us/training/modules/describe-security-capabilities-of-azure-sentinel/2-define-concepts-of-siem-soar>
upvoted 5 times

✉  **zellck**  11 months, 1 week ago

"SIEM" is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-security-capabilities-of-azure-sentinel/2-define-concepts-of-siem-soar>
A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.
upvoted 3 times

✉  **MacDanorld** 1 year, 5 months ago

Came out in my exams today

upvoted 4 times

✉  **jorgednunes** 1 year, 2 months ago

Really useful...

upvoted 2 times

✉  **Burnie** 1 year, 4 months ago

So useful. Thank you

upvoted 3 times

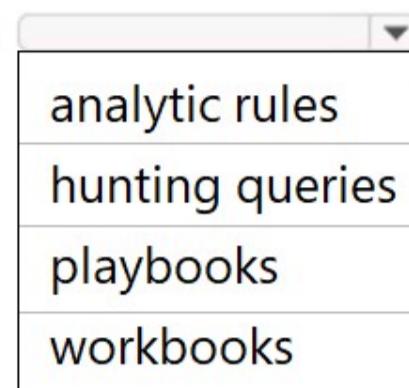
Question #126

Topic 1

HOTSPOT -

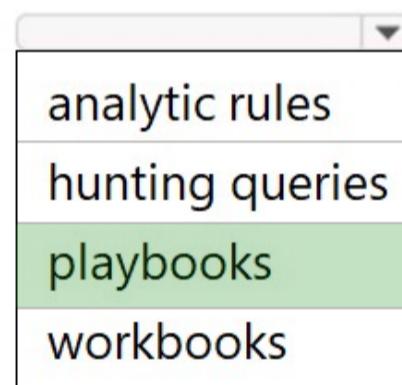
Select the answer that correctly completes the sentence.

Hot Area:

Answer Area**Microsoft Sentinel**

use Azure Logic Apps to automate and orchestrate responses to alerts.

Correct Answer:

Answer Area**Microsoft Sentinel**

use Azure Logic Apps to automate and orchestrate responses to alerts.

NAMP Highly Voted 1 year, 6 months ago

Congrats for reaching here! Good luck on your exam!

upvoted 27 times

AVHT Highly Voted 1 year, 3 months ago

Damn, I made it. I went through the practice questions twice. My exam is on Dec 10th 2022. I passed my AZ-900 Fundamentals, CompTIA Security+ and SC-900 is tomorrow! Thank you Exam Topics, changing lives!

upvoted 7 times

Darkfire Most Recent 8 months ago

Answer is correct

Keywords = Automate and orchestrate = Playbooks

upvoted 1 times

zellck 11 months, 1 week ago

"playbooks" is the answer.

<https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents#what-are-automation-rules-and-playbooks>

Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, which means that you get all the power, customizability, and built-in templates of Logic Apps. Each playbook is created for the specific subscription to which it belongs, but the Playbooks display shows you all the playbooks available across any selected subscriptions.

upvoted 1 times

PinkUnicorns 1 year, 2 months ago

I have used this site before it has been really useful. Cheers for this.

The answer is playbooks.

upvoted 5 times

ITOPS 1 year, 3 months ago

Where are the new questions it says 129 questions

upvoted 2 times

 **OrangeSG** 1 year, 3 months ago

Answer: playbooks

Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

Reference

Tutorial: Use playbooks with automation rules in Microsoft Sentinel

<https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

upvoted 2 times

 **MacDanorld** 1 year, 5 months ago

Came out in my exams today

upvoted 2 times

 **jellybiscuit** 1 year, 6 months ago

Playbooks is correct.

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC>

upvoted 4 times

Question #127

Topic 1

Which compliance feature should you use to identify documents that are employee resumes?

- A. pre-trained classifiers
- B. Activity explorer
- C. eDiscovery
- D. Content explorer

Correct Answer: A

Community vote distribution

A (100%)

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: A

Correct: <https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-tc-definitions?view=o365-worldwide#resume>

upvoted 11 times

 **zellck** Most Recent 11 months, 1 week ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-tc-definitions?view=o365-worldwide#resume>

Detects a resume document that a job applicant provides an employer, which has a detailed statement of the candidate's prior work experience, education, and accomplishments.

upvoted 2 times

 **ARM360** 11 months, 3 weeks ago

Selected Answer: A

Detects a resume document that a job applicant provides an employer, which has a detailed statement of the candidate's prior work experience, education, and accomplishments.

upvoted 1 times

Question #128

Topic 1

DRAG DROP

Match the pillars of Zero Trust to the appropriate requirements.

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

NOTE: Each correct match is worth one point.

Pillars	Answer Area
Data	Pillar Must be segmented
Identities	Pillar Must be verified by using strong authentication
Networks	Pillar Must be classified, labeled, and encrypted based on its attributes

Correct Answer:

Answer Area
Networks Must be segmented
Identities Must be verified by using strong authentication
Data Must be classified, labeled, and encrypted based on its attributes

✉  **ETU69**  1 year, 2 months ago

Correct

upvoted 7 times

✉  **Tahamaffia**  6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 2 times

✉  **masterb911** 7 months, 4 weeks ago

Correct

upvoted 1 times

✉  **rollingy** 11 months ago

correct !!

upvoted 1 times

✉  **zellck** 11 months, 1 week ago

1. Networks

2. Identities

3. Data

upvoted 2 times

✉  **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/4-describe-zero-trust-model>

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- Identities may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.
- Data should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.
- Networks should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

upvoted 1 times

✉  **zeos38** 1 year ago

Correct

upvoted 1 times

✉  **obaali1990** 1 year, 1 month ago

Correct

upvoted 2 times

Question #129

Topic 1

DRAG DROP

Match the types of compliance score actions to the appropriate tasks.

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

NOTE: Each correct match is worth one point.

Compliance score action	Answer Area
Corrective	<input type="text"/>
Detective	<input type="text"/>
Preventative	<input type="text"/>

Use encryption to protect data at rest.
Actively monitor systems to identify irregularities that might represent risks.

Answer Area	
Correct Answer:	<input type="text"/> Preventative Use encryption to protect data at rest. <input type="text"/> Detective Actively monitor systems to identify irregularities that might represent risks.

 W2S3 Highly Voted 1 year, 2 months ago

Protect = prevent

Monitor = detect

upvoted 8 times

 Darkfire Most Recent 8 months ago

Keywords:

Preventative = Protect at rest

Detective = Actively monitor

<https://learn.microsoft.com/en-us/purview/compliance-score-calculation?view=o365-worldwide>

upvoted 2 times

 zellck 11 months, 1 week ago

1. Preventative
2. Detective

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide#preventative-detective-and-corrective-actions>

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.

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.

upvoted 3 times

 obaali1990 1 year, 1 month ago

Correct

upvoted 3 times

 ETU69 1 year, 2 months ago

Correct

upvoted 4 times

Question #130

Topic 1

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

- A. authorization
- B. auditing
- C. administration
- D. authentication

Correct Answer: B

Community vote distribution

B (100%)

 **cris_exam** Highly Voted 1 year, 2 months ago

Selected Answer: B

Auditing is correct - the key word here is tracking, otherwise it would have been authorization.

See below article.

<https://social.technet.microsoft.com/wiki/contents/articles/15530.the-four-pillars-of-identity-identity-management-in-the-age-of-hybrid-it.aspx>
upvoted 7 times

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: B

Correct

upvoted 6 times

 **fmondez** Most Recent 10 months, 1 week ago

Selected Answer: B

Easy one I would say

upvoted 1 times

 **mjg23** 11 months, 1 week ago

B is the answer.

upvoted 1 times

 **obaali1990** 1 year, 1 month ago

B is correct

upvoted 3 times

Question #131

Topic 1

What can be created in Active Directory Domain Services (AD DS)?

- A. line-of-business (LOB) applications that require modern authentication
- B. computer accounts
- C. software as a service (SaaS) applications that require modern authentication
- D. mobile devices

Correct Answer: B

Community vote distribution

B (100%)

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: B

Correct

upvoted 11 times

 **Molota** Most Recent 9 months, 1 week ago

Selected Answer: B

correct

upvoted 1 times

 **Irban** 9 months, 1 week ago

Selected Answer: B

Correct

upvoted 1 times

 **fmontez** 10 months, 1 week ago

Selected Answer: B

AD DS = accounts

upvoted 1 times

 **marstot** 10 months, 2 weeks ago

Selected Answer: B

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

This data store, also known as the directory, contains information about Active Directory objects. These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts.

upvoted 1 times

Question #132

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

When users sign in, verifies their credentials to prove their identity.

- administration
- auditing
- authentication
- authorization

Answer Area

Correct Answer: When users sign in, verifies their credentials to prove their identity.

- administration
- auditing
- authentication**
- authorization

 **ETU69** Highly Voted 1 year, 2 months ago

Correct

upvoted 8 times

 **Barbados** Highly Voted 1 year, 1 month ago

Correct. Authentication

upvoted 6 times

 **zellck** Most Recent 11 months, 1 week ago

"authentication" is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/2-define-authentication-authorization>

Authentication is the process of proving that a person is who they say they are. When someone purchases an item with a credit card, they may be required to show an additional form of identification. This proves that they are the person whose name appears on the card. In this example, the user may show a driver's license that serves as a form of authentication and proves their ID.

upvoted 3 times

 **obaali1990** 1 year, 1 month ago

correct

upvoted 3 times

Question #133

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Authorization is used to identify the level of access to a resource.	<input type="radio"/>	<input type="radio"/>
Authentication is proving that users are who they say they are.	<input type="radio"/>	<input type="radio"/>
Authentication identifies whether you can read and write to a file.	<input type="radio"/>	<input type="radio"/>

Statements	Yes	No
Authorization is used to identify the level of access to a resource.	<input checked="" type="radio"/>	<input type="radio"/>
Authentication is proving that users are who they say they are.	<input checked="" type="radio"/>	<input type="radio"/>
Authentication identifies whether you can read and write to a file.	<input type="radio"/>	<input checked="" type="radio"/>

✉ **ETU69** Highly Voted 1 year, 2 months ago

Correct

upvoted 9 times

✉ **zellck** Highly Voted 11 months, 1 week ago

YYN is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/2-define-authentication-authorization>

Authentication is the process of proving that a person is who they say they are. When someone purchases an item with a credit card, they may be required to show an additional form of identification. This proves that they are the person whose name appears on the card. In this example, the user may show a driver's license that serves as a form of authentication and proves their ID.

Once you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called authorization.

In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to AuthZ.

upvoted 5 times

✉ **Molota** Most Recent 9 months, 1 week ago

YYN is correct

upvoted 2 times

✉ **obaali1990** 1 year, 1 month ago

Correct answers are YYN

upvoted 3 times

✉ **Barbados** 1 year, 1 month ago

Correct. Y/Y/N

upvoted 4 times

Question #134

What is a function of Conditional Access session controls?

- A. enforcing device compliance
- B. enforcing client app compliance
- C. enable limited experiences, such as blocking download of sensitive information
- D. prompting multi-factor authentication (MFA)

Correct Answer: D

Community vote distribution

C (76%)

D (24%)

 **muhtoy**  11 months, 2 weeks ago

Selected Answer: C

C. enable limited experiences, such as blocking download of sensitive information.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>
upvoted 8 times

 **beamage**  1 year, 1 month ago

Selected Answer: D

A function, not the definition of all functions, Just one....

upvoted 7 times

 **Manny_ez**  2 months, 1 week ago

Selected Answer: C

Its C. Session controls limit the experiences withing specific cloud applications.

Grant controls on the other hand block or grant access by requiring MFA.

upvoted 1 times

 **tc_praveen** 3 months, 1 week ago

C

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Defender for Cloud Apps portal to refine filters and set actions to take. With the access and session policies, you can:

Prevent data exfiltration: You can block the download, cut, copy, and print of sensitive documents on, for example, unmanaged devices
upvoted 1 times

 **BrkyUlukn** 3 months, 2 weeks ago

Suggested Answer: D

Conditional Access session controls enable user app access and sessions to be monitored and controlled in real time based on access and session policies.

Based on this definition, the best answer for your question isB. enable limited experiences, such as blocking download of sensitive information.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>
upvoted 1 times

 **DanPicardi** 8 months, 1 week ago

C is the correct answer

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#conditional-access-application-control>

upvoted 2 times

 **jaaake** 9 months, 1 week ago

Prompting MFA is a funciton of Conditional Access. But Enabling Limited Experiences is a function of Conditional Access session controls, as the session control only starts after successful authentication. Hence D is not, and C is right.

upvoted 5 times

 **Andreia_Almeida** 9 months, 3 weeks ago

Both seem to be right: <https://www.bing.com/search?q=what+is+a+function+of+conditional+access+session+controls%3F+microsoft+365&form=ANNH02&refig=dce410bbd44f4732bac0672cf9b28317>

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications.

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Defender for Cloud Apps portal to refine filters and set actions to take. With the access and session policies, you can:

- Prevent data exfiltration: You can block the download, cut, copy, and print of sensitive documents on, for example, unmanaged devices.
upvoted 4 times

hululolo 1 year ago

Correct Answer is C

upvoted 5 times

nikolaost 1 year, 1 month ago**Selected Answer: C**

C is correct

upvoted 4 times

Mithu94 1 year, 1 month ago**Selected Answer: C**

"Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications" <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

upvoted 5 times

luckyiki 1 year, 2 months ago**Selected Answer: D**

As stated by many

Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications.

upvoted 3 times

cris_exam 1 year, 2 months ago**Selected Answer: C**

Should be C.

See dingtheking's shared article.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

upvoted 4 times

dingtheking 1 year, 2 months ago**Selected Answer: C**<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

upvoted 4 times

KJUHIF 1 year, 2 months ago**Selected Answer: C**

C is correct

upvoted 3 times

RealPaz 1 year, 2 months ago**Selected Answer: C**

It's C

upvoted 2 times

Question #135

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Azure AD Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can detect whether user credentials were leaked to the public.	<input type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Azure AD Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input checked="" type="radio"/>
	Azure AD Identity Protection can detect whether user credentials were leaked to the public.	<input checked="" type="radio"/>	<input type="radio"/>
	Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input checked="" type="radio"/>	<input type="radio"/>

✉️ **PinkUnicorns** Highly Voted 1 year, 2 months ago

No, Yes, Yes - Correct
upvoted 9 times

✉️ **dawnbringer69** Most Recent 10 months ago

I would have to disagree with the comments in here.

As I see it the 3rd question is a tricky trap. When we evaluate a sign in risk, the risk level is calculated for the sign in action itself (as for example someone else rather than the actual user is trying to login), not the user risk (as for example the account of the user is compromised).

Hence my answer would be NYN
upvoted 1 times

✉️ **dawnbringer69** 9 months, 4 weeks ago

To make it even more clear, MFA is evoked in the Sign in Risk feature of Identity Protection. Not the User's Risk one. The last one evokes Password Change.

Hence the tricky Trap.
upvoted 2 times

✉️ **Mehe323** 7 months, 3 weeks ago

It is still true because even with user risk, an admin can configure to require multifactor authentication (and password change). The answer is therefore Y.

Read the part under User Risk Policy in Conditional Access:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

upvoted 1 times

✉️ **zellck** 11 months, 1 week ago

NYY is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#nonpremium-user-risk-detections>
- Leaked credentials

This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling

the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they're checked against Azure AD users' current valid credentials to find valid matches.

upvoted 3 times

✉  **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#sign-in-risk-based-conditional-access-policy>

During each sign-in, Identity Protection analyzes hundreds of signals in real-time and calculates a sign-in risk level that represents the probability that the given authentication request isn't authorized. This risk level then gets sent to Conditional Access, where the organization's configured policies are evaluated. Administrators can configure sign-in risk-based Conditional Access policies to enforce access controls based on sign-in risk, including requirements such as:

- Block access
- Allow access
- Require multifactor authentication

upvoted 2 times

✉  **XtraWest** 11 months, 1 week ago

Yes, Yes, Yes

upvoted 1 times

✉  **obaali1990** 1 year, 1 month ago

Yes yes No

upvoted 1 times

✉  **ETU69** 1 year, 2 months ago

Correct

upvoted 4 times

Question #136

Topic 1

What can you use to ensure that all the users in a specific group must use multi-factor authentication (MFA) to sign to Azure Active Directory (Azure AD)?

- A. Azure Policy
- B. a communication compliance policy
- C. a Conditional Access policy
- D. a user risk policy

Correct Answer: C

Community vote distribution

C (100%)

✉  **orionduo**  1 year, 2 months ago

Correct.

ref: <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

upvoted 7 times

✉  **ETU69**  1 year, 2 months ago

Selected Answer: C

Correct

upvoted 6 times

✉  **Tahamaffia**  6 months, 2 weeks ago

Got this question on my exam 05/09/2023

upvoted 1 times

✉  **zellck** 11 months, 1 week ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

upvoted 1 times

✉  **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/explore-access-management-capabilities/2-describe-conditional-access-azure-ad>

When the Conditional Access policy has been applied, an informed decision is reached on whether to grant access, block access, or require extra verification. The decision is referred to as the access controls portion of the Conditional Access policy and defines how a policy is enforced.

Common decisions are:

- Require one or more conditions to be met before granting access:

Require multi-factor authentication.

upvoted 1 times

Question #137

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	<input type="radio"/>	<input type="radio"/>
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	<input type="radio"/>	<input type="radio"/>
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	<input type="radio"/>	<input type="radio"/>

Correct Answer:	Statements	Yes	No
	You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
	User accounts created in Azure AD sync automatically to an on-premises Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
	When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	<input checked="" type="radio"/>	<input type="radio"/>

✉ **ETU69** Highly Voted 1 year, 2 months ago

Correct

upvoted 6 times

✉ **Molota** Most Recent 9 months, 1 week ago

Y N Y is correct

upvoted 1 times

✉ **zellck** 11 months, 1 week ago

YNY is the answer.

<https://learn.microsoft.com/en-us/training/modules/explore-basic-services-identity-types/6-describe-concept-of-hybrid-identity>
When it comes to authentication of hybrid identities, Microsoft offers several ways to authenticate.

- Azure AD Password hash synchronization.
- Azure AD Pass-through authentication
- Federated authentication

upvoted 3 times

✉ **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/what-is-inter-directory-provisioning>

Inter-directory provisioning is provisioning an identity between two different directory services systems. The most common scenario for inter-directory provisioning is when a user already in Active Directory is provisioned into Azure AD. This provisioning can be accomplished by agents such as Azure AD Connect sync or Azure AD Connect cloud provisioning.

upvoted 2 times

Question #138

Topic 1

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

Community vote distribution

ABC (100%)

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: ABC

Correct: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#select-authentication-methods-and-registration-options>

upvoted 7 times

 **zellck** Most Recent 11 months, 1 week ago

Selected Answer: ABC

ABC is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#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
- upvoted 3 times

 **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/explore-authentication-capabilities/4-describe-self-service-password-reset>

The following authentication methods are available for SSPR:

- Mobile app notification
 - Mobile app code
 - Email
 - Mobile phone
 - Office phone
 - Security questions
- upvoted 2 times

 **obaali1990** 1 year, 1 month ago

Selected Answers: ABC

upvoted 4 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: ABC

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#select-authentication-methods-and-registration-options>

upvoted 3 times

Question #139

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Azure AD B2C enables external users to sign in by using their preferred social or enterprise account identities.	<input type="radio"/>	<input type="radio"/>
External Azure AD B2C users are managed in the same directory as users in the Azure AD organization.	<input type="radio"/>	<input type="radio"/>
Custom branding can be applied to Azure AD B2C authentication.	<input type="radio"/>	<input type="radio"/>

Correct Answer:		
Statements	Yes	No
Azure AD B2C enables external users to sign in by using their preferred social or enterprise account identities.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
External Azure AD B2C users are managed in the same directory as users in the Azure AD organization.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Custom branding can be applied to Azure AD B2C authentication.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

✉ ETU69 **Highly Voted** 1 year, 2 months ago

Correct: See answer for second question at <https://learn.microsoft.com/en-us/azure/active-directory-b2c/tenant-management>
upvoted 7 times

✉ zellck **Most Recent** 11 months, 1 week ago

YNY is the answer.

<https://learn.microsoft.com/en-us/azure/active-directory-b2c/overview>

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

Azure AD B2C is a separate service from Azure Active Directory (Azure AD). It is built on the same technology as Azure AD but for a different purpose. It allows businesses to build customer facing applications, and then allow anyone to sign-up and into those applications with no restrictions on user account.

Azure AD B2C is a white-label authentication solution. You can customize the entire user experience with your brand so that it blends seamlessly with your web and mobile applications.

upvoted 4 times

✉ [Removed] 1 year, 1 month ago

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

upvoted 3 times

✉ cris_exam 1 year, 2 months ago

Correct.

A nice video about this below.

<https://azure.microsoft.com/nl-nl/blog/easily-enable-identity-and-access-management-with-social-logins-for-b2c-apps/>

upvoted 4 times

Question #140

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication	<input type="radio"/>	<input type="radio"/>
Windows Hello is an example of passwordless authentication	<input type="radio"/>	<input type="radio"/>
FIDO2 security keys are an example of passwordless authentication	<input type="radio"/>	<input type="radio"/>

Statements	Yes	No
Software tokens are an example of passwordless authentication.	<input type="radio"/>	<input checked="" type="radio"/>
Windows Hello is an example of passwordless authentication.	<input checked="" type="radio"/>	<input type="radio"/>
FIDO2 security keys are an example of passwordless authentication.	<input checked="" type="radio"/>	<input type="radio"/>

hiuzai Highly Voted 1 year, 1 month ago

Microsoft authenticator is also a software token!
upvoted 13 times

ETU69 Highly Voted 1 year, 2 months ago

Correct: Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

- Windows Hello for Business
- Microsoft Authenticator
- FIDO2 security keys

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>
upvoted 11 times

tc_praveen Most Recent 3 months ago

YYY is the answer.
upvoted 2 times

Darkfire 8 months ago

NYY

Based on:
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

- Windows Hello for Business
- Microsoft Authenticator
- FIDO2 security keys

Software tokens isn't mentioned as PasswordLess.
upvoted 1 times

✉ **dsharp** 8 months, 1 week ago

YYY

Software tokens as well

upvoted 1 times

✉ **zellck** 11 months, 1 week ago

YYY is the answer.

<https://learn.microsoft.com/en-us/training/modules/explore-authentication-capabilities/2-describe-authentication-methods>

upvoted 5 times

✉ **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

- Windows Hello for Business
- Microsoft Authenticator
- FIDO2 security keys

upvoted 1 times

✉ **muhtoy** 11 months, 2 weeks ago

YYY - Yes to all statements.

upvoted 2 times

✉ **ARM360** 11 months, 3 weeks ago

Answer should be YYY

A software token is a digital token sent to a requester's smartphone, computer, or tablet. It typically consists of a one-time password, usually a 6-8 digit code, which the user must enter, often along with a second authentication factor, to gain access. Authenticator apps typically rely on a shared secret key and support OATH event-based (HOTP) and time-based (TOTP) algorithms.

<https://rb.gy/8zw8s>

upvoted 3 times

✉ **MJFT** 1 year ago

YYY

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless>

upvoted 2 times

✉ **hiuzai** 1 year, 1 month ago

the answer should be yes, yes, yes

upvoted 5 times

Question #141

Topic 1

Which security feature is available in the free mode of Microsoft Defender for Cloud?

- A. threat protection alerts
- B. just-in-time (JIT) VM access to Azure virtual machines
- C. vulnerability scanning of virtual machines
- D. secure score

Correct Answer: D

Community vote distribution

D (100%)

✉  **ETU69**  1 year, 2 months ago

Selected Answer: D

Correct

upvoted 6 times

✉  **zellck**  11 months, 1 week ago

Selected Answer: D

D is the answer.

<https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud>

upvoted 2 times

✉  **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/describe-security-management-capabilities-of-azure/4-describe-enhanced-security-defender-cloud>

Microsoft Defender for Cloud (Free) - Microsoft Defender for Cloud is enabled for free on all your Azure subscriptions. Using this free mode provides the secure score and its related features: security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.

upvoted 1 times

✉  **obaali1990** 1 year, 1 month ago

Correct Answer: D

upvoted 3 times

Question #142

Topic 1

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) can be used on which operating systems?

- A. Windows 10 and newer only
- B. Windows 10 and newer and Android only
- C. Windows 10 and newer and iOS only
- D. Windows 10 and newer, Android, and iOS

Correct Answer: A

Community vote distribution

A (94%)

6%

✉  **Manny_ez** 2 months, 1 week ago

Selected Answer: A

A is the answer.

Endpoint data loss prevention is only supported on Windows 10 and newer, and MacOS
upvoted 2 times

✉  **BrkyUlukn** 3 months, 2 weeks ago

I think it must be answer C

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10/11 and macOS (the three latest released major versions) devices

<https://learn.microsoft.com/en-us/purview/endpoint-dlp-learn-about>
upvoted 1 times

✉  **esska** 8 months, 1 week ago

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices

upvoted 2 times

✉  **zellck** 11 months, 1 week ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started>
Microsoft Endpoint DLP allows you to monitor onboarded Windows 10, and Windows 11 and onboarded macOS devices running three latest released versions. Once a device is onboarded, DLP detects when sensitive items are used and shared. This gives you the visibility and control you need to ensure that they're used and protected properly, and to help prevent risky behavior that might compromise them.
upvoted 2 times

✉  **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/describe-information-protection-governance-capabilities-microsoft-365/5-describe-data-loss-prevention>
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices
upvoted 1 times

✉  **muhtoy** 11 months, 2 weeks ago

Selected Answer: A

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (three latest released versions) devices1

<https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>
upvoted 1 times

✉  **muhtoy** 11 months, 2 weeks ago

<https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (three latest released versions) devices1
upvoted 2 times

✉  **ARM360** 11 months, 3 weeks ago

Selected Answer: A

Mac OS is a desktop operating system for Macintosh computers; iOS is a mobile operating system. The two are different.

Endpoint activities you can monitor and take action on

Endpoint DLP enables you to audit and manage the following types of activities users take on sensitive items that are physically stored Windows 10, Windows 11, or macOS devices.

upvoted 2 times

✉ **jqatar** 1 year, 1 month ago

Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. With a DLP policy, you can identify, monitor, and automatically protect sensitive items across:

Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive

Office applications such as Word, Excel, and PowerPoint

Windows 10, Windows 11 and macOS (three latest released versions) endpoints

non-Microsoft cloud apps

on-premises file shares and on-premises SharePoint.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

upvoted 2 times

✉ **Mithu94** 1 year, 1 month ago

Selected Answer: A

Windows 10, Windows 11 and macOS (three latest released versions) endpoints

upvoted 3 times

✉ **Mithu94** 1 year, 1 month ago

Selected Answer: C

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

upvoted 1 times

✉ **Mithu94** 1 year, 1 month ago

Sorry, iSO is not supported. so current answer is A.

"Windows 10, Windows 11 and macOS (three latest released versions) endpoints"

upvoted 1 times

✉ **randomuser141234** 1 year, 2 months ago

Selected Answer: A

<https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>

Win 10, Win 11 and Mac OS is supported. Not mobile devices.

upvoted 2 times

✉ **cris_exam** 1 year, 2 months ago

This is a tricky one. Official documentation says the below:

Windows 10, Windows 11 and macOS (three latest released versions) endpoints

So, the right answer might actually be C because as per above, it also states that besides Windows 10 and newer, there are also the 3 latest IOS versions.

I hope this question won't pop up in the exam. :)) I think I will go with C anyway.

upvoted 4 times

✉ **cris_exam** 1 year, 2 months ago

my mistake - I miss-read macOS to iOS.

A is correct!!

upvoted 3 times

✉ **obaali1990** 1 year, 1 month ago

Thanks for rectifying it

upvoted 1 times

✉ **Mithu94** 1 year, 1 month ago

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

upvoted 1 times

✉ **ETU69** 1 year, 2 months ago

Selected Answer: A

Correct: <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

upvoted 3 times

Question #143

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input checked="" type="checkbox"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input checked="" type="checkbox"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input checked="" type="checkbox"/>	<input type="radio"/>

ETU69 Highly Voted 1 year, 2 months ago

Wrong: all should be Yes, So YYY is the correct answer. Also see question #60 of which this is a duplicate.

upvoted 23 times

cris_exam Highly Voted 1 year, 2 months ago

Yes - <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction#define-your-azure-native-resources>

Yes - <https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management#defender-cspm-plan-options>

Yes - <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction#define-your-on-premises-resources>
upvoted 9 times

azhrhsn Most Recent 2 months, 2 weeks ago

YYY. (Duplicate of #60)

Microsoft Defender for Cloud provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more

Box 2: Yes -

Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes -

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

upvoted 2 times

jnlnnn 5 months, 3 weeks ago

YNY, for item #2 question states "... all Azure subscriptions" but CSPM is only for Cloud, not all. zellck has the supporting excerpt in his post "...any subscription or account that has onboarded to Defender for Cloud"

upvoted 1 times

jaaake 9 months ago

It is YYY. CSPM is available for all versions.

upvoted 3 times

zellck 11 months, 1 week ago

YYY is the answer.

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management#defender-cspm-plan-options>
Defender for Cloud offers foundational multicloud CSPM capabilities for free. These capabilities are automatically enabled by default on any subscription or account that has onboarded to Defender for Cloud. The foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening, compliance with Microsoft Cloud Security Benchmark (MCSB), and a Secure score which measure the current status of your organization's posture.

upvoted 3 times

 **YesOpo** 1 year ago

Should be YYY

upvoted 3 times

 **obaali1990** 1 year, 1 month ago

Correct Answers: YYY

upvoted 3 times

 **herodes** 1 year, 2 months ago

Its twice here.. YYY

upvoted 2 times

 **pviolent** 1 year, 2 months ago

YYY is the correct answer.

upvoted 5 times

Question #144

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Azure Active Directory (Azure AD) Password Protection	▼
Azure Bastion	▼
Azure Information Protection (AIP)	▼
Azure Key Vault	▼

is a cloud service for storing application secrets

Correct Answer:

Azure Active Directory (Azure AD) Password Protection	▼
Azure Bastion	▼
Azure Information Protection (AIP)	▼
Azure Key Vault	▼

is a cloud service for storing application secrets

✉ **ETU69** 1 year, 2 months ago

Correct

upvoted 8 times

✉ **Darkfire** 8 months ago

Correct

<https://learn.microsoft.com/en-us/azure/key-vault/general/overview>

upvoted 1 times

✉ **zellck** 11 months, 1 week ago

"Azure Key Vault" is the answer.

<https://learn.microsoft.com/en-us/azure/key-vault/general/overview>

Azure Key Vault is one of several key management solutions in Azure, and helps solve the following problems:

- Secrets Management - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets

upvoted 2 times

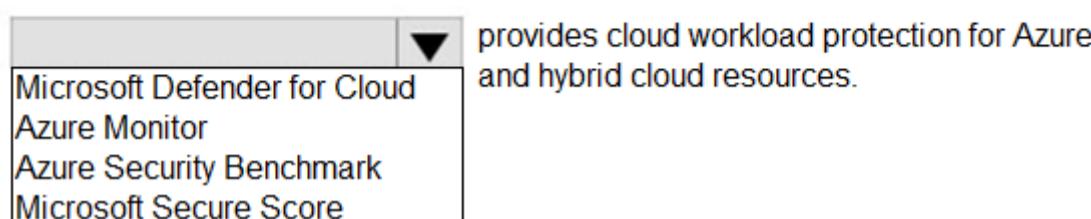
Question #145

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area



Correct Answer:

provides cloud workload protection for Azure and hybrid cloud resources.

ETU69 Highly Voted 1 year, 2 months ago

Correct

upvoted 9 times

orionduo Highly Voted 1 year, 2 months ago

Correct

ref: <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>

upvoted 7 times

zellck Most Recent 11 months, 1 week ago

"Microsoft Defender for Cloud" is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-security-management-capabilities-of-azure/3-describe-defender-cloud>

Microsoft Defender for Cloud is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms.

upvoted 4 times

Question #146

Topic 1

What is the maximum number of resources that Azure DDoS Protection Standard can protect without additional costs?

- A. 50
- B. 100
- C. 500
- D. 1000

Correct Answer: B

Community vote distribution

B (100%)

✉  **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: B

Correct: <https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-faq#how-does-pricing-work>
upvoted 11 times

✉  **penatuna** Highly Voted 1 year, 1 month ago

B is the right answer. However:

There's no Azure DDoS Protection Standard anymore.

"Azure DDoS Protection offers two tiers – IP Protection and Network Protection – to meet your security and cost needs".

<https://azure.microsoft.com/en-in/pricing/details/ddos-protection/>

upvoted 7 times

✉  **zelick** Most Recent 11 months, 1 week ago

Selected Answer: B

B is the answer.

<https://azure.microsoft.com/en-us/pricing/details/ddos-protection/>

Network Protection will have a fixed monthly charge, which includes protection for 100 public IP resources. Protection for additional public IP resources will be charged on a monthly per-resource basis. A single Azure DDoS Protection plan in a tenant can be used across multiple subscriptions

upvoted 1 times

✉  **orionduo** 1 year, 2 months ago

DDoS protection plans have a fixed monthly charge that covers up to 100 public IP addresses. Protection for additional resources is available.
<https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-faq#how-does-pricing-work>

upvoted 6 times

Question #147

What are two reasons to deploy multiple virtual networks instead of using just one virtual network? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. to meet governance policies
- B. to connect multiple types of resources
- C. to separate the resources for budgeting
- D. to isolate the resources

Correct Answer: **BD**

Community vote distribution

AD (79%)	BD (21%)
----------	----------

 **beam63** Highly Voted 1 year, 2 months ago

Seems to me it is: A and D.

The main reasons for segmentation are:

The ability to group related assets that are a part of (or support) workload operations.

Isolation of resources.

Governance policies set by the organization.

See: <https://learn.microsoft.com/en-us/azure/architecture/framework/security/design-network-segmentation>
upvoted 12 times

 **yasu_biztalc** Highly Voted 1 year, 2 months ago

A and D

upvoted 11 times

 **Aalkinani** Most Recent 1 week, 5 days ago

Selected Answer: AD

A. to meet governance policies: Some organizations may have governance policies that require certain resources or environments to be isolated from each other for security, compliance, or data protection reasons. Deploying multiple virtual networks allows these policies to be enforced effectively by isolating resources into separate networks.

D. to isolate the resources: By deploying multiple virtual networks, you can isolate different sets of resources from each other. This isolation enhances security by limiting the impact of potential security breaches or failures to specific sets of resources. It also allows for better network performance and resource management by reducing broadcast traffic and network congestion.

upvoted 1 times

 **mohammad1208** 7 months, 1 week ago

A & D is correct

upvoted 1 times

 **fiksarion** 8 months, 3 weeks ago

Question from SC900 - A and D

upvoted 3 times

 **dunget** 9 months, 2 weeks ago

Selected Answer: AD

like vlan

upvoted 1 times

 **mjg23** 11 months ago

Selected Answer: AD

A and D.

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: AD

AD is the answer.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm?source=recommendations#virtual-networks>

upvoted 1 times

 **obaali1990** 1 year, 1 month ago

Correct Answers: AD

upvoted 2 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: AD

A and D

upvoted 3 times

 **Tined** 1 year, 1 month ago

Selected Answer: AD

A and D

upvoted 3 times

 **examtopics11** 1 year, 1 month ago

Selected Answer: AD

agree with beam63 reference.

upvoted 3 times

 **nshm90** 1 year, 2 months ago

Selected Answer: AD

Agreed with yasu and beam.

Ans should be AD

upvoted 2 times

 **ETU69** 1 year, 2 months ago

Selected Answer: BD

Correct

upvoted 4 times

Question #148

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Sentinel provides quick insights into data by using

Azure Logic Apps.
Azure Monitor workbook templates.
Azure Resource Graph Explorer.
playbooks.

Microsoft Sentinel provides quick insights into data by using

Correct Answer:

Azure Logic Apps.
Azure Monitor workbook templates.
Azure Resource Graph Explorer.
playbooks.

 **cris_exam** Highly Voted 1 year, 2 months ago

Correct

<https://learn.microsoft.com/en-us/azure/sentinel/overview#create-interactive-reports-by-using-workbooks>
upvoted 5 times

 **zellck** Most Recent 11 months, 1 week ago

"Azure Monitor workbook templates" is the answer.

<https://learn.microsoft.com/en-us/azure/sentinel/overview#create-interactive-reports-by-using-workbooks>
After you onboard to Microsoft Sentinel, monitor your data by using the integration with Azure Monitor workbooks.

Workbooks display differently in Microsoft Sentinel than in Azure Monitor. But it may be useful for you to see how to create a workbook in Azure Monitor. Microsoft Sentinel allows you to create custom workbooks across your data. Microsoft Sentinel also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

upvoted 1 times

 **ETU69** 1 year, 2 months ago

Correct

upvoted 4 times

Question #149

Topic 1

You have an Azure subscription that contains multiple resources.

You need to assess compliance and enforce standards for the existing resources.

What should you use?

- A. Azure Blueprints
- B. the Anomaly Detector service
- C. Microsoft Sentinel
- D. Azure Policy

Correct Answer: D

Community vote distribution

D (100%)

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: D

Correct

upvoted 7 times

 **claudioosousa** Most Recent 2 months, 1 week ago

Selected Answer: D

D. Azure Policy

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/azure/governance/policy/overview>

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 2 times

 **Tined** 1 year, 1 month ago

Selected Answer: D

correct

upvoted 4 times

Question #150

Topic 1

Which Microsoft Defender for Cloud metric displays the overall security health of an Azure subscription?

- A. secure score
- B. resource health
- C. completed controls
- D. the status of recommendations

Correct Answer: A

Community vote distribution

A (100%)

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: A

Correct

upvoted 8 times

 **JS_Jasey** Highly Voted 1 year, 2 months ago

This is a tricky one, if it was resources issues/health then it would have been resources health BUT the question is Security health hence its Secure Score.

upvoted 5 times

 **zellck** Most Recent 11 months, 1 week ago

Selected Answer: A

A is the answer.

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#overview-of-secure-score>
Microsoft Defender for Cloud has two main goals:

- to help you understand your current security situation
- to help you efficiently and effectively improve your security

The central feature in Defender for Cloud that enables you to achieve those goals is the secure score.

Defender for Cloud continually assesses your cross-cloud resources for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

upvoted 4 times

 **obaali1990** 1 year, 1 month ago

Correct answer: A

upvoted 2 times

 **Mithu94** 1 year, 1 month ago

Selected Answer: A

Correct

upvoted 3 times

Question #151

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can use information barriers with Microsoft Exchange.	<input type="radio"/>	<input type="radio"/>
You can use information barriers with Microsoft SharePoint.	<input type="radio"/>	<input type="radio"/>
You can use information barriers with Microsoft Teams.	<input type="radio"/>	<input type="radio"/>

Correct Answer:	Answer Area		
	Statements	Yes	No
	You can use information barriers with Microsoft Exchange.	<input type="radio"/>	<input checked="" type="radio"/>
	You can use information barriers with Microsoft SharePoint.	<input checked="" type="radio"/>	<input type="radio"/>
	You can use information barriers with Microsoft Teams.	<input checked="" type="radio"/>	<input type="radio"/>

✉ **cris_exam** Highly Voted 1 year, 2 months ago

NO - <https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide#information-barriers-and-exchange-online>

Only Exchange Online deployments are currently supported for IB policies. If your organization needs to define and control email communications, consider using Exchange mail flow rules.

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.

YES - <https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide>

YES - <https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide>
upvoted 10 times

✉ **ETU69** Highly Voted 1 year, 2 months ago

Correct: <https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide>
upvoted 9 times

✉ **Tahamaffia** Most Recent 6 months, 2 weeks ago

Got this question on my exam 05/09/2023
upvoted 2 times

✉ **zellck** 11 months, 1 week ago

NNN is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers>

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.

upvoted 3 times

✉ **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/describe-insider-risk-capabilities-microsoft-365/4-describe-information-barriers>
Microsoft Purview Information Barriers is supported in Microsoft Teams, SharePoint Online, and OneDrive for Business.

upvoted 2 times

Question #152

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Insider risk management is configured from the

- Microsoft 365 admin center.
- Microsoft 365 compliance center.
- Microsoft 365 Defender portal.
- Microsoft Defender for Cloud Apps portal.

Answer Area

Insider risk management is configured from the

Correct Answer:

- Microsoft 365 admin center.
- Microsoft 365 compliance center.**
- Microsoft 365 Defender portal.
- Microsoft Defender for Cloud Apps portal.

 **dingtheking** Highly Voted 1 year, 2 months ago

Microsoft Purview compliance portal
upvoted 11 times

 **PinkUnicorns** Highly Voted 1 year, 2 months ago

its renamed so I assume the exam is still labelling it as M365 Compliance Center. Just remember its now Microsoft Purview.

Correct answer
upvoted 7 times

 **zellck** Most Recent 11 months, 1 week ago

"Microsoft 365 compliance center" is the answer.
It is now called Microsoft Purview compliance portal.

<https://learn.microsoft.com/en-us/training/modules/describe-insider-risk-capabilities-microsoft-365/2-management-solution>

Microsoft Purview Insider Risk Management is a solution that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Insider risk management is available in the Microsoft Purview compliance portal.

upvoted 2 times

 **SOCKa** 1 year, 2 months ago

Microsoft Purview
upvoted 3 times

 **ETU69** 1 year, 2 months ago

Correct: <https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-solution-overview?view=o365-worldwide>
upvoted 4 times

Question #153

Topic 1

You need to ensure repeatability when creating new resources in an Azure subscription.

What should you use?

- A. Microsoft Sentinel
- B. Azure Policy
- C. Azure Batch
- D. Azure Blueprints

Correct Answer: D

Community vote distribution

D (100%)

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: D

Correct

upvoted 7 times

 **jaaake** Most Recent 9 months, 1 week ago

Just like AWS CloudFormation, but with CloudFormation the logical link between the CloudFormation template and the VM created is broken permanently once the VM is created successfully (including all bootstrapping)

upvoted 1 times

 **zellck** 11 months, 1 week ago

Selected Answer: D

D is the answer.

<https://learn.microsoft.com/en-us/azure/governance/blueprints/overview>

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and start up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

upvoted 3 times

 **azure365lol** 11 months, 2 weeks ago

repeatable = blueprints

upvoted 4 times

Question #154

Topic 1

What is a characteristic of a sensitivity label in Microsoft 365?

- A. encrypted
- B. restricted to predefined categories
- C. persistent

Correct Answer: C

Community vote distribution

C (100%)

 **zellck** Highly Voted 11 months, 1 week ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-a-sensitivity-label-is>
When you assign a sensitivity label to content, it's like a stamp that's applied and is:

- Customizable. Specific to your organization and business needs, you can create categories for different levels of sensitive content in your organization. For example, Personal, Public, General, Confidential, and Highly Confidential.
- Clear text. Because a label is stored in clear text in the metadata for files and emails, third-party apps and services can read it and then apply their own protective actions, if required.
- Persistent. Because the label is stored in metadata for files and emails, the label stays with the content, no matter where it's saved or stored. The unique label identification becomes the basis for applying and enforcing policies that you configure.

upvoted 7 times

 **ETU69** Highly Voted 1 year, 2 months ago

Selected Answer: C

Coorect

upvoted 6 times

 **Darkfire** Most Recent 8 months ago

Selected Answer: C

Correct

Persistent = keyword to Sensitivity Label

upvoted 2 times

 **cris_exam** 1 year, 2 months ago

Selected Answer: C

Correct - <https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-a-sensitivity-label-is>

upvoted 6 times

Question #155

DRAG DROP

Match the Microsoft Purview Insider Risk Management workflow step to the appropriate task.

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

NOTE: Each correct match is worth one point.

Steps	Answer Area
Action	<input type="text"/>
Investigate	<input type="text"/>
Triage	<input type="text"/>

Review and filter alerts.

Create cases in the Case dashboard.

Send a reminder of corporate policies to users.

Answer Area	
Correct Answer:	Triage Review and filter alerts.
	Investigate Create cases in the Case dashboard.
	Action Send a reminder of corporate policies to users.

 **ETU69** Highly Voted  1 year, 2 months ago

Correct

upvoted 9 times

 **DanPicardi** Most Recent  8 months, 1 week ago

the given answer is correct

upvoted 1 times

 **zellck** 11 months, 1 week ago

1. Triage

2. Investigate

3. Action

<https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide#workflow>

upvoted 1 times

 **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/describe-insider-risk-capabilities-microsoft-365/2-management-solution>

Triage - New activities that need investigation automatically generate alerts that are assigned a Needs review status. Reviewers in the organization can quickly identify these alerts and scroll through each to evaluate and triage. As part of the triage process, reviewers can view alert details for the policy match, view user activity associated with the match, see the severity of the alert, and review user profile information.

Investigate - Cases are created for alerts that require deeper review and investigation of the details and circumstances around the policy match. The Case dashboard provides an all-up view of all active cases, open cases over time, and case statistics for the organization.

Action - After cases are investigated, reviewers can quickly act to resolve the case or collaborate with other risk stakeholders in the organization.

upvoted 2 times

Question #156

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Microsoft Purview provides sensitive data classification.	<input type="radio"/>	<input type="radio"/>
Microsoft Sentinel is a data lifecycle management solution.	<input type="radio"/>	<input type="radio"/>
Microsoft Purview can only discover data that is stored in Azure.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Correct Answer: Microsoft Purview provides sensitive data classification.	<input checked="" type="checkbox"/>	<input type="radio"/>
Microsoft Sentinel is a data lifecycle management solution.	<input checked="" type="checkbox"/>	<input type="radio"/>
Microsoft Purview can only discover data that is stored in Azure.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉  **KJUHIF**  1 year, 2 months ago

YNN is correct.
Purview is data lifecycle mgmtt solution
upvoted 19 times

✉  **OlikuTR**  4 months, 1 week ago

Remember bois

If you're not sure and you see "Only"

You HAVE 90% its an No
upvoted 6 times

✉  **tattybizzy** 1 week, 2 days ago
Great tip
upvoted 1 times

✉  **Aalkinani**  1 week, 5 days ago

Microsoft Purview provides sensitive data classification as part of its functionality, allowing organizations to identify and classify sensitive data across various data sources, not just those stored in Azure.

Microsoft Sentinel is primarily a security information and event management (SIEM) solution designed for security monitoring, threat detection, and incident response. It focuses on analyzing security data to provide insights and enable organizations to respond to security threats effectively. It is not primarily a data lifecycle management solution.

Microsoft Purview is capable of discovering data stored in various locations, including Azure, on-premises environments, other cloud platforms, and SaaS applications. It offers broad data discovery capabilities, allowing organizations to gain insights into their data estate regardless of where the data resides.

upvoted 2 times

✉  **dsharp** 8 months, 1 week ago

YNN
Sentinel is not data lifecycle management solution
upvoted 3 times

✉  **jaaake** 9 months, 1 week ago

Sentinel is not a Data Lifecycle Management solution: it's a SIEM and sort of a SOAR I guess
upvoted 2 times

 **zellck** 11 months, 1 week ago

YNN is the answer.

<https://learn.microsoft.com/en-us/azure/sentinel/overview>
Microsoft Sentinel is a scalable, cloud-native solution that provides:
- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)

<https://learn.microsoft.com/en-us/azure/purview/overview>

Microsoft Purview's solutions in the governance portal provide a unified data governance service that helps you manage your on-premises, multicloud, and software-as-a-service (SaaS) data.

upvoted 5 times

 **jj0097** 1 year ago

YNN is the correct one
upvoted 3 times

 **clauimagagnotti** 1 year ago

YNN is correct
upvoted 2 times

 **obaali1990** 1 year, 1 month ago

Correct answers: YNN
upvoted 2 times

 **Mithu94** 1 year, 1 month ago

YNN is correct
upvoted 2 times

 **luckyiki** 1 year, 2 months ago

YNN is correct
upvoted 3 times

 **ibonifac** 1 year, 2 months ago

Y,N,N - Microsoft Purview Data Lifecycle Management was formerly named Microsoft Information Governance. It helps organizations manage their risk through discovering, classifying, labeling, and governing their data. NOT Sentinel
upvoted 4 times

 **Sute_Sydney** 1 year, 2 months ago

Purview is data lifecycle management solution - Sentinel is only an Information and Event Log Manager.
upvoted 4 times

 **ETU69** 1 year, 2 months ago

Correct
upvoted 3 times

<https://www.examtopics.com/exams/microsoft/sc-900/custom-view/>

 **dingtheking** 1 year, 2 months ago

YNN is correct.
upvoted 5 times

Question #157

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Compliance score

Microsoft Purview compliance portal reports

The Trust Center

Trust Documents

measures a company's progress in completing actions that help reduce risks around data protection and regulatory standards.

Answer Area

Correct Answer: Compliance score

Microsoft 365 compliance center reports

The Trust Center

Trust Documents

measures a company's progress in completing actions that help reduce risks around data protection and regulatory standards.

✉ **MoneyStacking** Highly Voted 1 year, 2 months ago

We made it, good luck guys!

upvoted 15 times

✉ **ETU69** Highly Voted 1 year, 2 months ago

Correct

upvoted 6 times

✉ **zellck** Most Recent 11 months, 1 week ago

"Compliance score" is the answer.

<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide#understanding-your-compliance-score>
 Compliance Manager awards you points for completing improvement actions taken to comply with a regulation, standard, or policy, and combines those points into an overall compliance score. Each action has a different impact on your score depending on the potential risks involved. Your compliance score can help prioritize which action to focus on to improve your overall compliance posture.

Compliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance.

upvoted 3 times

✉ **zellck** 11 months, 1 week ago

<https://learn.microsoft.com/en-us/training/modules/describe-compliance-management-capabilities-microsoft-365/4-describe-compliance-score>

Compliance score measures progress in completing recommended improvement actions within controls. The score can help an organization to understand its current compliance posture. It also helps organizations to prioritize actions based on their potential to reduce risk.

upvoted 2 times

✉ **Gatorgirl** 1 year ago

I received an email from the ExamTopics support team last night. They said that there are in fact only 157 questions NOT 161. They are correcting the number of total questions to 157 as it should be. SO.....we all have ALL of the available questions (not missing any). Hope this helps!

upvoted 6 times

✉ **Paul_white** 1 year ago

Thanks, dear, you're a darling. i was worried

upvoted 2 times

✉ **YSHUANG** 1 year ago

where are question 158 to 161 ?

upvoted 3 times

✉ **Gatorgirl** 1 year ago

Did anyone get an answer to this question of why we are missing 4 questions (158-161)? I just sent an email to the ExamTopics Support team. I will post their answer if I get one. Just worried these will be 4 of the questions they will ask!!!

upvoted 1 times

✉ **[Removed]** 1 year, 1 month ago

"Viewing questions 157-157 out of 161 questions" as of Feb 20, 2023.

upvoted 4 times

Question #158

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Asymmetric encryption uses a public key and private key pair.	<input type="radio"/>	<input type="radio"/>
Symmetric encryption uses a public key and private key pair.	<input type="radio"/>	<input type="radio"/>
You can use decryption to retrieve original content from a content hash.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
Asymmetric encryption uses a public key and private key pair.	<input checked="" type="radio"/>	<input type="radio"/>
Symmetric encryption uses a public key and private key pair.	<input type="radio"/>	<input checked="" type="radio"/>
You can use decryption to retrieve original content from a content hash.	<input checked="" type="radio"/>	<input type="radio"/>

Beita Highly Voted 11 months, 3 weeks ago

Should be YNN
upvoted 15 times

zellck Highly Voted 11 months, 1 week ago

YNN is the answer.

<https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/5-describe-encryption-hashing>
Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original.
upvoted 6 times

tc_praveen Most Recent 3 months ago

YNN is the answer.
upvoted 1 times

dsharp 8 months, 1 week ago

YNN it is of course
There is no way to decrypt back from a hash!
upvoted 3 times

jaaake 9 months, 1 week ago

Indeed its YNN. With reference to the 3rd point, you there's no way back from the hash to the original content
upvoted 1 times

manofsteel9 10 months ago

Answer should be YNN.
upvoted 3 times

la_toupi 11 months ago

YNN , the hash solution is not use to decrypt
upvoted 4 times

XtraWest 11 months, 1 week ago

Last one N as per bing ai
upvoted 4 times

✉  **wstydiwy_tajnder** 11 months, 2 weeks ago
of course should be YNN
upvoted 4 times

Question #159

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area**Statements**

Asymmetric encryption uses a public key and private key pair.

Yes**No**

Symmetric encryption uses a public key and private key pair.

You can use decryption to retrieve original content from a content hash.

Correct Answer:**Answer Area****Statements**

Asymmetric encryption uses a public key and private key pair.

Yes**No**

Symmetric encryption uses a public key and private key pair.

You can use decryption to retrieve original content from a content hash.

✉  **jaaake**  9 months, 1 week ago

A copy of #158 but this time with the correct answer
upvoted 7 times

Question #160

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining

▼
availability.
confidentiality.
integrity.
transparency.

Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining

Correct Answer:

▼
availability.
confidentiality.
integrity.
transparency.

✉  **Darkfire** 8 months ago

Integrity = correct

<https://learn.microsoft.com/en-us/compliance/assurance/assurance-dealing-with-data-corruption>

<https://learn.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes>

upvoted 3 times

✉  **Molota** 9 months, 1 week ago

Correct: ensuring DATA is not altered...."Integrity"

upvoted 3 times

Question #161

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

▼	
Assessments	
Improvement actions	
Solutions	
Templates	

track compliance with groupings of controls from a specific regulation or requirement.

▼	
Assessments	
Improvement actions	
Solutions	
Templates	

track compliance with groupings of controls from a specific regulation or requirement.

Correct Answer:

-  **DanPicardi** 8 months, 1 week ago
the answer is correct
upvoted 1 times

-  **deroen** 8 months, 2 weeks ago

assessments - Compliance Manager assessments help your organization evaluate its compliance with industry and regional regulations.
<https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments>

upvoted 3 times

Question #162

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
In software as a service (SaaS), applying application updates is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input type="radio"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input type="radio"/>	<input type="radio"/>

Statements	Yes	No
In software as a service (SaaS), applying application updates is the responsibility of the organization.	<input type="radio"/>	<input checked="" type="checkbox"/>
Correct Answer: In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	<input checked="" type="checkbox"/>	<input type="radio"/>
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉  **chrisan99** Highly Voted 9 months, 3 weeks ago

Surely this is N,Y,Y

upvoted 23 times

✉  **Paddy71** Most Recent 3 months ago

There seem to be more answers wrong than correct – this is annoying – I doubt the paid value of this service

upvoted 2 times

✉  **TomG** 7 months, 1 week ago

It should be No Yes Yes since Information and Data always organisation's responsibilities not cloud providers

upvoted 1 times

✉  **Darkfire** 8 months ago

I vote NNY

<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

1. SaaS = Software as a Service, you consume the hosted application from Microsoft. The updates are the responsibility of the hoster.

2. IaaS = Infrastructure as a Service, the Cloud hoster is responsible for Physical hosts, Physical network and Physical datacenter.

3. For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type).

upvoted 2 times

✉  **Mizlett** 2 weeks, 3 days ago

You're saying is NNY... but the logic you outlined indicates the answer NYY..for IaaS the cloud service provider is responsible for the network. My vote is NYY

upvoted 2 times

✉  **Mehe323** 8 months ago

From the SC-900 course from Microsoft:

Responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

upvoted 2 times

✉  **DanPicardi** 8 months, 1 week ago

the given answer is correct NYY

upvoted 2 times

✉  **dsharp** 8 months, 1 week ago

also voting NYY
upvoted 2 times

 **jaaake** 9 months, 1 week ago
Perhaps the wrong answers are intentional to spark the discussion.
upvoted 3 times

 **Molota** 9 months, 1 week ago
NYY should be the response
upvoted 4 times

 **kodathedog** 9 months, 2 weeks ago
NYY is the correct answer.
upvoted 3 times

 **wborquez** 9 months, 2 weeks ago
NYY es la respuesta correcta
upvoted 2 times

 **Jae_eef06** 9 months, 2 weeks ago
NYY is the correct answer
upvoted 2 times

Question #163

Topic 1

What should you use to associate the same identity to more than one Azure virtual machine?

- A. an Azure AD user account
- B. a user-assigned managed identity
- C. a system-assigned managed identity
- D. an Azure AD security group

Correct Answer: B

Community vote distribution

 B (100%)

 **mohammad1208** 7 months, 1 week ago
B is correct
upvoted 1 times

 **Darkfire** 8 months ago
Selected Answer: B
B is correct

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>
You can create a user-assigned managed identity and assign it to one or more Azure Resources.
upvoted 3 times

 **novak18** 9 months, 2 weeks ago
The given answer is correct

Supporting links below:

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-portal-windows-vm>

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-manage-user-assigned-managed-identities?pivot=identity-mi-methods-apz#manage-access-to-user-assigned-managed-identities>

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/qs-configure-cli-windows-vm>
upvoted 2 times

Question #164

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Security defaults require an Azure AD Premium license.	<input type="radio"/>	<input type="radio"/>
Security defaults can be enabled for a single Azure AD user.	<input type="radio"/>	<input type="radio"/>
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	<input type="radio"/>	<input type="radio"/>

Statements	Yes	No
Security defaults require an Azure AD Premium license.	<input type="radio"/>	<input checked="" type="radio"/>
Correct Answer: Security defaults can be enabled for a single Azure AD user.	<input type="radio"/>	<input checked="" type="radio"/>
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	<input checked="" type="radio"/>	<input type="radio"/>

✉  Darkfire 8 months ago

Answers are correct

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>
upvoted 2 times

✉  lilou123 9 months ago

Correct answer
upvoted 1 times

Question #165

Topic 1

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

Community vote distribution

BCE (100%)

✉  **Darkfire** 8 months ago

Selected Answer: BCE

Correct

upvoted 4 times

✉  **jaaake** 9 months, 1 week ago

Indeed. Security questions can be used for SSPR

upvoted 1 times

✉  **Molota** 9 months, 1 week ago

The given answer is correct

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
upvoted 1 times

✉  **novak18** 9 months, 2 weeks ago

The given answer is correct

Supporting link below:

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

upvoted 1 times

Question #166

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
An external email address can be used to authenticate self-service password reset (SSPR).	<input checked="" type="checkbox"/>	<input type="radio"/>
A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	<input checked="" type="checkbox"/>	<input type="radio"/>
To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	<input type="radio"/>	<input checked="" type="checkbox"/>

✉ **kodathedog** Highly Voted 9 months, 2 weeks ago

YYN is correct, see <https://learn.microsoft.com/en-us/training/modules/explore-authentication-capabilities/4-describe-self-service-password-reset>, "The following authentication methods are available for SSPR: Email"

upvoted 5 times

✉ **azhrhsn** Most Recent 2 months, 2 weeks ago

YYN is correct.
Azure AD allows users to register multiple authentication methods, including external email addresses, phone numbers, or authentication apps. These methods can serve as alternate means for users to reset their passwords securely without administrator intervention.

upvoted 2 times

✉ **mohammad1208** 7 months, 1 week ago

YYN
<https://learn.microsoft.com/en-us/training/modules/explore-authentication-capabilities/4-describe-self-service-password-reset>

upvoted 4 times

✉ **Molota** 9 months, 1 week ago

Should be:

NYN

upvoted 2 times

✉ **Docxx** 9 months, 2 weeks ago

1 - NO, because it only send by email a verification code to reset the password
<https://www.youtube.com/embed/rA8TvhNcCvQ?azure-portal=true>

upvoted 2 times

✉ **DanPicardi** 8 months, 2 weeks ago

Directly from <https://learn.microsoft.com/en-us/training/modules/explore-authentication-capabilities/4-describe-self-service-password-reset>

The following authentication methods are available for SSPR:

Mobile app notification

Mobile app code

Email

Mobile phone

Office phone

Security questions

so the correct answers should be YYN
upvoted 2 times

Question #167

Topic 1

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) can be used on which operating systems?

- A. Windows 10 and newer only
- B. Windows 10 and newer and Android only
- C. Windows 10 and newer and macOS only
- D. Windows 10 and newer, Android, and macOS

Correct Answer: C

Community vote distribution

C (100%)

-  **azhrhsn** 2 months, 2 weeks ago
C. Windows 10 and newer and macOS only
upvoted 1 times
-  **mohammad1208** 7 months, 1 week ago
C is correct
upvoted 1 times
-  **Darkfire** 8 months ago
Selected Answer: C
C is correct

<https://learn.microsoft.com/en-us/purview/endpoint-dlp-getting-started?view=o365-worldwide#see-also>
Microsoft Endpoint DLP allows you to monitor onboarded Windows 10, and Windows 11 and onboarded macOS devices running any of the three latest released versions.

There is also an variation of this question where iOS is mentioned.

iOS = for mobile OS
MacOS = for desktops/laptops

iOS = not supported for Endpoint Data Loss Prevention.
upvoted 2 times

-  **novak18** 9 months, 2 weeks ago
The given answer is correct

Supporting link below:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide#see-also>
upvoted 3 times

-  **novak18** 9 months, 1 week ago
I'm wondering if D is the actual answer and not C
upvoted 2 times
-  **DanPicardi** 8 months, 1 week ago
the answer is C... just Windows 10 and newer and macOS only devices
upvoted 1 times

Question #168

Topic 1

You have an Azure subscription that contains a Log Analytics workspace.

You need to onboard Microsoft Sentinel.

What should you do first?

- A. Create a hunting query.
- B. Correlate alerts into incidents.
- C. Connect to your security sources.
- D. Create a custom detection rule.

Correct Answer: C

Community vote distribution

C (100%)

bindadarsh7 7 months ago

C. Connect to your security sources.
upvoted 1 times

Darkfire 8 months ago

Selected Answer: C

C is correct

<https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources>

After you onboard Microsoft Sentinel into your workspace, use data connectors to start ingesting your data into Microsoft Sentinel. Microsoft Sentinel comes with many out of the box connectors for Microsoft services, which integrate in real time. For example, the Microsoft 365 Defender connector is a service-to-service connector that integrates data from Office 365, Azure Active Directory (Azure AD), Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps.

upvoted 3 times

DanPicardi 8 months, 1 week ago

the answer is correct
upvoted 2 times

novak18 9 months, 2 weeks ago

The given answer is correct

The support link below might be the one, not sure

Link >> <https://learn.microsoft.com/en-us/azure/sentinel/best-practices-workspace-architecture>

upvoted 3 times

Question #169

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	<input type="radio"/>	<input type="radio"/>
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	<input type="radio"/>	<input type="radio"/>
Azure DDoS Protection Standard protects against protocol attacks.	<input type="radio"/>	<input type="radio"/>

Answer Area

	Statements	Yes	No
Correct Answer:	Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	<input type="radio"/>	<input checked="" type="radio"/>
	Azure DDoS Protection Standard is enabled by default in an Azure subscription.	<input type="radio"/>	<input checked="" type="radio"/>
	Azure DDoS Protection Standard protects against protocol attacks.	<input checked="" type="radio"/>	<input type="radio"/>

 novak18 Highly Voted 9 months, 2 weeks ago

The given answer is correct

Supporting links below:

<https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview>

<https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-features>
upvoted 8 times

Question #170

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

The features of Microsoft Defender for Cloud block malware and other unwanted applications, while reducing the network attack surface on Azure virtual machines.

- access and application control
- Cloud Security Posture Management (CSPM)
- container security
- vulnerability assessment

Correct Answer:

Answer Area

The features of Microsoft Defender for Cloud block malware and other unwanted applications, while reducing the network attack surface on Azure virtual machines.

- access and application control
- Cloud Security Posture Management (CSPM)
- container security
- vulnerability assessment

novak18 Highly Voted 9 months, 2 weeks ago

I think the given answer is correct

Supporting links below:

<https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls>

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

upvoted 8 times

tc_praeven Most Recent 3 months, 1 week ago

Correct answer.

upvoted 2 times

Question #171

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can use Microsoft Purview Information Barriers to detect messages that contain inappropriate language.	<input type="radio"/>	<input type="radio"/>
You can use Microsoft Purview Communication Compliance to scan files stored in Microsoft SharePoint Online.	<input type="radio"/>	<input type="radio"/>
You can use Microsoft Purview Communication Compliance to scan internal and external emails in Microsoft Exchange Online	<input type="radio"/>	<input type="radio"/>

Answer Area			
	Statements	Yes	No
Correct Answer:	You can use Microsoft Purview Information Barriers to detect messages that contain inappropriate language.	<input type="radio"/>	<input checked="" type="radio"/>
	You can use Microsoft Purview Communication Compliance to scan files stored in Microsoft SharePoint Online.	<input type="radio"/>	<input checked="" type="radio"/>
	You can use Microsoft Purview Communication Compliance to scan internal and external emails in Microsoft Exchange Online	<input checked="" type="radio"/>	<input type="radio"/>

✉️  **chrisan99** Highly Voted 9 months, 3 weeks ago

I think this is YNY
<https://learn.microsoft.com/en-us/microsoft-365/compliance/communication-compliance-policies?view=o365-worldwide>
 upvoted 6 times

✉️  **Mehe323** 8 months ago

The statement refers to detecting. According to the SC-900 learning path:

"Information barriers are policies that admins can configure to prevent individuals or groups from communicating with each other."

Barriers are about putting controls in place, not about detecting.

upvoted 5 times

✉️  **tc_praveen** Most Recent 3 months, 1 week ago

YNY is correct.

Microsoft Purview Communication Compliance provides the tools to help organizations detect regulatory compliance (for example, SEC or FINRA) and business conduct violations such as sensitive or confidential information, harassing or threatening language, and sharing of adult content.
 upvoted 1 times

✉️  **Darkfire** 8 months ago

NNY is correct

Informational Barriers

<https://learn.microsoft.com/en-us/purview/information-barriers?view=o365-worldwide>

Communication Compliance

<https://learn.microsoft.com/en-us/purview/communication-compliance?view=o365-worldwide>

upvoted 3 times

✉️  **Kikinova** 8 months, 2 weeks ago

Answers are correct. Woohoo you have made it ! Good luck Guys for your exam !

upvoted 1 times

✉ **jaaake** 9 months ago

NNY is correct. With reference to the second point, I believe the design intention of Communication Compliance is to apply it to tools that are used to communicate explicitly, and hence SharePoint Online was omitted. Having said that, I wouldn't be surprised if it was included in the future.

upvoted 1 times

✉ **kodathedog** 9 months, 2 weeks ago

NNY is correct.
upvoted 3 times

✉ **novak18** 9 months, 2 weeks ago

I think the given answer is correct which is NNY

Supporting links below:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide#integration-with-microsoft-365-services>

upvoted 1 times

Question #172

Topic 1

HOTSPOT

-

Select the answer that correctly completes the sentence.

Answer Area

Single sign-on (SSO) configured between multiple identity providers is an example of

federation.
integration.
password hash synchronization.
pass-through authentication.

Answer Area

Correct Answer:

Single sign-on (SSO) configured between multiple identity providers is an example of

federation.
integration.
password hash synchronization.
pass-through authentication.

✉ **Darkfire** Highly Voted 8 months ago

Answer is correct

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-fed>

upvoted 7 times

✉ **bindadarsh7** Most Recent 7 months ago

Federation is correct.
upvoted 3 times

Question #173

Topic 1

You plan to move resources to the cloud.

You are evaluating the use of Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) cloud models.

You plan to manage only the data, user accounts, and user devices for a cloud-based app.

Which cloud model will you use?

- A. SaaS
- B. PaaS
- C. IaaS

Correct Answer: A

Community vote distribution

A (100%)

✉️ 🚑 Ayind3 4 months, 2 weeks ago

Intune, is that you?

upvoted 1 times

✉️ 🚑 Darkfire 8 months ago

Selected Answer: A

A is correct

<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Responsibility always retained by the customer:

- Information and Data
- Devices (Mobile and PCs)
- Accounts and Identities

upvoted 4 times

Question #174

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Enabling a system-assigned managed identity creates a service principal that

- can be shared with multiple Azure resources.
- is managed separately from the resource that uses it.
- is tied to the lifecycle of the resource that uses it.
- must be registered manually with Azure AD.

Correct Answer:

Answer Area

Enabling a system-assigned managed identity creates a service principal that

- can be shared with multiple Azure resources.
- is managed separately from the resource that uses it.
- is tied to the lifecycle of the resource that uses it.
- must be registered manually with Azure AD.

 **mohammad1208** 7 months, 1 week ago

Answer is correct

upvoted 2 times

 **Darkfire** 8 months ago

Answer is correct

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

A service principal of a special type is created in Azure AD for the identity. The service principal is tied to the lifecycle of that Azure resource. When the Azure resource is deleted, Azure automatically deletes the service principal for you.

upvoted 2 times

Question #175

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device identity can be stored in Azure AD.	<input type="radio"/>	<input type="radio"/>
A single system-assigned managed identity can be used by multiple Azure resources.	<input type="radio"/>	<input type="radio"/>
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Device identity can be stored in Azure AD.	<input checked="" type="checkbox"/>	<input type="radio"/>
A single system-assigned managed identity can be used by multiple Azure resources.	<input type="radio"/>	<input checked="" type="checkbox"/>
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	<input type="radio"/>	<input checked="" type="checkbox"/>

 **mohammad1208** Highly Voted 7 months, 1 week ago

YNN is correct
upvoted 6 times

 **ICTzaakwaarnemer** Most Recent 4 months, 1 week ago

YNY is correct
upvoted 3 times

 **tattybizzy** 1 week, 2 days ago

No. A user assigned managed identity can exist even after the resource has been deleted. This is the key difference between user assigned and system assigned identities.
upvoted 1 times

 **Darkfire** 8 months ago

Answer is correct

<https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>
upvoted 4 times

 **DanPicardi** 8 months, 1 week ago

the answer is correct
upvoted 4 times

Question #176

Topic 1

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

- A. Adoption Score
- B. Microsoft Secure Score
- C. Secure score in Microsoft Defender for Cloud
- D. Compliance score

Correct Answer: D

Community vote distribution

D (100%)

 **Darkfire** 8 months ago

Selected Answer: D

Answer is correct

<https://learn.microsoft.com/en-us/purview/compliance-score-calculation>
upvoted 3 times

Question #177

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider.	<input type="radio"/>	<input type="radio"/>
Federation provides single sign-on (SSO) with multiple service providers.	<input type="radio"/>	<input type="radio"/>
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider.	<input checked="" type="checkbox"/>	<input type="radio"/>
Federation provides single sign-on (SSO) with multiple service providers.	<input checked="" type="checkbox"/>	<input type="radio"/>
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	<input type="radio"/>	<input checked="" type="checkbox"/>

bigvic18 Highly Voted 8 months, 1 week ago

GitHub is listed as one of the identity providers. Check the Microsoft document: <https://learn.microsoft.com/en-us/azure/app-service/overview-authentication-authorization#identity-providers>

upvoted 7 times

DanPicardi 8 months, 1 week ago

so the correct answer is YYN

upvoted 1 times

Arv84 Most Recent 2 months, 2 weeks ago

YYY

Federation - When you set up SSO to work between multiple identity providers, it's called federation.

With modern authentication, all services, including all authentication services, are supplied by a central identity provider.

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjm8ZCS3c-DAxWVT2wGHRXvCj8QFnoECAgQAw&url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fentra%2Ffundamentals%2Fidentity-fundamental-concepts%23%3A~%3Atext%3DWith%2520modern%2520authentication%252C%2520all%2520services%2Ccentrally%2520by%2520the%2520identity%2520provider.&usg=AOvVaw0pWfksnhx1_cfOUT03axGi&opi=89978449

upvoted 2 times

Paddy71 3 months ago

And another one wrong in this....

An identity provider creates, maintains, and manages identity information while offering authentication, authorization, and auditing services.
<https://learn.microsoft.com/en-us/entra/fundamentals/identity-fundamental-concepts>

upvoted 1 times

Tomix 5 months ago

so the correct answer is NYY
upvoted 1 times

 **dsharp** 8 months, 1 week ago

NYN
GitHub surely isn't an identity provider.
A modern identity provider should manage authentication and authorization but auditing might be managed by a separate system.
upvoted 1 times

 **dsharp** 8 months, 1 week ago

The answer should be NYY
From the ppt presentation slides:
"IdP offers authentication, authorization, and auditing services."
upvoted 1 times

 **tubsss** 4 months, 3 weeks ago

the answer would be YYY I think since Github is seen as a IP.
upvoted 4 times

 **DanPicardi** 8 months, 1 week ago

Correct YYN. Git Hub can be used as Identity Provider
upvoted 1 times

Question #178

Topic 1

DRAG DROP

You need to identify which cloud service models place the most responsibility on the customer in a shared responsibility model.

In which order should you list the service models from the most customer responsibility to the least? To answer, move all models from the list of models to the answer area and arrange them in the correct order.

Models

- platform as a service (PaaS)
- software as a service (SaaS)
- on-premises datacenter
- infrastructure as a service (IaaS)

Answer Area



Correct Answer:

- | Answer Area |
|------------------------------------|
| on-premises datacenter |
| infrastructure as a service (IaaS) |
| platform as a service (PaaS) |
| software as a service (SaaS) |

 **Darkfire** Highly Voted 8 months ago

Answer is correct

<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
upvoted 7 times

 **tc_praveen** Most Recent 3 months, 1 week ago

Answer is correct
upvoted 2 times

 **bda92b3** 5 months ago

Correct answer
upvoted 2 times

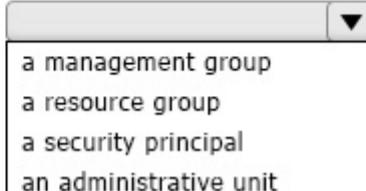
Question #179

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can assign  to an Azure AD role.

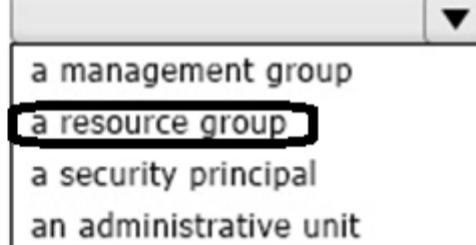
- a management group
- a resource group
- a security principal
- an administrative unit

Answer Area

You can assign

to an Azure AD role.

Correct Answer:

- 
- a management group
 - a resource group**
 - a security principal
 - an administrative unit

 tc_praveen 3 months, 1 week ago

Service principal.

On the Members tab, select User, group, or service principal to assign the selected role to one or more Microsoft Entra users, groups, or service principals (applications).

Click Select members. Find and select the users, groups, or service principals.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal#:~:text=On%20the%20Members%20tab%2C%20select,%2C%20groups%2C%20or%20service%20principals.>

upvoted 1 times

 Roy2022 1 day, 20 hours ago

But the answer says "security" think its a typo

upvoted 1 times

 Tomix 5 months ago

security principle

upvoted 3 times

 jai0000 5 months, 1 week ago

security principle

upvoted 1 times

 DanPicardi 8 months, 1 week ago

Security Principal should be the correct answer

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

upvoted 3 times

 dsharp 8 months, 1 week ago

Security principal should be the answer.

You can assigns security principal to an Azure AD Role.

You cannot directly assign a resource group to Azure AD Role.

upvoted 3 times

Question #180

You have an Azure subscription.

You need to implement approval-based, time-bound role activation.

What should you use?

- A. access reviews in Azure AD
- B. Azure AD Privileged Identity Management (PIM)
- C. Azure AD Identity Protection
- D. Conditional access in Azure AD

Correct Answer: B

Community vote distribution

B (100%)

✉  **Darkfire** 8 months ago

Selected Answer: B

B is correct answer

upvoted 3 times

✉  **DanPicardi** 8 months, 1 week ago

Correct

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

upvoted 3 times

Question #181

What should you use in the Microsoft 365 Defender portal to view security trends and track the protection status of identities?

- A. Reports
- B. Incidents
- C. Hunting
- D. Secure score

Correct Answer: A

Community vote distribution

A (100%)

✉  **azhrhsn** 2 months, 2 weeks ago

A. Reports

The "Reports" section within the Microsoft 365 Defender portal provides a comprehensive view of security-related data and trends, including insights into identity-related security events and the protection status of identities across your Microsoft 365 environment.

upvoted 1 times

✉  **Darkfire** 8 months ago

Selected Answer: A

A is correct

Keywords = trends and track = Reports

upvoted 3 times

Question #182

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area▼

- Azure Application Insights
- Azure Network Watcher
- Log Analytics workspaces
- Microsoft cloud security benchmark**

provides baseline recommendations and guidance for protecting Azure services.

Correct Answer:

Answer Area▼

- Azure Application Insights
- Azure Network Watcher
- Log Analytics workspaces
- Microsoft cloud security benchmark**

provides baseline recommendations and guidance for protecting Azure services.

 **mohammad1208** 7 months, 1 week ago

Correct

upvoted 1 times

 **Darkfire** 8 months ago

Answer is correct

<https://learn.microsoft.com/en-us/security/benchmark/azure/overview>

upvoted 2 times

Question #183

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	<input type="radio"/>	<input type="radio"/>
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	<input type="radio"/>	<input type="radio"/>
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	<input type="radio"/>	<input checked="" type="radio"/>
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	<input checked="" type="radio"/>	<input type="radio"/>

✉️  **xRiot007**  6 months, 1 week ago

No - Sentinel uses Logic Apps to automate workflows via playbooks

No - Sentinel uses analytics to correlate alerts into incidents

Yes - <https://learn.microsoft.com/en-us/azure/sentinel/overview#hunt-for-security-threats-by-using-built-in-queries>

upvoted 5 times

✉️  **Darkfire**  8 months ago

Answer is correct

<https://learn.microsoft.com/en-us/azure/sentinel/overview>

upvoted 2 times

✉️  **dsharp** 8 months, 1 week ago

Correct

upvoted 2 times

Question #184

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	<input type="radio"/>	<input type="radio"/>
You can restrict accessing a SharePoint Online site by using Information Barriers.	<input type="radio"/>	<input type="radio"/>
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	<input checked="" type="radio"/>	<input type="radio"/>
You can restrict accessing a SharePoint Online site by using Information Barriers.	<input checked="" type="radio"/>	<input type="radio"/>
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	<input checked="" type="radio"/>	<input type="radio"/>

 **dsharp** Highly Voted 8 months, 1 week ago

NYY

You cannot restrict communication through Exchange/mail.

upvoted 9 times

 **DanPicardi** 8 months, 1 week ago

I think you're right!

upvoted 2 times

 **Ramye** Most Recent 3 months, 1 week ago

Given answers are correct - YYY

Information barriers and SharePoint and OneDrive

In SharePoint and OneDrive, IB policies detect and prevent the following kinds of unauthorized collaboration:

Adding a member to a site

Accessing site or content by a user

Sharing site or content with another user

Searching a site

For more information, see Information barriers in SharePoint and Information barriers in OneDrive.

Information barriers and Exchange Online

IB policies aren't available to restrict communication and collaboration between groups and users in email messages. Only Exchange Online deployments are currently supported for IB policies.

Source: <https://learn.microsoft.com/en-us/purview/information-barriers>

upvoted 1 times

 **Ramye** 3 months ago

The keyword is Exchange Online that supports information barriers functionality
upvoted 1 times

 **tc_praveen** 3 months, 1 week ago

NYY

Can't restrict communication through Exchange/mail.

upvoted 1 times

 **Curious76** 7 months ago

NYY

Microsoft Exchange Online does not natively support Information Barriers for restricting communication between users. Information Barriers are typically a feature found in Microsoft Teams and SharePoint Online to prevent certain users or groups from communicating or collaborating with each other.

upvoted 2 times

 **Darkfire** 8 months ago

Should be NYY

YYY is correct

<https://learn.microsoft.com/en-us/purview/information-barriers?view=o365-worldwide>

IB policies aren't available to restrict communication and collaboration between groups and users in email messages. Only Exchange Online deployments are currently supported for IB policies. If your organization needs to define and control email communications, consider using Exchange mail flow rules.

upvoted 1 times

 **dsharp** 8 months, 1 week ago

NYY

You cannot restrict only mail communication

upvoted 2 times

 **DanPicardi** 8 months, 1 week ago

YYY correct

upvoted 1 times

Question #185

Topic 1

Which portal contains the solution catalog?

- A. Microsoft Purview compliance portal
- B. Microsoft 365 Defender portal
- C. Microsoft 365 admin center
- D. Microsoft 365 Apps admin center

Correct Answer: A

Community vote distribution

A (100%)

 **DanPicardi** Highly Voted 8 months, 1 week ago

Correct

<https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-solution-catalog?view=o365-worldwide>

upvoted 6 times

 **azhrhsn** Most Recent 2 months, 2 weeks ago

B. Microsoft 365 Defender portal

The Microsoft 365 Defender portal contains the solution catalog, which encompasses a collection of security solutions and tools to manage and strengthen the security posture of your Microsoft 365 environment.

upvoted 2 times

 **tc_praveen** 3 months, 1 week ago

A is correct

upvoted 2 times

 **Darkfire** 8 months ago

Selected Answer: A

A is correct

upvoted 4 times

Question #186

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

In the Microsoft Purview compliance portal, you can use  to remove features from the navigation pane.

- Compliance Manager
- Customize navigation
- Policies
- Settings

Correct Answer:

Answer Area

In the Microsoft Purview compliance portal, you can use  to remove features from the navigation pane.

- Compliance Manager
- Customize navigation
- Policies
- Settings

 **tc_praVeEN** 3 months, 1 week ago

Correct Answer.

upvoted 1 times

 **CertAddict69** 7 months, 2 weeks ago

Terrible wording.

upvoted 2 times

 **Darkfire** 8 months ago

Answer is correct

upvoted 1 times

 **DanPicardi** 8 months, 1 week ago

The answer is correct

<https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide>

upvoted 3 times

Question #187

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Communication compliance is configured by using the Microsoft 365 admin center.	<input type="radio"/>	<input type="radio"/>
Microsoft SharePoint Online supports communication compliance.	<input type="radio"/>	<input type="radio"/>
Communication compliance can remediate compliance issues.	<input type="radio"/>	<input type="radio"/>

Correct Answer:	Answer Area												
	<table border="1"> <thead> <tr> <th>Statements</th> <th>Yes</th> <th>No</th> </tr> </thead> <tbody> <tr> <td>Communication compliance is configured by using the Microsoft 365 admin center.</td> <td><input type="radio"/></td> <td><input checked="" type="radio"/></td> </tr> <tr> <td>Microsoft SharePoint Online supports communication compliance.</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Communication compliance can remediate compliance issues.</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> </tbody> </table>	Statements	Yes	No	Communication compliance is configured by using the Microsoft 365 admin center.	<input type="radio"/>	<input checked="" type="radio"/>	Microsoft SharePoint Online supports communication compliance.	<input checked="" type="radio"/>	<input type="radio"/>	Communication compliance can remediate compliance issues.	<input checked="" type="radio"/>	<input type="radio"/>
Statements	Yes	No											
Communication compliance is configured by using the Microsoft 365 admin center.	<input type="radio"/>	<input checked="" type="radio"/>											
Microsoft SharePoint Online supports communication compliance.	<input checked="" type="radio"/>	<input type="radio"/>											
Communication compliance can remediate compliance issues.	<input checked="" type="radio"/>	<input type="radio"/>											

MonicaKarim 2 weeks, 4 days ago

I believe it's no no yes
 1. Microsoft purview not admin center
 2. <https://learn.microsoft.com/en-us/purview/communication-compliance>
 3. Correct
 upvoted 2 times

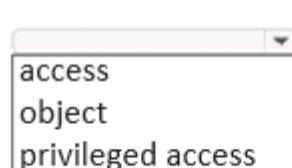
Question #188

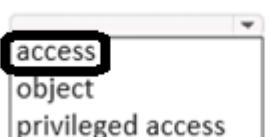
Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can use dynamic groups in Azure AD to automate the  lifecycle process.

Correct Answer:	Answer Area
	<p>You can use dynamic groups in Azure AD to automate the  lifecycle process.</p>

Question #189

Topic 1

When you enable Azure AD Multi-Factor Authentication (MFA), how many factors are required for authentication?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: B

Question #190

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Microsoft Defender for Cloud assesses Azure resources

- continuously
- daily
- every 15 minutes
- hourly

for security issues.

Correct Answer:

Answer Area

Microsoft Defender for Cloud assesses Azure resources

- continuously
- daily
- every 15 minutes
- hourly

for security issues.

Question #191

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Retention policies assign the same retention settings to all the files in a Microsoft SharePoint Online library.	<input type="radio"/>	<input type="radio"/>
Retention labels can be assigned to individual files and email messages.	<input type="radio"/>	<input type="radio"/>
You can assign multiple retention labels to an email message or a document.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
Retention policies assign the same retention settings to all the files in a Microsoft SharePoint Online library.	<input checked="" type="checkbox"/>	<input type="radio"/>
Retention labels can be assigned to individual files and email messages.	<input checked="" type="checkbox"/>	<input type="radio"/>
You can assign multiple retention labels to an email message or a document.	<input type="radio"/>	<input checked="" type="checkbox"/>

  Kozilla 1 month ago

correct

upvoted 1 times

Question #192

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

- A certificate
- A service principal
- A system-assigned managed identity
- A user-assigned managed identity

Answer Area

- Correct Answer:
- A certificate
 - A service principal
 - A system-assigned managed identity
 - A user-assigned managed identity

 ICTZaakwaarnemer 1 day, 16 hours ago

A user-assigned identity is a standalone Azure resource that can be assigned to your app. An app can have multiple user-assigned identities.
So, he's

upvoted 1 times

Question #193

Topic 1

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Conditional Access policies are enforced first-factor authentication.

- after
- before
- during
- instead of

Answer Area

Correct Answer:
Conditional Access policies are enforced after first-factor authentication.

 RasmusOestergaard 1 month, 1 week ago

Correct see <https://learn.microsoft.com/en-us/entra/identity/conditional-access/location-condition>
upvoted 2 times

Question #194

Topic 1

DRAG DROP

Match the types of Conditional Access signals to the appropriate definitions.

To answer, drag the appropriate Conditional Access signal type from the column on the left to its definition on the right. Each signal type may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Conditional access signals

Device
Location
Sign-in risk
User risk

Answer Area

The probability that an identity or account is compromised.

--

The probability that an authentication request isn't authorized by the identity owner.

Question #195

Topic 1

Which Microsoft Purview solution can be used to identify data leakage?

- A. insider risk management
- B. Compliance Manager
- C. communication compliance
- D. eDiscovery

Correct Answer: A

Question #196

Topic 1

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

<https://shop335422782.taobao.com> 淘宝搜索店铺:黑马专业认证
微信添加 hello231119

Answer Area

Statements	Yes	No
Conditional Access is implemented by using policies in Microsoft Entra ID.	<input type="radio"/>	<input type="radio"/>
A Conditional Access policy can block or allow Microsoft Entra ID connections based upon the specific platform of a user's device.	<input type="radio"/>	<input type="radio"/>
A Conditional Access policy can be applied to a Microsoft 365 group.	<input type="radio"/>	<input type="radio"/>

Answer Area

Correct Answer:

Statements	Yes	No
Conditional Access is implemented by using policies in Microsoft Entra ID.	<input checked="" type="radio"/>	<input type="radio"/>
A Conditional Access policy can block or allow Microsoft Entra ID connections based upon the specific platform of a user's device.	<input checked="" type="radio"/>	<input type="radio"/>
A Conditional Access policy can be applied to a Microsoft 365 group.	<input checked="" type="radio"/>	<input type="radio"/>