Question 1

Which Microsoft Purview solution can be used to identify data leakage?

Options:

A- insider risk management

B- Compliance Manager

C- communication compliance

D- eDiscovery

Answer:

A

Question 2

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	Answer Area	
Device		The probability that an identity or account is compromised.
		The probability that an authentication request isn't authorized by the identity owner.
Sign-in risk		

Answer:

Question Type: **MultipleChoice**

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.

Options:

A- a network interface

B- an Azure App Service web app

C- a virtual network

D- a virtual network subnet

E- a resource group

Question 4

Question Type: **MultipleChoice**

What can you use to view the Microsoft Secure Score for Devices?

Options:

A- Microsoft Defender for Cloud Apps

B- Microsoft Defender for Endpoint

C- Microsoft Defender for Identity

D- Microsoft Defender for Office 365

Answer:

B

Explanation:

Microsoft Secure Score for Devices

Artikel

12.05.2022

3Minuten Lesedauer

Applies to:

Microsoft Defender for Endpoint Plan 2

Microsoft Defender Vulnerability Management

Microsoft 365 Defender

Some information relates to pre-released product which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

To sign up for the Defender Vulnerability Management public preview or if you have any questions, contact us (mdvmtrial@microsoft.com).

Already have Microsoft Defender for Endpoint P2? Sign up for a free trial of the Defender Vulnerability Management Add-on.

Configuration score is now part of vulnerability management as Microsoft Secure Score for Devices.

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat attacks. It reflects the collective security configuration state of your devices across the following categories:

Application

Operating system

Network

Accounts

Security controls

Select a category to go to the Security recommendations page and view the relevant recommendations.

Turn on the Microsoft Secure Score connector

Forward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as your Microsoft Secure Score data.

Changes might take up to a few hours to reflect in the dashboard.

In the navigation pane, go to Settings > Endpoints > General > Advanced features

Scroll down to Microsoft Secure Score and toggle the setting to On.

Select Save preferences.

How it works

Microsoft Secure Score for Devices currently supports configurations set via Group Policy. Due to the current partial Intune support, configurations which might have been set through Intune might show up as misconfigured. Contact your IT Administrator to verify the actual configuration status in case your organization is using Intune for secure configuration management.

The data in the Microsoft Secure Score for Devices card is the product of meticulous and ongoing vulnerability discovery process. It is aggregated with configuration discovery assessments that continuously:

Compare collected configurations to the collected benchmarks to discover misconfigured assets

Map configurations to vulnerabilities that can be remediated or partially remediated (risk reduction)

Collect and maintain best practice configuration benchmarks (vendors, security feeds, internal research teams)

Collect and monitor changes of security control configuration state from all assets

Question 5

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.

Steps	Answer Area	
Action		Review and filter alerts
Answer:		
Investigate		Create cases in the Case dashboard
Explanation:		
Triage		Send a reminder of corporate policies to users

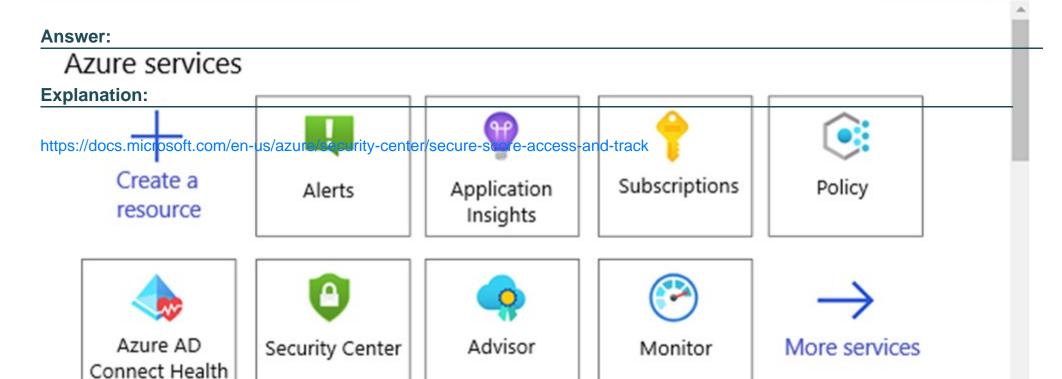https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide

Question 6

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

Microsoft Azure   🔍 Search resources, services, and docs (G+/)   ···

Answer:

Azure services

Explanation:

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

+ Create a resource	Alerts	Application Insights	Subscriptions	Policy
Azure AD Connect Health	Security Center	Advisor	Monitor	→ More services