PDFVCE

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

Exam : **SC-900**

Title : Microsoft Security Compliance and Identity Fundamentals

Vendor : Microsoft

Version : DEMO

NO.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

Answer: C

Explanation:

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

NO.2 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
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Answer:

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Explanation:

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Microsoft Entra Conditional Access (CA) evaluates signals from the user, device, location, and risk to make access decisions. The platform explicitly notes that CA decisions occur after primary sign-in:

"Conditional Access policies are enforced after the first-factor authentication has been completed." This means a user must successfully present their initial credentials (e.g., password, Windows Hello, FIDO2) before the CA engine evaluates policy logic. Therefore, the statement that CA is evaluated before a user is authenticated is not correct.
Regarding scoping, CA can target ordinary and privileged identities. The assignment options allow administrators to aim policies at users, groups, and directory roles: "You can include or exclude users and groups... [and] include or exclude specific Azure AD directory roles from a Conditional Access policy." Because Global Administrator is a directory role, policies can be applied to those accounts (with Microsoft's best-practice guidance to maintain at least one excluded break-glass account to prevent lockout).
For signals/conditions, CA supports device platform filtering. The documented device platform condition states: "This condition is based on the operating system platform of the device... iOS, Android, Windows, macOS (and others)." Administrators commonly use this to require different controls (like MFA or compliant device) based on Android or iOS.
Putting these together:
CA can apply to Global Administrators (Yes).
CA is evaluated after first-factor authentication (No to "before").
Device platform (e.g., Android/iOS) is a valid CA signal (Yes).

NO.3 Which solution performs security assessments and automatically generates alerts when a vulnerability is found?

A. cloud security posture management (CSPM)

B. DevSecOps

C. cloud workload protection platform (CWPP)

D. security information and event management (SIEM)

Answer: A

Explanation:
In Microsoft's cloud security terminology, Cloud Security Posture Management (CSPM) is the solution specifically designed to perform continuous security assessments of cloud resources and generate alerts when misconfigurations or vulnerabilities are detected. In Microsoft Defender for Cloud, the CSPM capabilities continuously analyze Azure, multi-cloud, and hybrid resources against built-in security benchmarks and regulatory standards. The platform evaluates configurations, detects insecure settings, missing protections, and exposure paths, then raises security recommendations and alerts so administrators can remediate issues that increase risk.
Microsoft's security and SCI learning content describes CSPM as providing "continuous assessment, visibility, and guidance to improve the security posture of your cloud environment," including automatic alerting when high-risk issues or vulnerabilities are found. These assessments are mapped to standards and best practices, helping organizations reduce risk proactively instead of waiting for an active attack.
By contrast, DevSecOps is a practice or methodology, not a specific product. A Cloud Workload Protection Platform (CWPP) focuses on runtime protection of workloads such as VMs, containers, and PaaS services. A SIEM solution (like Microsoft Sentinel) ingests and correlates logs and alerts from many sources but does not itself perform the core security posture assessments of cloud configurations. Therefore, the SCI domain clearly aligns this function with CSPM.

NO.4 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 Entra ID Protection can add users to groups based on the users' risk level.	○	○
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public.	○	○
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	○	○

Answer:

Answer Area

Statements	Yes	No
Microsoft Entra ID Protection can add users to groups based on the users' risk level.	○	○
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public.	○	○
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	○	○

Explanation:

Answer Area

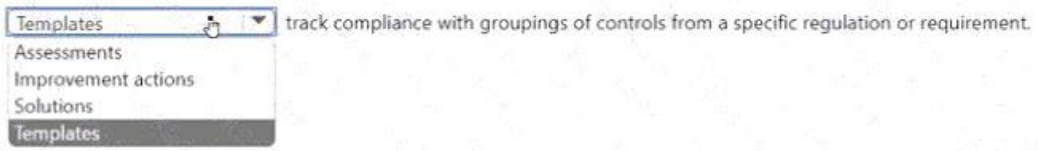
Statements	Yes	No
Microsoft Entra ID Protection can add users to groups based on the users' risk level.	○	●
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public.	●	○
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	●	○

Microsoft Entra ID Protection is designed to detect and respond to identity compromise by calculating user risk and sign-in risk and surfacing risk detections such as "leaked credentials," "anonymous IP address,"
"impossible travel," and related signals. Microsoft explains that Identity Protection "uses adaptive machine learning and threat intelligence to detect risky users and risky sign-ins and assigns each a risk level of Low, Medium, or High." These detections include "Leaked credentials (found on public or dark-web lists)", confirming that Identity Protection can detect when user credentials have been exposed.
ID Protection is integrated with Conditional Access to take policy-driven actions: "Risk-based Conditional Access policies let you require multi-factor authentication (MFA), block access, or require password change when a user or sign-in risk level is met." The built-in policies include User risk policy and Sign-in risk policy, which can automatically enforce MFA or password reset when the configured risk threshold is reached.
However, Identity Protection does not manage Azure AD group membership. There is no capability to add users to groups based on risk level; group membership changes are outside the scope of Identity Protection's controls. Instead, remediation is applied through Conditional Access or password reset policies driven by the calculated risk.
Therefore: adding users to groups based on risk (No); detecting leaked credentials (Yes); invoking

MFA based on risk via Conditional Access (Yes).

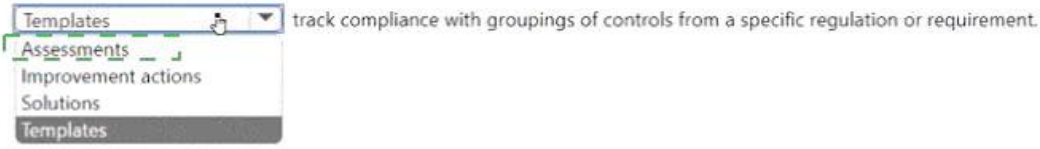
NO.5 Select the answer that correctly completes the sentence.

Answer Area



Answer:

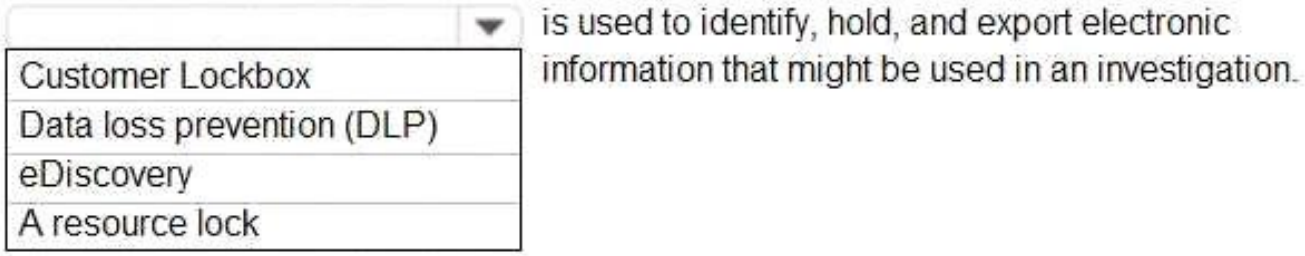
Answer Area



Explanation:
Assessments
In Microsoft Purview Compliance Manager, assessments are the core components used to track compliance with groupings of controls from specific regulations, standards, or requirements. According to official Microsoft Security, Compliance, and Identity (SCI) learning content, particularly within the SC-400 and SC-900 certification tracks, the role of assessments is explicitly defined as: "Assessments in Compliance Manager help you track, implement, and improve compliance with requirements from standards and regulations. Each assessment maps to a specific regulation or control framework, such as ISO 27001, NIST, GDPR, or HIPAA, and includes a set of controls and recommended improvement actions." Further extracted content from SCI documentation confirms: "An assessment is used to measure your compliance posture against a particular regulation or standard. It includes control mappings and provides insight into what's in place and what still needs to be addressed to meet the compliance goals." The other options in the dropdown - Templates, Improvement actions, and Solutions - serve different functions:
Templates provide a blueprint for creating assessments.
Improvement actions are actionable steps generated within assessments.
Solutions in Microsoft Purview refer to bundled capabilities like Insider Risk Management, Information Protection, etc.
Therefore, to track compliance with groupings of controls from a specific regulation or requirement, the correct and Microsoft-verified term is " Assessments. "

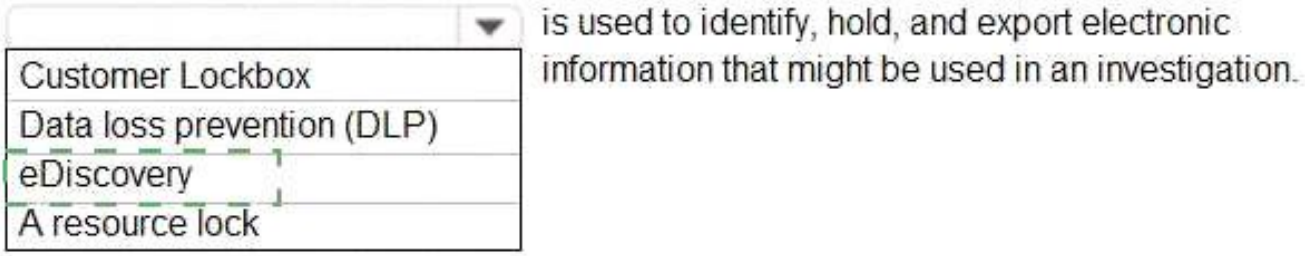
NO.6 Select the answer that correctly completes the sentence.

Answer Area



Answer:

Answer Area



Explanation:
eDiscovery
In Microsoft Purview, eDiscovery is the purpose-built compliance solution for legal and investigative workflows. Microsoft's SCI materials describe eDiscovery as the tool that enables organizations to identify, preserve/hold, collect, review, and export potentially relevant content across Microsoft 365 services. Official guidance explains that eDiscovery (Standard) "provides search, hold, and export capabilities" for content in Exchange, SharePoint, OneDrive, Teams, and more. Another description states that eDiscovery (Premium) helps you "identify, preserve, collect, review, analyze, and export content" for legal matters and internal investigations. These capabilities are designed to support the eDiscovery lifecycle by allowing admins and case managers to: create cases, define custodians and non-custodial data sources, run targeted searches, apply legal holds to prevent data alteration or deletion, perform review and analytics, and export responsive data packages for counsel or regulators.
By contrast, Data Loss Prevention (DLP) protects sensitive information from accidental or inappropriate sharing; Customer Lockbox governs Microsoft engineer access to your data for support; and resource locks protect Azure resources from accidental deletion or modification. Therefore, the Microsoft SCI control that is explicitly used to identify, hold, and export electronic information for an investigation is Microsoft Purview eDiscovery.

NO.7 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.

Answer: A C

Explanation:

Microsoft Purview Data Loss Prevention (DLP) is designed to prevent the inadvertent or inappropriate sharing of sensitive data across Microsoft 365 services. Microsoft's guidance states that DLP "helps you discover, monitor, and protect sensitive items across Microsoft 365," and that with DLP policies you can

"identify, monitor, and automatically protect sensitive items in Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams." This directly supports option C, because DLP can detect sensitive info in OneDrive documents and automatically apply protective actions such as blocking external sharing, restricting access, or auditing the event.

DLP also provides end-user coaching through policy tips: "Policy tips are informative notices that appear when users are working with content that contains sensitive info ... to help prevent data loss." When a user is about to send or share sensitive data in violation of policy, these tips surface in Outlook and Office apps (including when files are stored in SharePoint/OneDrive), aligning with option A.

By contrast, enabling disk encryption (e.g., BitLocker) and applying device security baselines are endpoint

/device management tasks handled through Microsoft Intune or Group Policy-not by DLP. Therefore, A and C are the correct tasks you can implement with Microsoft 365 DLP policies.

NO.8 Select the answer that correctly completes the sentence.

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)

Answer:

Answer Area

Microsoft Defender for Identity can identify advanced threats from [on-premises Active Directory Domain Services (AD DS)] signals.

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

Explanation:

Answer Area

Microsoft Defender for Identity can identify advanced threats from [on-premises Active Directory Domain Services (AD DS)] signals.

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

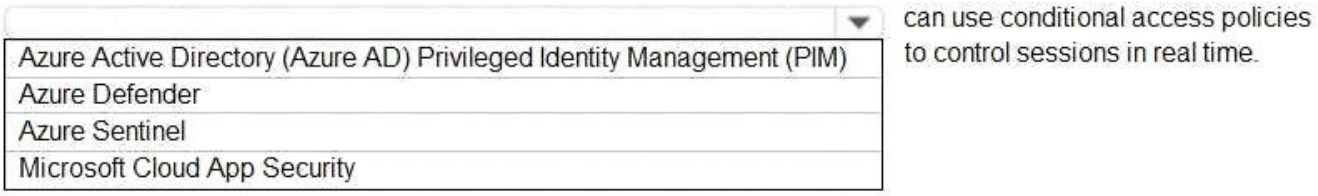
Microsoft Defender for Identity (formerly Azure ATP) is designed to protect on-premises identity infrastructures by analyzing signals from Active Directory Domain Services (AD DS). In Microsoft's SCI guidance, Defender for Identity is described as a "cloud service that uses sensors installed on your domain controllers to monitor and analyze user activities and information across your on-premises Active Directory." The sensors "collect authentication, replication, and other security-relevant events and network traffic," enabling analytics to detect techniques such as Pass-the-Hash, Pass-the-Ticket, Golden Ticket, reconnaissance, lateral movement, and domain dominance. The product's purpose is to surface advanced threats, compromised identities, and malicious insider actions by continuously profiling and learning from AD DS behavior and security events.

While Defender for Identity integrates with other Microsoft security solutions (for example,

Microsoft 365 Defender and Microsoft Defender for Cloud Apps) to enrich investigations, it does not rely on Azure Active Directory (Microsoft Entra ID) signals for its core detections, nor does it collect telemetry from Azure AD Connect itself. Instead, its foundational telemetry source is on-premises AD DS domain controllers via lightweight sensors, which provide the deep authentication and directory-service context required to identify sophisticated identity-based attacks in hybrid environments.

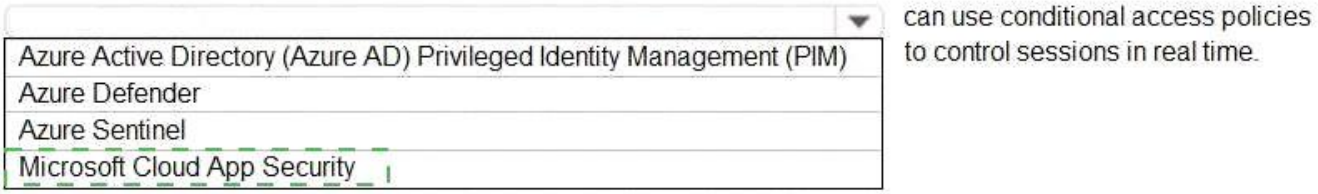
NO.9 Select the answer that correctly completes the sentence.

Answer Area



Answer:

Answer Area



Explanation:

Answer Area

In Microsoft's Security, Compliance, and Identity guidance, Microsoft Cloud App Security (now Microsoft Defender for Cloud Apps) integrates with Azure AD Conditional Access to provide Conditional Access App Control. This capability enables organizations to "monitor and control user sessions in real time" by routing traffic through a reverse proxy once a Conditional Access policy is triggered. With session controls, admins can enforce actions such as block, allow with inspection, apply download restrictions, require label application, or limit access to web apps based on context (user, device state, location, risk). SCI learning paths describe that Defender for Cloud Apps works with Conditional Access policies to provide session-based conditional access that "protects data in real time," giving granular control after authentication while a session is active.

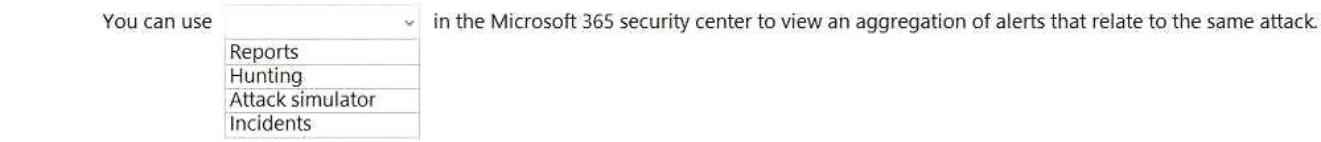
By comparison, Azure AD Privileged Identity Management (PIM) focuses on just-in-time elevation and governance of privileged roles, not real-time in-app session control. Azure Defender (Defender for Cloud) provides cloud workload protection and posture management, not Conditional Access session enforcement.

Azure Sentinel (Microsoft Sentinel) is a SIEM/SOAR platform for analytics, hunting, and automation and does not apply Conditional Access session policies. Therefore, the Microsoft product that uses

Conditional Access policies to control sessions in real time is Microsoft Cloud App Security (Defender for Cloud Apps).

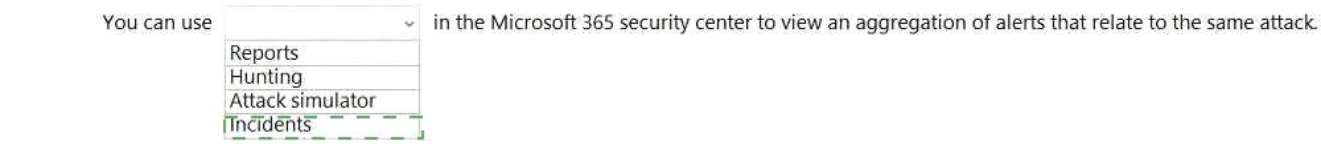
NO.10 Select the answer that correctly completes the sentence.

Answer Area



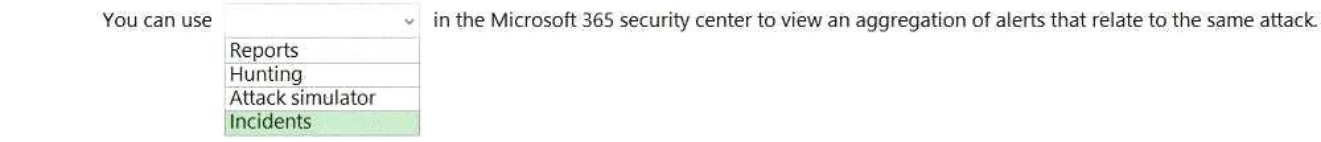
Answer:

Answer Area



Explanation:

Answer Area



In Microsoft 365 Defender (Microsoft 365 security center), Incidents are designed to consolidate and correlate security signals so analysts can see the full scope of an attack. Microsoft's documentation explains that an incident is "a collection of related alerts that, when viewed together, provide a richer context for the attack and its impact." The service "automatically groups alerts that are likely to be associated with the same threat activity," which allows security teams to investigate a single incident rather than many fragmented alerts.

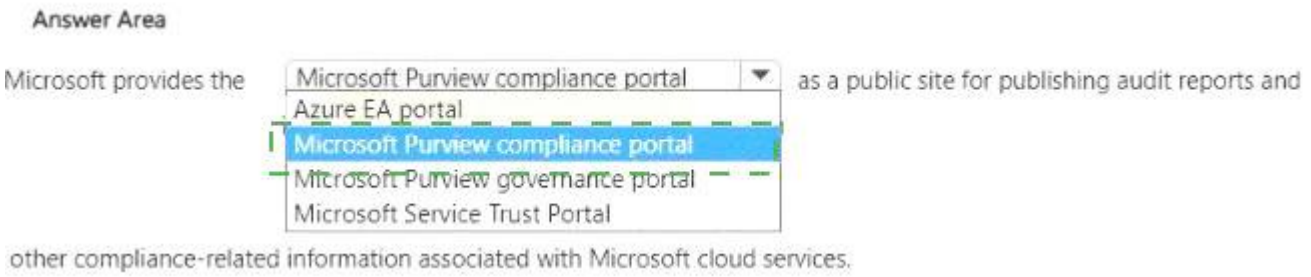
Microsoft further notes that incidents "aggregate alerts, affected assets (users, devices, mailboxes), evidences, and entities into one view," helping analysts triage, investigate, and remediate more efficiently.

This is distinct from other areas in the portal: Reports provide trend and posture reporting; Hunting offers proactive, query-based threat hunting across raw data; and Attack simulator (in Defender for Office 365) is used to run training and awareness simulations (e.g., phishing), not to aggregate real alerts. Therefore, when you need to "view an aggregation of alerts that relate to the same attack" in the Microsoft 365 security center, the correct place is Incidents, which presents the correlated attack story and enables end-to-end response and remediation from a single, consolidated record.

NO.11 completes the sentence.

Answer Area

Answer:



Explanation:

In Microsoft's Security, Compliance, and Identity guidance, the Microsoft Service Trust Portal (STP) is identified as the public destination where Microsoft publishes independent audit reports, compliance certifications, assessment reports, and trust-related documentation for Microsoft cloud services. The documentation explains that the STP provides customers with access to materials such as SOC 1/SOC 2 reports, ISO/IEC certifications, audit summaries, and compliance guides, enabling organizations to evaluate Microsoft's controls and map them to their own regulatory requirements. The STP is expressly positioned for transparency and due diligence, allowing customers and auditors to review Microsoft's compliance posture and understand how Microsoft manages security, privacy, and compliance across its cloud platforms.
By contrast, the Microsoft Purview compliance portal is a tenant-admin portal used to configure and manage compliance solutions (e.g., DLP, Information Protection, eDiscovery, Insider Risk, Compliance Manager) within your organization-not a public repository of Microsoft's audit artifacts. The Microsoft Purview governance portal focuses on data governance and cataloging scenarios. The Azure EA portal is used for Enterprise Agreement billing and usage management. Therefore, the public site for publishing audit reports and other compliance-related information for Microsoft cloud services is the Microsoft Service Trust Portal.

NO.12 Which three authentication methods can Microsoft Entra users use to reset their password? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. text message to a phone

B. certificate

C. mobile app notification

D. security questions

E. picture password

Answer: A C D

Explanation:
Microsoft Entra self-service password reset (SSPR) supports multiple verification methods that users can register and use to prove their identity during a reset. Microsoft's documentation lists the SSPR methods as:
"Mobile app notification," "Mobile app code," "Email," "Mobile phone (text message or call)," "Office

phone," and "Security questions." Administrators choose which of these are allowed and how many methods are required. During the reset flow, SSPR "prompts the user to verify with the registered methods" before permitting a password change. Notably, certificates and picture passwords are not SSPR verification methods in Microsoft Entra ID. Therefore, among the options provided: a text message to a phone (mobile phone), a mobile app notification (Microsoft Authenticator), and security questions are valid SSPR authentication methods; certificate and picture password are not supported for SSPR. This aligns with SCI learning content that positions SSPR as a user-empowering capability to securely restore access using admin-approved methods without help-desk intervention.

NO.13 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

Answer: A

Explanation:

Microsoft Defender for Office 365 includes Safe Attachments, a protection that "checks attachments in a secure, virtual environment to detect malicious behavior." In Microsoft's guidance, Safe Attachments is described as part of the anti-malware pipeline that "routes messages with attachments to a detonation chamber; if no suspicious activity is detected, the message is released to the recipient, and if malicious behavior is found, the attachment is blocked or removed." Administrators can choose Block, Replace, Dynamic Delivery, or Monitor actions. The Dynamic Delivery option specifically supports the use case in the question: the email body is delivered while the attachment is scanned, and "the attachment is automatically reattached and forwarded to the recipient only when it is determined to be safe." This capability is unique to Defender for Office 365's Safe Attachments, not to be confused with endpoint antivirus or identity tools.

Defender Antivirus protects Windows devices, Defender for Identity secures on-premises identities, and Defender for Endpoint focuses on endpoint detection and response. Therefore, the Microsoft service you use to scan email attachments and forward them only when clean is Microsoft Defender for Office 365 (Safe Attachments).

NO.14 Which feature is included in Microsoft Entra ID Governance?

A. Identity Protection

B. Privileged Identity Management

C. Permissions Management

D. Verifiable credentials

Answer: B

NO.15 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
Compliance Manager tracks only customer-managed controls.	○	○
Compliance Manager provides predefined templates for creating assessments.	○	○
Compliance Manager can help you asses whether data adheres to specific data protection standards.	○	○

Answer:

Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls.	○	○
Compliance Manager provides predefined templates for creating assessments.	○	○
Compliance Manager can help you asses whether data adheres to specific data protection standards.	○	○

Explanation:
Compliance Manager tracks only customer-managed controls. No
Compliance Manager provides predefined templates for creating assessments. Yes Compliance Manager can help you assess whether data adheres to specific data protection standards. No
Microsoft Purview Compliance Manager is described as a feature that "helps you manage your organization's compliance requirements" by giving you assessments, improvement actions, and a compliance score that
"measures your progress in completing recommended actions" aligned to regulations and standards. The service does not track only customer-managed controls; Microsoft's documentation clarifies that Compliance Manager includes "Microsoft-managed controls and customer-managed controls," and it tracks both within each assessment to show overall posture. It also provides prebuilt (predefined) assessment templates for common regulations and industry standards so organizations can "create assessments from templates" such as GDPR, ISO/IEC 27001, and the Data Protection Baseline. Importantly, Compliance Manager evaluates control implementation and improvement actions mapped to requirements; it does not scan or classify individual data to determine whether specific data items "adhere" to a standard. Instead, it helps you assess organizational compliance posture by tracking the status of controls, assigning actions, and recording evidence. Thus:
"Tracks only customer-managed controls" # No (it tracks Microsoft-managed and customer-managed).
"Provides predefined templates for creating assessments" # Yes (prebuilt templates are a core

feature).
"Helps you assess whether data adheres to specific data protection standards" # No (it measures control
/compliance posture, not data-level adherence).
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

NO.16 Which compliance feature should you use to identify documents that are employee resumes?

A. pre-trained classifiers

B. Content explorer

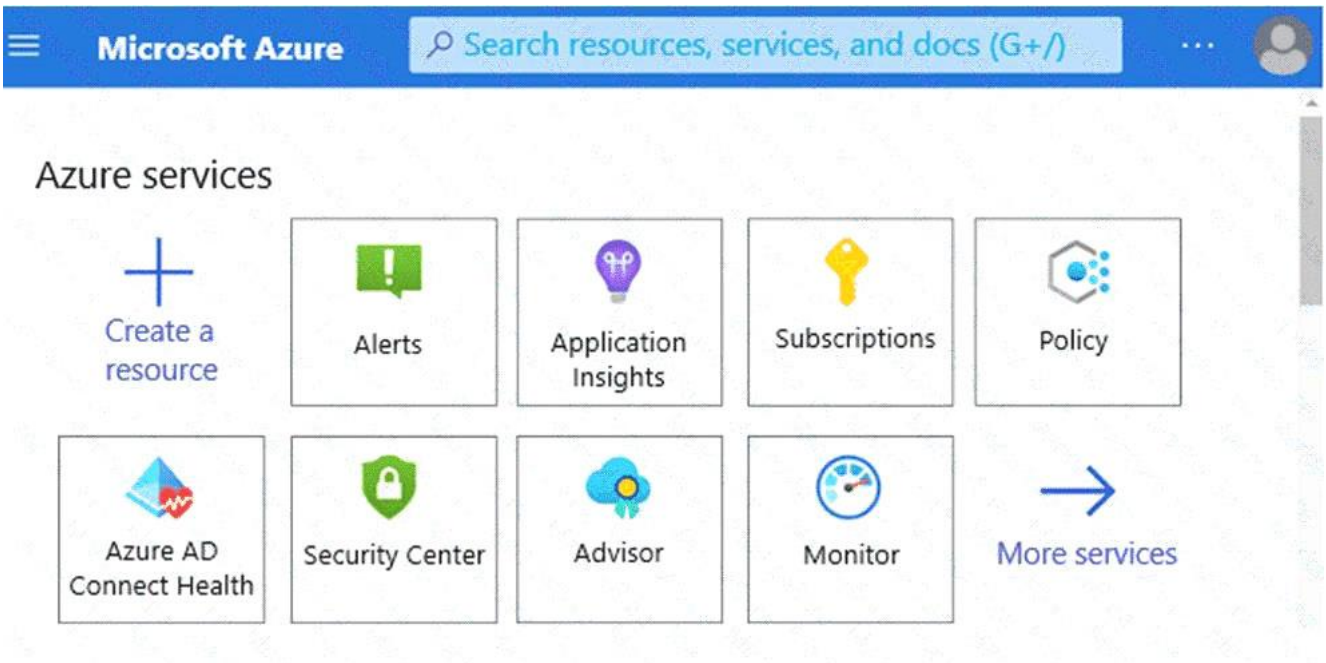
C. Activity explorer

D. eDiscovery

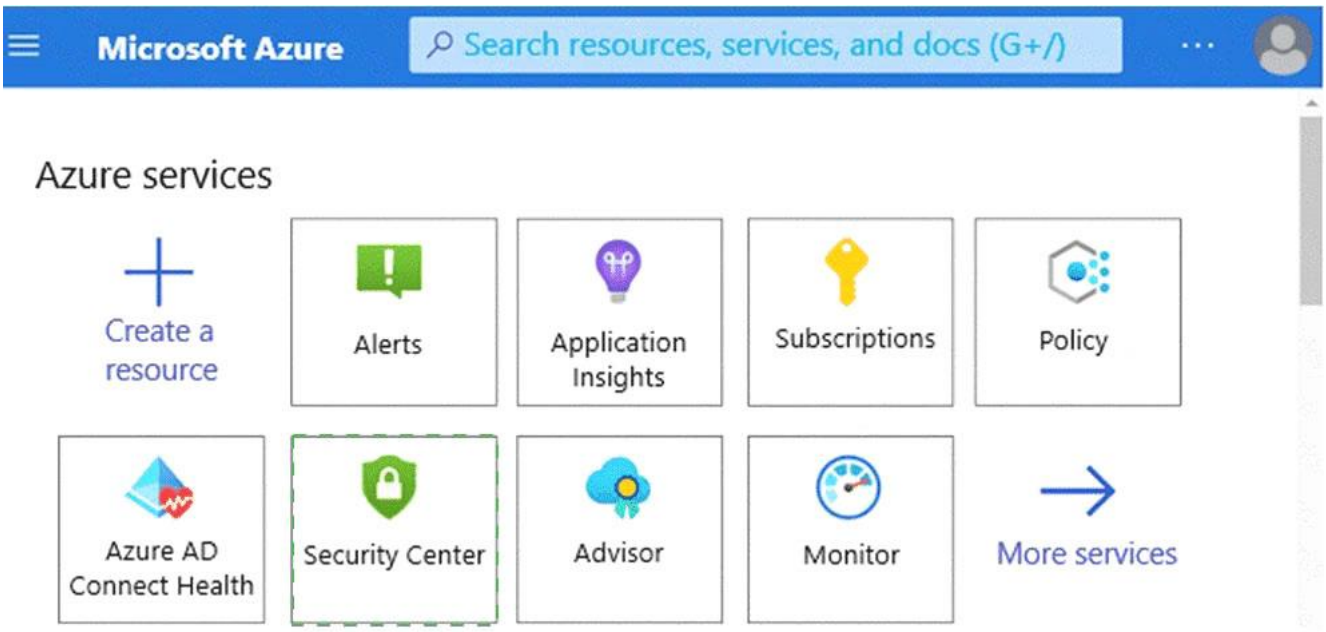
Answer: A

Explanation:
In Microsoft Purview Information Protection, pre-trained (Microsoft-provided) trainable classifiers are designed to automatically recognize specific categories of content by learning from examples rather than relying only on patterns or keywords. Microsoft's guidance explains that trainable classifiers "look for data by learning from examples," and that Microsoft supplies a catalog of "pre-trained classifiers that you can use immediately in your tenant." The documentation explicitly lists content types these classifiers can recognize, including "Resumes," along with other categories such as Source code, Threat and harassment, and more.
Because they're already trained by Microsoft, you can use them "to identify and classify items across SharePoint, OneDrive, and Exchange," and then take actions such as auto-labeling or enforcing DLP policies based on the classifier match.
By contrast, Content explorer is a reporting tool that lets you view where sensitive info types/labels were found; it doesn't identify resumes on its own. Activity explorer shows events like DLP policy matches over time. eDiscovery is used for legal hold, search, and review, not for semantic content identification. Therefore, to identify documents that are employee resumes, the correct Microsoft compliance feature is the pre-trained (Microsoft-provided) trainable classifier for Resumes.

NO.17 Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.



Answer:



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

NO.18 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. the Anomaly Detector service

B. Microsoft Sentinel

C. Azure Blueprints

D. Azure Policy

Answer: D
Explanation:
Microsoft describes Azure Policy as the built-in governance service that lets you "create, assign, and manage policies" to enforce organizational standards and "assess compliance at scale." It continuously evaluates existing resources for compliance and can take effect-enforcement actions such as deny, append, or modify during create/update operations. Azure Policy "helps you audit and enforce your standards" across subscriptions and resource groups, and its compliance dashboard shows overall and per-policy compliance states for all resources. By contrast, Azure Blueprints focuses on orchestrating deployments of artifacts (such as policy assignments, role assignments, and templates) for new environments; Microsoft guidance positions Policy as the engine that evaluates and enforces those standards on existing resources. Sentinel is a SIEM /SOAR for security analytics, and Anomaly Detector is a Cognitive Service-not a governance/compliance enforcement tool. Therefore, to assess compliance and enforce standards for existing Azure resources, the prescribed control plane is Azure Policy with its evaluation cycle, initiative (policy set) support, and remediation tasks.

NO.19 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
Answer: B
Explanation:
Microsoft Secure Score for Devices
Artikel
12.05.2022
3 Minuten 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

NO.20 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

Answer: D

Explanation:
Microsoft Purview Information Protection (in the Microsoft 365 compliance center) enables you to discover, classify, label, and protect sensitive information across emails, documents, and other data stores. Labels and policies can enforce encryption, access restrictions, and visual markings, helping prevent unauthorized disclosure of sensitive data-inside or outside your organization.

NO.21 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.	○	○
You can restrict accessing a SharePoint Online site by using Information Barriers.	○	○
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	○	○

Answer:

Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	○	○
You can restrict accessing a SharePoint Online site by using Information Barriers.	○	○
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	○	○

Explanation:

Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	●	○
You can restrict accessing a SharePoint Online site by using Information Barriers.	●	○
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	●	○

Microsoft documents Information Barriers (IB) as a Microsoft Purview capability that "restricts communication and collaboration between specific groups of users" across Microsoft 365. The service coverage explicitly includes "Microsoft Teams, SharePoint, OneDrive, and Exchange Online."
In Exchange Online, IB policies "block communication" between segmented users, which includes sending or receiving email and related collaboration, thereby meeting the statement about restricting communication in Exchange.
With IB v2, Microsoft states that policies also apply to SharePoint and OneDrive so that users in different segments are "prevented from accessing sites and content" not permitted by policy. This means a SharePoint Online site can be segmented so that members outside the allowed segments are denied access, satisfying the second statement.
For Microsoft Teams, IB policies "restrict collaboration scenarios such as chats, channel conversations, and file sharing" when participants are in segments that shouldn't interact. Because Teams file sharing is backed by SharePoint/OneDrive, IB v2 enforcement "prevents sharing and accessing files across restricted segments." In effect, a user cannot share a file with another user in Teams if an IB policy disallows interaction between their segments.
These behaviors align with SCI guidance that IB policies are designed to reduce conflict-of-interest risk by controlling who can communicate, collaborate, or access content across Microsoft 365 workloads.

NO.22 What types of files can Microsoft Purview sensitive information type classifiers be used to

classify?

A. Images

B. Video files

C. Documents

D. Audio files

Answer: C