MICROSOFT SC-100 Exam Questions

Total Questions: 200+
Demo Questions: 35
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
Microsoft SC-100 Exam Questions by Cert Empire

Question: 1

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure. You need to perform threat modeling by using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure. What should you use to start the threat modeling process?

A. the STRIDE model

B. the DREAD model

C. OWASP threat modeling

Answer:

A

Explanation:

The Microsoft Cloud Adoption Framework (CAF) for Azure aligns its security best practices with the Microsoft Security Development Lifecycle (SDL). A fundamental step in the SDL is threat modeling, for which Microsoft created and advocates the STRIDE model. STRIDE is a methodology used to systematically identify and categorize potential security threats. It provides a structured, top-down approach by prompting analysis of how an attacker could achieve Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, or Elevation of Privilege against the components of an application or system architecture. This makes it the correct starting point for threat identification within the Microsoft framework.

Why Incorrect Options are Wrong:

B. the DREAD model: DREAD is a model for risk-rating and prioritizing threats after they have been identified. It is not used to start the identification process. Furthermore, Microsoft has deprecated the DREAD model.
C. OWASP threat modeling: While OWASP provides excellent and widely respected threat modeling methodologies, the question specifically asks about the approach based on the Microsoft Cloud Adoption Framework, which is intrinsically linked to Microsoft's own SDL and the STRIDE model.

References:

1. Microsoft Security Development Lifecycle (SDL) Documentation: "The SDL uses the STRIDE model, which characterizes known threats according to the kinds of attacks that are used to exploit them (see table below). STRIDE stands for: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege."
Source: Microsoft Docs, "Microsoft Security Development Lifecycle," Threat Modeling section.
2. Microsoft Cloud Adoption Framework (CAF) Documentation: The CAF's "Secure methodology"

integrates principles from established frameworks like the SDL. "Threat modeling is a core process in the Microsoft Security Development Lifecycle (SDL)." This directly links the CAF's security approach to the SDL, where STRIDE is the primary threat identification model.
Source: Microsoft Learn, "Cloud Adoption Framework Secure methodology Security operations Threat modeling for applications."
3. Microsoft Threat Modeling Tool Documentation: The official Microsoft Threat Modeling Tool is built upon the STRIDE methodology. "The Threat Modeling Tool is a core element of the Microsoft Security Development Lifecycle (SDL). It allows software architects to identify and mitigate potential security issues early... The tool is built on the STRIDE methodology."
Source: Microsoft Docs, "Threat Modeling Tool overview."

Question: 2

You have an Azure AD tenant that syncs with an Active Directory Domain Services AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD. You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices. You plan to remove all the domain accounts from the Administrators group on the Windows computers. You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised. What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)

B. Privileged Access Workstations (PAWs)

C. Azure AD Privileged Identity Management (PIM)

D. Azure AD identity Protection

Answer:

A

Explanation:

The primary goal is to provide administrative access to Windows computers only when needed while minimizing the risk of lateral movement from a compromised administrator account. Local Administrator Password Solution (LAPS) is a Microsoft security feature designed specifically for this scenario in an Active Directory environment. LAPS ensures that the password for the built-in local administrator account is unique on every managed computer, complex, and automatically rotated. When an IT administrator requires access, they can retrieve the specific computer's current password from Active Directory. This mechanism provides access on an as-needed basis and critically prevents an attacker from using a compromised local administrator password from one machine to access others, thereby stopping lateral movement.

Why Incorrect Options are Wrong:

B. Privileged Access Workstations (PAWs): PAWs are hardened, dedicated computers used by administrators for sensitive tasks, not a solution for granting temporary administrative rights to standard endpoints.
C. Azure AD Privileged Identity Management (PIM): PIM provides just-in-time access primarily for Azure AD and Azure resource roles. While it can grant temporary local admin rights, LAPS is the more direct and foundational solution for preventing lateral movement via shared local administrator passwords.
D. Azure AD Identity Protection: This is a service for detecting and responding to identity-based threats and risks, such as suspicious sign-ins. It does not manage or grant administrative

privileges.

References:

1. Microsoft Documentation, "Local Administrator Password Solution (LAPS) overview": "LAPS mitigates this risk of lateral movement by setting a different, randomized password for the common local administrator account on every computer in the domain... An authorized user can query Active Directory for the password and use it to log on to a specific computer." This directly supports LAPS as the solution for providing as-needed access while preventing lateral movement. Source: https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview, Introduction section.
2. Microsoft Documentation, "Securing privileged access overview": In the recommended roadmap for securing privileged access, the documentation explicitly states, "Deploy Local Admin Password Solution (LAPS) to protect devices from pass-the-hash and lateral traversal attacks." This positions LAPS as a Microsoft Security Best Practice for the scenario described. Source: https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-overview, "Privileged access roadmap" section.
3. Microsoft Documentation, "What are Privileged Access Workstations (PAW)?": "A Privileged Access Workstation (PAW) provides a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors." This clarifies that PAWs are about securing the administrator's environment, not managing endpoint access. Source: https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices, Overview section.

Question: 3

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS). You need to define the recovery steps for a ransomware attack that encrypted data in the subscription The solution must follow Microsoft Security Best Practices. What is the first step in the recovery plan?

A. Disable Microsoft OneDnve sync and Exchange ActiveSync.

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. From Microsoft Defender for Endpoint perform a security scan.

Answer:

A

Explanation:

The first and most critical step in responding to a ransomware attack that affects cloud data is containment. Disabling Microsoft OneDrive sync and Exchange ActiveSync immediately severs the connection between potentially compromised endpoints and the cloud storage. This action prevents the sync clients from uploading encrypted versions of files and overwriting the clean copies stored in Microsoft 365. By stopping the synchronization, you preserve the integrity of the data in the cloud, including file version history, which is essential for the subsequent recovery process using features like OneDrive's "Files Restore."

Why Incorrect Options are Wrong:

B. Recover files to a cleaned computer or device.
This is a later step in the recovery process. You must first contain the threat and eradicate the malware before attempting to restore data.
C. Contact law enforcement.
This is an important procedural step in the overall incident response plan, but it is not a technical action to contain or mitigate the immediate damage.
D. From Microsoft Defender for Endpoint perform a security scan.
While scanning is crucial for identifying the scope of the compromise, the immediate priority is to stop the ongoing damage. Disabling sync is a faster containment action than waiting for scans to complete.

References:

1. Microsoft Sentinel documentation, "Human-operated ransomware attack playbook."
Under the Containment phase, the playbook explicitly lists "Disable synchronization services" as a key step. It states, "If the attacker is targeting cloud file storage for encryption, disable synchronization services to stop the spread." This confirms that stopping sync is a primary containment action.
2. Microsoft Learn, "Recover from a ransomware attack in Microsoft 365."
This guide outlines a multi-step recovery plan. The first step is "Verify and secure your environment," which emphasizes containing the affected devices to prevent the ransomware from encrypting more files. Disabling sync is a core part of this containment for cloud services. The document later details using "Files Restore" for OneDrive, a feature whose effectiveness depends on having unencrypted versions of files, which is protected by stopping sync early.
3. Microsoft Security, "Ransomware response."
In the "Containment" section of the response plan, Microsoft advises to "Isolate compromised systems to prevent lateral movement." For cloud-synced data, disabling the sync mechanism is the logical equivalent of isolating the cloud repository from further harm originating from compromised endpoints.

Question: 4

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS). You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices. You need to ensure that a compromised administrator account cannot be used to delete the backups What should you do?

A. From a Recovery Services vault generate a security PIN for critical operations.

B. From Azure Backup, configure multi-user authorization by using Resource Guard.

C. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault

D. From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup
Contributor role.

Answer:

B

Explanation:

To prevent a single compromised administrator account from deleting backups, the Microsoft Security Best Practice is to implement a separation of duties for critical operations. Multi-user authorization (MUA) using Resource Guard in Azure Backup is designed for this exact purpose. It ensures that destructive actions, such as deleting backups or reducing retention, require approval from a separate administrator who has permissions on the Resource Guard, which is typically managed by a different team. This prevents a single point of compromise from leading to data loss and is a core component of a ransomware recovery strategy.

Why Incorrect Options are Wrong:

A. The security PIN adds an extra authentication step, but it does not enforce separation of duties. A compromised administrator who has access to the Azure portal could still perform the destructive action.
C. Registering MABS with a Recovery Services vault is a standard configuration step required for backups to function; it does not provide any specific security protection against malicious deletion.
D. PIM provides just-in-time (JIT) access, which limits the time an account has elevated privileges. However, once the role is activated by the compromised user, they would have full permission to delete backups.

References:

1. Microsoft Learn, "Multi-user authorization for Azure Backup using Resource Guard," Section: "About Multi-user authorization for Backup." This document states, "Multi-user authorization (MUA) for Azure Backup allows you to add an additional layer of protection to critical operations on your Recovery Services vaults... This provides maximum security for your backups, ensuring that even in a scenario of a rogue administrator, critical operations can be performed only after getting the required authorizations."
2. Microsoft Learn, "Backup and restore plan to protect against ransomware," Section: "Protect backups from attacks." This best practice guide explicitly recommends MUA: "To provide an additional layer of security before executing critical operations, Azure Backup provides multi-user authorization (MUA)... We highly recommend you enable MUA to provide enhanced protection for your backups."
3. Microsoft Learn, "Security features to help protect hybrid backups from attacks," Section: "Preventing attacks." This document lists both MUA and the security PIN as features. However, MUA with Resource Guard is presented as the more robust solution for preventing malicious actions by enforcing authorization from a separate principal.
4. Microsoft Learn, "What is Privileged Identity Management?," Section: "What does it do?". This document explains that PIM's purpose is to provide time-based and approval-based role activation to mitigate risks of excessive permissions, but it does not prevent an authorized (or compromised but activated) user from performing actions allowed by their role.

Question: 5

You have a Microsoft 365 subscription. You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA). You need to recommend a solution that automatically restricts access to Microsoft Exchange Online. SharePoint Online, and Teams m near-real-lime (NRT) in response to the following Azure AD events: • A user account is disabled or deleted • The password of a user is changed or reset. • All the refresh tokens for a user are revoked • Multi-factor authentication (MFA) is enabled for a user Which two features should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. continuous access evaluation

B. a sign-in risk policy

C. Azure AD Privileged Identity Management (PIM)

D. Conditional Access

E. Azure AD Application Proxy

Answer:

A, D

Explanation:

The solution requires a near-real-time (NRT) response to specific Azure AD events, aligning with the Zero Trust principle of continuous verification.
Continuous Access Evaluation (CAE) is the specific Azure AD feature designed for this. It allows resource providers like Exchange Online and SharePoint Online to subscribe to critical security events. When an event such as a user being disabled or a password reset occurs, CAE enables the service to revoke the session in near-real-time, rather than waiting for the access token's standard expiry.
Conditional Access is the policy engine where access rules are defined. CAE works in conjunction with Conditional Access policies. While Conditional Access sets the rules (e.g., require MFA), CAE provides the mechanism to re-evaluate and enforce these policies dynamically during an active session based on the specified triggers.

Why Incorrect Options are Wrong:

B. a sign-in risk policy: This evaluates risk only at the time of sign-in, not continuously throughout an active session for the events listed.
C. Azure AD Privileged Identity Management (PIM): This is for managing and providing just-in-time access for privileged administrative roles, not for general user access to applications.
E. Azure AD Application Proxy: This is used to provide secure remote access to on-premises

applications, which is not relevant for cloud services like Exchange Online and SharePoint Online.

References:

1. Microsoft Learn, "Continuous access evaluation in Azure AD": This document explicitly states, "When a critical event is evaluated, CAE allows resource providers to revoke access to resources in near real time." It lists the exact event triggers from the question, including "User account is deleted or disabled," "User password is changed or reset," and "Administrator explicitly revokes all refresh tokens for a user."
2. Microsoft Learn, "Conditional Access: Session": This document details how session controls work within Conditional Access policies and explains, "Continuous access evaluation... works by revoking access in near real time when there are changes in user conditions." This confirms the direct relationship between Conditional Access and CAE.
3. Microsoft Cybersecurity Reference Architectures (MCRA), "Zero Trust identity and device access policies": The MCRA documentation establishes Conditional Access as the central "Zero Trust policy engine" for user access. The architecture relies on this engine to enforce policies, and CAE is a critical capability that enhances its real-time enforcement power. (See the diagrams and accompanying text under the "Policy enforcement" section).

Question: 6

HOTSPOT You are planning the security levels for a security access strategy. You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA). Which security level should you configure for each job role? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

[image could not be rendered]

Answer:

Developer: Specialized security

Standard user: Enterprise security

IT administrator: Privileged security

Explanation:

This configuration aligns with the Microsoft Cybersecurity Reference Architectures (MCRA) tiered model for securing access, which is based on the principle of least privilege and the potential impact of an account compromise.

• IT administrator accounts have extensive control over critical IT systems and infrastructure. Their compromise could lead to a full-scale enterprise breach. Therefore, they require the highest level of protection, categorized as Privileged security.

• Standard user accounts are used for general productivity tasks (e.g., email, documents) and have limited permissions. They are protected by a strong, organization-wide baseline of controls, defined as Enterprise security.

• Developer accounts, while not typically IT administrators, have high-impact access to sensitive assets like source code, development environments, and deployment pipelines. A compromised developer account can be used to inject malicious code or steal intellectual property, requiring

enhanced protections categorized as Specialized security.

References:

Microsoft Learn. (2023). Securing privileged access overview. This official documentation directly defines the three security levels and provides examples for each.
Page/Section: "Security levels" section. It states, "The specialized level is for users that have a large business impact, but don't have IT administrative privileges... Examples of these roles include developers with access to sensitive code..." It defines privileged for IT administrators and enterprise for all other standard users.
Link: https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels
Microsoft. (2022). Microsoft Cybersecurity Reference Architectures (MCRA) - Security Privileged Access. This document outlines the security strategy for different roles.
Page/Section: Slide/Diagram titled "Privileged Access: Role Profiles". This diagram visually maps "Admins" to the Privileged profile, "Sensitive/High Impact" roles (like developers) to the Specialized profile, and "End Users" to the Enterprise profile.
Link: The MCRA documents are available for download from Microsoft's official sites, often updated. A direct link to the specific version can be found on the main MCRA page: https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

Question: 7

Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure. You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). What should you recommend?

A. Compliance Manager in Microsoft Purview

B. Microsoft Defender for Cloud

C. Microsoft Sentinel

D. Microsoft Defender for Cloud Apps

Answer:

B

Explanation:

Microsoft Defender for Cloud is the primary Cloud Security Posture Management (CSPM) tool for Azure. It includes a regulatory compliance dashboard that continuously assesses the Azure environment against a wide range of security standards and benchmarks. This dashboard includes a built-in initiative for NIST SP 800-53, which directly supports the implementation of the NIST Cybersecurity Framework (CSF). Defender for Cloud provides a compliance score, identifies non-compliant resources, and offers actionable recommendations to remediate issues. The Microsoft Cloud Adoption Framework (CAF) security methodology explicitly recommends using Defender for Cloud to monitor and enforce compliance.

Why Incorrect Options are Wrong:

A. Compliance Manager in Microsoft Purview: This tool manages organizational compliance across the entire Microsoft 365 ecosystem, focusing on control mapping and reporting, rather than the direct technical assessment of Azure resources.

C. Microsoft Sentinel: This is a Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution for threat detection and response, not for compliance posture assessment.

D. Microsoft Defender for Cloud Apps: This is a Cloud Access Security Broker (CASB) designed to secure software-as-a-service (SaaS) applications, not for evaluating the compliance of Azure infrastructure resources.

References:

1. Microsoft Learn, "Tutorial: Improve your regulatory compliance": "Microsoft Defender for Cloud helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard... By default, every subscription has the Microsoft cloud security benchmark assigned... You can add other standards such as NIST SP 800-53...". This document directly states that Defender for Cloud is the tool for this task and specifically mentions NIST.
2. Microsoft Cloud Adoption Framework, "Security governance and compliance": "Microsoft Defender for Cloud provides visibility of your compliance posture against these policies and regulations. It also helps you track the status of your compliance over time." This reference connects the Cloud Adoption Framework directly to the use of Microsoft Defender for Cloud for compliance evaluation.
3. Microsoft Learn, "What is Microsoft Defender for Cloud?": "Microsoft Defender for Cloud is a cloud security posture management (CSPM) and cloud workload protection platform (CWPP)... Defender for Cloud helps you find and fix security vulnerabilities... and strengthen your overall security posture." This defines the tool's primary purpose, which aligns with the question's requirement.
4. Microsoft Learn, "Microsoft Purview Compliance Manager": This document describes Compliance Manager's role in helping "manage your organization's compliance requirements," highlighting its focus on managing controls and assessments across services, which is a different function than the direct technical evaluation pro$_{C}$v$_{e}$i$_{r}$d$_{tE}$e$_{m}$d$_{pir}$b$_{e}$y Defender for Cloud for Azure resources.

Question: 8

Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure. You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure. You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow. What should you include in the recommendation?

A. custom roles in Azure Pipelines

B. branch policies in Azure Repos

C. Azure policies

D. custom Azure roles

Answer:

B

Explanation:

Branch policies in Azure Repos are the designated security control for protecting important branches (e.g., main, release). By configuring a branch policy, you can enforce specific conditions that must be met before code can be merged. The primary policy for this scenario is to require all changes to be submitted via a pull request, which prevents direct pushes to the protected branch. This ensures that all code undergoes a formal review and validation process, a core principle of DevSecOps, before being integrated and deployed by the CI/CD workflow.

Why Incorrect Options are Wrong:

A. custom roles in Azure Pipelines: These roles manage permissions for pipeline resources (e.g., who can edit or run a pipeline), not how code is merged into a source code repository.
C. Azure policies: Azure Policy enforces governance rules on Azure resources (e.g., virtual machines, storage accounts) at the subscription or management group level, not on source code within Azure Repos.
D. custom Azure roles: Custom Azure roles (RBAC) define permissions for managing Azure resources. They do not provide granular control over repository-specific workflows like requiring pull requests.

References:

1. Microsoft Learn, "Improve code quality with branch policies": This document explicitly states, "Branch policies are an important part of the Git workflow and enable you to... Require pull requests for changes." It details how to set up a policy to block direct pushes and mandate pull requests. (Reference Section: "Branch policy settings", "Require a pull request").

2. Microsoft Learn, "DevSecOps controls in Azure": In the context of the Cloud Adoption Framework, this documentation discusses securing the development environment. It highlights the importance of protecting the codebase, stating, "Protect code with branch policies. Enforce code reviews to limit the risk of unreviewed code getting into a production environment." (Reference Section: "Secure development environment", "Codebase").
3. Microsoft Learn, "Security roles" (Azure Pipelines): This page defines the scope of pipeline security roles, such as Administrator, User, and Contributor, confirming they manage access to pipeline assets and do not control Git branch workflows. (Reference Section: "Pipeline permissions and security roles").
4. Microsoft Learn, "What is Azure Policy?": This source defines Azure Policy as a service for creating, assigning, and managing policies that enforce rules over your Azure resources, distinguishing its function from repository-level controls. (Reference Section: "Overview").

Question: 9

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices. You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices. What should you include in the response plan?

A. controlled folder access

B. application isolation

C. memory scanning

D. machine isolation

E. user isolation

Answer:

D

Explanation:

A post-breach response plan for a compromised computer, especially in a ransomware scenario, must prioritize containment to prevent lateral movement. The Microsoft Detection and Response Team (DART) methodology emphasizes this containment phase. Machine isolation is a core response capability in Microsoft Defender for Endpoint designed for this purpose. It disconnects the compromised device from the network, effectively stopping the threat from spreading to other resources. The isolated machine maintains a connection only to the Defender for Endpoint service, allowing security teams to conduct investigations and remediation actions safely without risk of further network contamination. This is the most direct and effective immediate response action for a compromised endpoint.

Why Incorrect Options are Wrong:

A. controlled folder access: This is a preventative Attack Surface Reduction (ASR) control configured before an attack to protect specific folders, not a post-breach response action.
B. application isolation: This is less comprehensive than machine isolation. An attacker may have compromised the entire operating system, making application-level isolation insufficient for containment.
C. memory scanning: This is a detection method used by security tools to find threats, not a response or containment action taken after a compromise is confirmed.
E. user isolation: This action, such as disabling an account, is appropriate for a compromised identity, not for containing a threat on a compromised computer itself.

References:

1. Microsoft Learn. "Take response actions on a device in Microsoft Defender for Endpoint." Under the section Isolate devices from the network, it states, "This action can help prevent the attacker from controlling the compromised device and performing other activities such as data exfiltration and lateral movement." This directly supports machine isolation as a primary post-breach response.
2. Microsoft Security Blog. "The Microsoft DART ransomware approach and best practices." In the article, under the Contain phase of the incident response lifecycle, a key recommended activity is to "Isolate compromised systems: Disconnect affected systems from the network to prevent further spread." This aligns the answer directly with the DART approach mentioned in the question.
3. Microsoft Learn. "SC-100: Design solutions for security operations." In the module covering incident response with Microsoft Sentinel and Microsoft Defender XDR, containment actions are a key topic. The documentation emphasizes using built-in tool capabilities, such as device isolation in Defender for Endpoint, to contain threats during an active incident.

Question: 10

HOTSPOT For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA). You need to protect against the following external threats of an attack chain: • An attacker attempts to exfiltrate data to external websites. • An attacker attempts lateral movement across domain-joined computers. What should you include in the recommendation for each threat? To answer, select the appropriate options in the answer area.

[image could not be rendered]

Answer:

1st: Microsoft Defender for Cloud Apps

2nd: Microsoft Defender for Identity

Explanation:

Microsoft Defender for Cloud Apps is the correct choice for preventing data exfiltration to external websites. It functions as a Cloud Access Security Broker (CASB), providing visibility and control over data traveling to and from cloud applications. It uses behavioral analytics and anomaly detection to identify suspicious activities, such as mass downloads or uploads to unsanctioned apps, which are common indicators of data exfiltration attempts.

Microsoft Defender for Identity is specifically designed to detect and investigate advanced threats, compromised identities, and malicious insider actions directed at an on-premises Active Directory environment. It analyzes network traffic and events from domain controllers to identify the techniques attackers use for lateral movement, such as Pass-the-Hash, Pass-the-Ticket, and remote code execution on domain-joined machines.

References:

Microsoft Defender for Cloud Apps Documentation: Microsoft's official documentation states, "Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services."
Source: Microsoft Learn, "What is Defender for Cloud Apps?", Microsoft Docs.
Microsoft Defender for Identity Documentation: The official documentation for Microsoft Defender for Identity highlights its role in detecting lateral movement. "Microsoft Defender for Identity... identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization. Key capabilities include... Monitoring user activities, and identifying advanced attacks based on the kill-chain model, such as reconnaissance, lateral

movement, and domain dominance."
Source: Microsoft Learn, "What is Microsoft Defender for Identity?", Microsoft Docs.
Microsoft Cybersecurity Reference Architectures (MCRA): The MCRA documentation on "Privileged Access" explicitly shows Microsoft Defender for Identity as a key component for protecting against credential theft and lateral movement within the on-premises part of a hybrid enterprise.
Source: Microsoft Cybersecurity Reference Architectures, "Privileged Access Security," Section: Technical components for Privileged Access.

Question: 11

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment. You need to recommend the top three modernization areas to prioritize as part of the plan. Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. user access and productivity

C. infrastructure and development

D. modern security operations

E. operational technology (OT) and IoT

Answer:

A, B, D

Explanation:

The Zero Trust Rapid Modernization Plan (RaMP) is a set of key initiatives to guide the adoption of a Zero Trust security model. For a rapid plan, prioritization focuses on areas with the highest impact on risk reduction. The foundational step is securing identities and managing their access, which is covered by user access and productivity. Concurrently, it is critical to establish comprehensive visibility and threat response capabilities, addressed by modern security operations (SecOps). The ultimate goal of Zero Trust is to protect business-critical assets, making the discovery, classification, and protection of sensitive information a top priority, which falls under data, compliance, and governance. These three areas form the core of an initial, high-impact Zero Trust implementation.

Why Incorrect Options are Wrong:

C. infrastructure and development: While a critical component of the full RaMP, securing the entire infrastructure and integrating security into development (DevSecOps) are typically longer-term efforts addressed after initial access controls are hardened.
E. operational technology (OT) and IoT: This is a specialized initiative within RaMP. It is a top priority only for organizations with substantial OT or IoT assets, not a universal starting point for all companies.

References:

1. Microsoft Learn, "Zero Trust rapid modernization plan (RaMP) overview." This document outlines the key initiatives of the RaMP framework. It lists "User access and productivity," "Modernize security operations (SecOps)," and "Data, compliance, and governance" as distinct

strategic areas. The "rapid" nature of the plan implies prioritizing foundational and high-impact initiatives first.
2. Microsoft Learn, "Zero Trust adoption framework for identities." Under the "Implementation guidance" section, it states, "Identities... represent a critical component of a Zero Trust strategy... This is a great place to start your Zero Trust journey." This supports prioritizing "user access and productivity."
3. Microsoft Learn, "Zero Trust adoption framework for SecOps." The overview emphasizes that SecOps must evolve to "rapidly remediate attacks" by integrating intelligence across the ecosystem, making it a crucial, concurrent priority for visibility and response.
4. Microsoft Learn, "Zero Trust adoption framework for data." The introduction states, "Ultimately, security is about protecting data." This highlights the centrality of data protection, making it a top priority once foundational access controls and visibility are in place.

Question: 12

You have an operational model based on the Microsoft Cloud Adoption framework for Azure. You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, database, files, and storage accounts. What should you include in the recommendation?

A. security baselines in the Microsoft Cloud Security Benchmark

B. modern access control

C. business resilience

D. network isolation

Answer:

A

Explanation:

The Microsoft Cloud Security Benchmark (MCSB) is a framework of security recommendations and best practices for Azure. It is a core component of the security governance discipline within the Microsoft Cloud Adoption Framework (CAF). The MCSB provides security baselines, which are sets of cloud-centric controls tailored for specific Azure services. These baselines offer a structured approach to securing various resource types, including endpoints, databases, files, and storage accounts, by defining the recommended security configuration. Therefore, recommending the use of security baselines from the MCSB directly addresses the need for a solution focused on cloud-centric control areas to protect these resources.

Why Incorrect Options are Wrong:

B. modern access control: This is a security principle (e.g., Zero Trust) and a component of a larger strategy, not a comprehensive set of control areas for diverse resources.
C. business resilience: This is a broader business objective focused on continuity and disaster recovery, not a specific technical solution for securing individual assets.
D. network isolation: This is a single, specific security control technique, not a complete framework of control areas covering all the specified resource types.

References:

1. Microsoft Learn. (2023). Introduction to the Microsoft cloud security benchmark. In "Microsoft Defender for Cloud documentation". Section: "What is the Microsoft cloud security benchmark?". "The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure..."
2. Microsoft Learn. (2023). Cloud Adoption Framework - Security - Governance. In "Microsoft Cloud Adoption Framework for Azure documentation". Section: "Benchmark". "Use the Microsoft

cloud security benchmark to provide a single, consolidated view of security recommendations... This benchmark is the foundation for security baselines in Azure."
3. Microsoft Learn. (2023). Azure security baselines overview. In "Microsoft Defender for Cloud documentation". Section: "What are the Azure security baselines?". "Each baseline consists of a set of recommendations that help you secure the specific service. These recommendations are from the Microsoft cloud security benchmark." This page lists baselines for services like Azure Storage and Azure SQL Database.

Question: 13

You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications. You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

A. the Azure landing zone accelerator

B. the Azure Will-Architected Framework

C. Azure Security Benchmark v3

D. Azure Advisor

Answer:

A

Explanation:

The Azure landing zone accelerator is a deployment experience within the Azure portal that provides an automated, opinionated implementation of the Azure landing zones conceptual architecture. This architecture is a core component of the Microsoft Cloud Adoption Framework (CAF). The accelerator uses Infrastructure as Code to rapidly deploy a scalable, multi-subscription environment with foundational services for networking, security, and governance. This directly addresses the need to deploy components like NSGs, Key Vault, and Bastion while minimizing deployment effort and adhering to CAF security best practices.

Why Incorrect Options are Wrong:

B. the Azure Well-Architected Framework: This is a set of guiding principles and best practices for designing high-quality workloads, not a deployable solution or tool for building an environment.
C. Azure Security Benchmark v3: This is a collection of security recommendations and controls used to assess and harden an environment. It is a guideline, not a deployment mechanism.
D. Azure Advisor: This is a recommendation engine that analyzes existing Azure resources to provide guidance on optimization. It is not a tool for deploying a new environment from scratch.

References:

1. Microsoft Cloud Adoption Framework for Azure Documentation, "What is an Azure landing zone?": "An Azure landing zone is the output of a multi-subscription Azure environment that accounts for scale, security governance, networking, and identity... The Azure landing zone accelerator is a deployment experience based on the Azure portal. It deploys an opinionated implementation based on the Azure landing zones conceptual architecture." This source confirms the accelerator is a deployment solution based on CAF principles.
2. Microsoft Azure Documentation, "Microsoft Azure Well-Architected Framework": "The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload." This defines WAF as a set of principles, not a deployment tool.
3. Microsoft Azure Documentation, "Introduction to the Azure Security Benchmark (ASB)": "The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure." This identifies ASB as a set of recommendations, not a deployment solution.
4. Microsoft Azure Documentation, "Introduction to Azure Advisor": "Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions..." This establishes Advisor as a tool for optimizing existing deployments, not creating new ones.

Question: 14

You have an on-premises network and a Microsoft 365 subscription. You are designing a Zero Trust security strategy. Which two security controls should you include as part of the Zero Trust solution? Each correct answer part of the solution. NOTE: Each correct answer is worth one point.

A. Block sign-attempts from unknown location.

B. Always allow connections from the on-premises network.

C. Disable passwordless sign-in for sensitive account.

D. Block sign-in attempts from noncompliant devices.

Answer:

A, D

Explanation:

A Zero Trust security model operates on the principle of "never trust, always verify." This means every access request must be explicitly verified before granting access, regardless of its origin. Blocking sign-in attempts from unknown or risky locations (A) and from noncompliant devices (D) are core implementations of the "Verify Explicitly" principle. These controls use real-time signals-such as user location, device health, and compliance status-to make intelligent access decisions. Azure AD Conditional Access is the primary tool used to enforce these policies, forming a cornerstone of a Microsoft-centric Zero Trust architecture.

Why Incorrect Options are Wrong:

B. Always allow connections from the on-premises network.
This contradicts the "Assume Breach" principle. Zero Trust treats all networks, including internal corporate networks, as untrusted and potentially compromised.
C. Disable passwordless sign-in for sensitive account.
This is contrary to Zero Trust guidance, which promotes stronger, phishing-resistant authentication. Passwordless methods are more secure than traditional passwords and are recommended for all accounts, especially sensitive ones.

References:

1. Microsoft Learn, "What is Zero Trust?". Under the "Guiding principles of Zero Trust" section, it states, "Verify explicitly. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies." This supports using location (A) and device health (D) as signals.
2. Microsoft Learn, "Securing identity with Zero Trust". In the "Verify explicitly" section, the documentation explicitly lists signals for verification: "Apply policies based on user risk, device

health, location, and more." This directly validates options A and D as correct Zero Trust controls.
3. Microsoft Learn, "Conditional Access design principles and dependencies". The article lists "Location" and "Device compliance" as common signals used in Conditional Access policies, which are described as the "policy engine at the heart of the Zero Trust access model." This confirms the technical implementation for A and D.
4. Microsoft Learn, "Embrace passwordless authentication". This document states, "Passwordless authentication methods are more secure. They replace passwords with something you have, plus something you are or something you know." This directly refutes the logic in option C.

Question: 15

You have an Azure subscription. You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar. Developers use Azure DevOps to deploy web apps to App Service Environments- When a new app is deployed, a CNAME record for the app is registered in contoso.com. You need to recommend a solution to secure the DNS record tor each web app. The solution must meet the following requirements: • Ensure that when an app is deleted, the CNAME record for the app is removed also • Minimize administrative effort. What should you include in the recommendation?

A. Microsoft Defender for DevOps

B. Microsoft Defender foe App Service

C. Microsoft Defender for Cloud Apps

D. Microsoft Defender for DNS

Answer:

B

Explanation:

The core security risk described is a "dangling DNS" entry, which can lead to a subdomain takeover. This occurs when an Azure App Service is deleted, but the CNAME record in the external DNS zone (contoso.com) is not removed, leaving it pointing to a non-existent resource. An attacker could then create a resource in Azure with the same name to hijack the subdomain. Microsoft Defender for App Service is specifically designed to detect this threat. It monitors DNS configurations that point to your App Services and generates an alert when it identifies a DNS entry pointing to a deprovisioned web app. This automates the detection process, fulfilling the requirement to minimize administrative effort by flagging the exact records that need to be removed.

Why Incorrect Options are Wrong:

A. Microsoft Defender for DevOps: This service secures the CI/CD pipeline, focusing on vulnerabilities in code, secrets, and infrastructure-as-code templates, not on runtime DNS configurations of deployed resources.
C. Microsoft Defender for Cloud Apps: This is a Cloud Access Security Broker (CASB) that protects data in SaaS applications (like Microsoft 365, Salesforce). It is not used for monitoring PaaS infrastructure like App Service.
D. Microsoft Defender for DNS: This service monitors DNS queries made from Azure resources to detect malicious activity like communication with C2 servers. It does not monitor DNS records pointing to Azure resources.

References:

1. Microsoft Learn, Introduction to Microsoft Defender for App Service: "Defender for App Service is a native cloud security solution that's used to protect your applications that are running on the App Service. .... One of the threats it covers is dangling DNS detection. When you remove a web site from an App Service, the DNS record that points to the App Service isn't removed at the same time. A dangling DNS entry is a DNS record that points to a resource that has been deprovisioned. This record can be a security risk for your organization."
2. Microsoft Learn, Reference table for all Microsoft Defender for Cloud alerts: The alert AppServicesSubdomainTakeover is listed for the App Service plan. Its description states: "Microsoft Defender for Cloud detected a dangling DNS entry in your DNS zone that points to a deprovisioned App Service web app. .. This makes your organization vulnerable to a subdomain takeover."
3. Microsoft Learn, Introduction to Microsoft Defender for DNS: "Microsoft Defender for DNS provides an additional layer of protection for your resources by... Continuously monitoring all DNS queries from your Azure resources and running advanced security analytics to alert you when suspicious activity is detected." This confirms its focus is on outbound queries, not inbound records.
4. Microsoft Learn, What is Microsoft Defender for DevOps?: "Microsoft Defender for DevOps is a new service in Defender for Cloud that provides security teams with the ability to secure applications and resources from code to cloud across multi-pipeline environments....." This confirms its focus on the development lifecycle.

Question: 16

HOTSPOT Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders The domain syncs with Azure AD by using Azure AD Connect Azure AD Connect has group writeback enabled. You have a Microsoft 365 subscription that uses Microsoft SharePoint Online. You have multiple project teams. Each team has an AD DS group that syncs with Azure AD Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams. You need to recommend an Azure AD identity Governance solution that meets the following requirements: • Project managers must verify that their project group contains only the current members of their project team • The members of each project team must only have access to the resources of the project to which they are assigned • Users must be removed from a project group automatically if the project manager has MOT verified the group s membership for 30 days. • Administrative effort must be minimized. What should you include in the recommendation? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

[image could not be rendered]

Answer:

Identity Governance feature: Access reviews

Project team configuration: From Azure AD, create a security group for each project and enable group writeback for each group

Explanation:

The best Identity Governance feature to meet these requirements is Access reviews. This feature is specifically designed to manage and attest to group memberships and application access. It allows you to assign reviewers, such as project managers, to periodically verify that users still require access. Crucially, it can be configured to automatically remove users from a group if their access is denied or not reviewed within a specified timeframe (e.g., 30 days), which directly fulfills key requirements while minimizing administrative effort.

For the configuration, the existing groups synced from on-premises Active Directory cannot have their membership modified directly by Azure AD, as their source of authority is on-premises. To allow Access reviews to automatically remove users, you must use cloud-mastered groups. The correct approach is to create new security groups in Azure AD and then enable group writeback. This makes the cloud-managed group available in the on-premises AD, allowing it to be used for permissions on both the Windows Server shared folders and the SharePoint Online sites.

References:

Microsoft Entra documentation, "What are access reviews?": This document states, "You can manage the access lifecycle by using Azure Active Directory (Azure AD) access reviews. Access reviews help your organization do things like... Ensure that only the right people have continued access... When reviews are finished, you can then make changes and remove access for users who no longer need it." It also details the automatic removal capability.

Microsoft Entra documentation, "Azure AD Connect: Group writeback": This source explains the functionality and prerequisites for group writeback. It clarifies, "Group writeback allows you to write cloud groups back to your on-premises Active Directory instance by using Azure Active Directory (Azure AD) Connect Sync... This feature allows you to manage groups in the cloud, while controlling access to on-premises applications and resources." This supports the chosen configuration for managing hybrid resource access.

Microsoft Entra documentation, "Review access to groups and applications in access reviews": In the section on reviewing access, it is noted that for groups synchronized from an on-premises AD, automatic removal via Access Reviews is not possible unless the group is a writeback-enabled group. This limitation necessitates the creation of new, cloud-mastered groups with writeback enabled to fulfill the automation requirement.

Question: 17

You are designing a security operations strategy based on the Zero Trust framework. You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts. What should you do?

A. Enable built-in compliance policies in Azure Policy.

B. Enable self-healing in Microsoft 365 Defender.

C. Automate data classification.

D. Create hunting queries in Microsoft 365 Defender.

Answer:

B

Explanation:

The most effective way to minimize the operational load on Tier 1 Security Operations Center (SOC) analysts is to enable self-healing capabilities. In Microsoft 365 Defender, this is achieved through Automated Investigation and Response (AIR). AIR automatically investigates alerts, determines if a threat is real, and takes remediation actions without manual intervention. This process significantly reduces the volume of alerts that Tier 1 analysts must manually triage, investigate, and remediate. By handling common and high-volume threats automatically, AIR allows analysts to focus their efforts on more complex and critical incidents, directly addressing the goal of reducing their operational load. This aligns with the Zero Trust principle of "assume breach" by enabling rapid, automated containment and response.

Why Incorrect Options are Wrong:

A. Enable built-in compliance policies in Azure Policy.
Azure Policy is a governance service for enforcing organizational standards and assessing resource compliance. It does not automate incident response or reduce the real-time alert queue for SOC analysts.
C. Automate data classification.
Automating data classification helps in prioritizing incidents by identifying alerts that involve sensitive data. While this improves efficiency, it does not reduce the overall number of alerts that need to be triaged.
D. Create hunting queries in Microsoft 365 Defender.
Threat hunting is a proactive, often manual, activity performed by experienced (Tier 2/3) analysts to find undetected threats. This task increases, rather than minimizes, the operational workload.

References:

1. Microsoft Learn, "Automated investigation and response (AIR) in Microsoft 365 Defender."
Reference: Under the section "How AIR works," the documentation states, "As security alerts are triggered, it's up to your security operations team to look into those alerts and take steps to protect your organization... To help with this deluge of alerts, Microsoft 365 Defender includes automated investigation and response (AIR) capabilities... AIR can save your security operations team time and effort..." This directly supports that AIR (self-healing) reduces the SOC workload.
2. Microsoft Learn, "Zero Trust adoption framework for SecOps."
Reference: In the "Automate" section of the implementation guidance, it recommends to "Automate response actions to the extent possible to improve the mean time to remediate (MTTR)." Enabling self-healing is a primary method for achieving this automation.
3. Microsoft Learn, "Overview of Azure Policy."
Reference: The overview states, "Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements." This confirms its purpose is governance and compliance, not incident response automation.
4. Microsoft Learn, "Overview of advanced hunting in Microsoft 365 Defender."
Reference: The documentation describes advanced hunting as "a query-based threat hunting tool... that lets you proactively inspect events... to locate threat indicators and entities." This defines it as a proactive, investigative tool, which is contrary to reducing the initial alert load for Tier 1 analysts.

Question: 18

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines. You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure. What should you recommend?

A. an Azure AD user account that has a password stored in Azure Key Vault

B. a group managed service account (gMSA)

C. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management
(PIM)

D. a managed identity in Azure

Answer:

D

Explanation:

The Microsoft Cloud Adoption Framework's DevSecOps best practices strongly advocate for eliminating secrets from CI/CD pipelines to reduce the attack surface. Managed identities provide an automatically managed identity in Azure Active Directory (Azure AD) for services like Azure DevOps. When used with a service connection configured for Workload Identity Federation, it allows the pipeline to authenticate to Azure resources without storing any passwords, client secrets, or certificates in Azure DevOps. This secret-less approach is the most secure and recommended method for service-to-service authentication, directly aligning with modern DevSecOps principles.

Why Incorrect Options are Wrong:

A. Using an Azure AD user account with a password, even in Key Vault, introduces a manageable secret that must be rotated and can be compromised. Best practice is to eliminate secrets entirely.
B. Group managed service accounts (gMSAs) are an on-premises Active Directory Domain Services (AD DS) identity type and are not designed for authenticating cloud services like Azure DevOps to Azure.
C. Azure AD Privileged Identity Management (PIM) is designed for just-in-time (JIT) access for human users, often requiring interactive approval or MFA, making it unsuitable for automated, non-interactive CI/CD pipelines.

References:

1. Microsoft Cloud Adoption Framework, DevSecOps controls, "Secure the pipeline" section: "Use service principals that have the minimum permissions required. Rotate secrets and certificates regularly. Better yet, use managed identities to remove the need for secrets and certificates." This directly recommends managed identities over secret-based methods.
Source: Microsoft Learn, learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#secure-the-pipeline
2. Azure DevOps Documentation, "Connect to Microsoft Azure by using an ARM service connection": This document describes the "Workload Identity federation" authentication method for service connections, stating, "Workload identity federation allows you to create a secret-free service connection in Azure Pipelines to Azure." This is the modern implementation that leverages managed identities or other workload identities.
Source: Microsoft Learn, learn.microsoft.com/en-us/azure/devops/pipelines/library/connect-to-azure?view=azure-devops#create-an-azure-resource-manager-service-connection-using-workload-identity-federation
3. Azure Active Directory Documentation, "What are managed identities for Azure resources?": "Managed identities for Azure resources is a feature of Azure Active Directory... You can use the identity to authenticate to any service that supports Azure AD authentication, without having any credentials in your code." This explains the fundamental benefit and purpose of managed identities, which is to eliminate credentials.

Source: Microsoft Learn, learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question: 19

DRAG DROP Your company wants to optimize ransomware incident investigations. You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach. Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

[image could not be rendered]

Answer:

Assess the current situation and identify the scope.

Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.

Identify the compromise recovery process.

Explanation:

The correct sequence aligns with the Microsoft Detection and Response Team (DART) incident response methodology, which prioritizes understanding the situation before acting.

• Assess the current situation and identify the scope: This is the immediate first step in any incident response. It involves initial triage to understand the extent of the compromise, which systems are affected, and the nature of the attack.

• Identify which LOB apps are unavailable: This is a crucial part of assessing the scope. It quantifies the business impact by pinpointing critical services that are down, which is essential for prioritizing response and recovery efforts.

• Identify the compromise recovery process: Once the scope and impact are understood, the focus shifts to planning the remediation. This involves identifying viable recovery options, such as restoring from backups, and defining the process to bring services back online safely.

The other actions, such as implementing new strategies or updating processes, are post-incident activities that occur after the immediate threat is contained and services are restored.

References:

Microsoft Security Blog, "Microsoft DART ransomware approach and best practices": This guide outlines the DART team's multiphased approach. Phase 1: Assess, Contain, and Control directly corresponds to the first two steps of assessing the situation and impact. Phase 2: Plan and Prepare for Recovery aligns with the third step of identifying the recovery process. (See sections

on "Phase 1" and "Phase 2").
Microsoft Learn, "Plan for ransomware and extortion incident response": This documentation emphasizes that the initial response phase involves "Assessing the business impact of the incident." This includes identifying which critical systems and line-of-business applications are affected before moving on to containment and recovery planning. (See the "Incident Response" section).

Question: 20

HOTSPOT You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. AJI the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent. You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks: • A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers • A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers What should you use for each risk? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

[image could not be rendered]

Answer:

1st Box: Soft delete

2nd Box: Multi-user authorization (MUA) by using Resource Guard

Explanation:

This solution applies a defense-in-depth strategy using Azure Backup's security features to mitigate specific ransomware risks.

• Deleted backups: The most direct protection against the malicious deletion of backup data is Soft delete. This feature ensures that when backups are deleted, the data isn't immediately purged. Instead, it's retained in a soft-deleted state for 14 days (by default), providing a critical window to recover the data before it's permanently lost. This directly counters an attacker's attempt to eliminate recovery options.

• Disabled backups: To prevent a single compromised administrator account from disabling future backups (a "Stop Protection" operation), Multi-user authorization (MUA) by using Resource Guard is the correct control. MUA enforces a separation of duties by requiring an action initiated by the Backup administrator to be approved by another user with security permissions (via the Resource Guard). This proactive measure prevents a single point of compromise from sabotaging backup policies.

References:

Microsoft Documentation, Azure Backup - "Soft delete for Azure Backup": This document explicitly states, "With soft delete, even if a malicious actor deletes a backup (or backup data is accidentally deleted), the backup data is retained for 14 additional days, allowing the recovery of that backup item with no data loss." This directly supports using soft delete to counter the risk of deleted backups.

Microsoft Documentation, Azure Backup - "Multi-user authorization for Azure Backup": This source details the operations protected by MUA. The list of protected critical operations includes "Modify protection" and "Stop backup," which align with the risk of "Disabled backups." The documentation clarifies that MUA adds an essential authorization layer to prevent such unauthorized changes.

Question: 21

For of an Azure deployment you are designing a security architecture based on the Microsoft Cloud Security Benchmark. You need to recommend a best practice for implementing service accounts for Azure API management. What should you include in the recommendation?

A. device registrations in Azure AD

B. application registrations m Azure AD

C. Azure service principals with certificate credentials

D. Azure service principals with usernames and passwords

E. managed identities in Azure

Answer:

E

Explanation:

The Microsoft Cloud Security Benchmark (MCSB) strongly recommends using managed identities for Azure resources wherever possible. Managed identities provide an automatically managed identity in Azure Active Directory (Azure AD) for services like Azure API Management. This approach is superior because it eliminates the need for developers to manage credentials (like secrets, passwords, or certificates) in code or configuration files. Azure handles the credential lifecycle, including rotation, which significantly enhances security and reduces operational overhead, aligning with modern security best practices for service-to-service authentication.

Why Incorrect Options are Wrong:

A. device registrations in Azure AD: Device registration is used to manage and secure end-user devices (e.g., laptops, mobile phones) accessing corporate resources, not for authenticating Azure services.
B. application registrations in Azure AD: While an application registration is a related concept, a managed identity is the specific, recommended implementation for a service's identity, abstracting away the underlying service principal and its credential management.
C. Azure service principals with certificate credentials: This is more secure than passwords but still requires manual or scripted management of the certificate lifecycle (creation, rotation, renewal), which managed identities handle automatically.
D. Azure service principals with usernames and passwords: This is the least secure method and is explicitly discouraged. Storing and managing passwords for service accounts introduces significant security risks, such as credential leakage.

References:

1. Microsoft Cloud Security Benchmark v1, Control IM-3: Securely manage application and service identities. The guidance states: "Use managed identities for Azure resources where the feature is available to access other resources. The credential of a managed identity is fully managed by the platform and protected from unauthorized access."
2. Microsoft Learn, "What are managed identities for Azure resources?". This document explains that managed identities are the recommended solution for service-to-service authentication as they eliminate the need for developers to manage credentials. It states, "You don't have to manage credentials. Credentials are not even accessible to you."
3. Microsoft Learn, "How to use managed identities in Azure API Management". This official documentation confirms the applicability and best practice for the specific service in the question. It states, "A managed identity from Azure Active Directory (Azure AD) allows your API Management instance to easily and securely access other Azure AD-protected resources... Azure manages this identity, so you don't have to provision or rotate any secrets."

Question: 22

HOTSPOT You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender You need to recommend a solution to meet the following requirements: • Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware • Automatically generate incidents when the IP address of a command-and control server is detected in the events What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

[image could not be rendered]

Answer:

1st: A threat intelligence connector

2nd: A threat detection rule

Explanation:

To integrate third-party security information, such as known malware or command-and-control server IP addresses, into Microsoft Sentinel, you must use a threat intelligence connector. These specialized data connectors are designed to ingest threat indicators from Threat Intelligence Platforms (TIPs) or other external feeds.

Once the threat intelligence data is in Sentinel, you need a mechanism to correlate it with your internal event logs. A threat detection rule (now called an analytics rule) performs this function. You configure a rule that queries your logs for matches against the imported threat indicators. When a match is found, such as traffic to a known malicious IP address, the rule automatically generates an alert and an incident for investigation.

References:

Microsoft. (2024). Understand threat intelligence in Microsoft Sentinel. Microsoft Learn. In the "Integrate threat intelligence with connectors" section, it states, "Microsoft Sentinel provides data connectors to ingest threat indicators from a wide variety of sources." This confirms the use of connectors for integration.
Microsoft. (2024). Use threat intelligence to detect threats in Microsoft Sentinel. Microsoft Learn. The document explains, "After you've imported threat indicators into Microsoft Sentinel... use the built-in analytics rules that match your threat indicators with your event logs... The name of the rule is Microsoft Security Threat Intelligence Analytics." This directly links analytics rules (threat detection rules) to generating incidents from threat intelligence data.

Question: 23

You have an Azure subscription that contains a Microsoft Sentinel workspace. Your on-premises network contains firewalls that support forwarding event logs m the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel. What should you include m the recommendation?

A. an Azure logic app

B. an on-premises Syslog server

C. an on-premises data gateway

D. Azure Data Factory

Answer:

B

Explanation:

To ingest Common Event Format (CEF) logs from on-premises devices into Microsoft Sentinel, the standard architecture involves a log forwarder. This forwarder is a dedicated Linux machine, which can be on-premises or an Azure VM, that functions as a Syslog server. The on-premises firewalls are configured to send their CEF-formatted Syslog messages to this server's IP address. The server, equipped with the Azure Monitor Agent (AMA) or the legacy Log Analytics agent, then parses these messages and forwards them securely to the Microsoft Sentinel workspace. This is the officially recommended method for connecting data sources that use the CEF standard without a dedicated connector.

Why Incorrect Options are Wrong:

A. an Azure logic app: Logic Apps are used for Security Orchestration, Automation, and Response (SOAR) workflows, not as a primary mechanism for high-volume log ingestion.
C. an on-premises data gateway: This gateway enables services like Power BI and Power Apps to connect to on-premises data sources; it is not used for forwarding Syslog logs to Sentinel.
D. Azure Data Factory: This is a large-scale data integration (ETL/ELT) service and is not the appropriate or efficient tool for real-time security log ingestion from Syslog sources.

References:

1. Microsoft Documentation, "Ingest Common Event Format (CEF) logs with the AMA connector": "To connect your CEF-supported appliance to Microsoft Sentinel, you need to deploy a server, known as the log forwarder... The log forwarder receives logs from your appliances over Syslog and forwards them to your Microsoft Sentinel workspace." This document details the setup of a Linux machine to act as this Syslog server/forwarder.

2. Microsoft Documentation, "Plan costs and understand Microsoft Sentinel pricing and billing": Under the "Data collection" section, it mentions, "For some data sources like Syslog, Common Event Format (CEF)... you are required to set up a Log Forwarder on an Azure virtual machine or an on-premises server." This confirms the requirement of a server acting as a Syslog forwarder.
3. Microsoft Documentation, "Connect data sources to Microsoft Sentinel": The overview for connecting external solutions often points to the use of Syslog or CEF via a log forwarder. For CEF, it states, "Connect your external solution using Common Event Format (CEF) to Microsoft Sentinel over Syslog." This directly links the CEF format to the Syslog protocol, which requires a Syslog server to receive the logs before forwarding.

Question: 24

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AO credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

A. an Azure AD enterprise application

B. a retying party trust in Active Directory Federation Services (AD FS)

C. Azure AD Application Proxy

D. Azure AD B2C

Answer:

A

Explanation:

To integrate a third-party Software as a Service (SaaS) application with Azure Active Directory (Azure AD) for Single Sign-On (SSO), the standard and recommended method is to configure it as an enterprise application within the Azure AD tenant. This process involves adding the application from the Azure AD gallery (if it's a pre-integrated app) or registering it as a non-gallery application. Once registered, you can configure SSO using protocols like SAML or OpenID Connect, assign users and groups, and apply Conditional Access policies to secure access. This provides a seamless authentication experience for users, allowing them to sign in with their existing Azure AD credentials.

Why Incorrect Options are Wrong:

B. a relying party trust in Active Directory Federation Services (AD FS): AD FS is an on-premises federation service. While it can enable SSO, it is not the direct, cloud-native solution for an Azure AD tenant integrating with a SaaS app.
C. Azure AD Application Proxy: This service is designed to provide secure remote access and SSO to on-premises web applications, not for integrating with external, cloud-based SaaS applications.
D. Azure AD B2C: This is a separate identity management service for customer-facing applications (Business-to-Consumer). It is used for managing consumer identities, not for employee access to corporate applications.

References:

1. Microsoft Learn Azure Active Directory Documentation: "What is application management in Azure Active Directory?". This document states, "Application management in Azure Active Directory (Azure AD) is the process of creating, configuring, managing, and monitoring applications in the cloud. When an application is registered in an Azure AD tenant, it's called an enterprise application." It further explains that this is the method for integrating SaaS applications.
2. Microsoft Learn Azure Active Directory Documentation: "Quickstart: Add an enterprise application". This guide details the steps for adding a SaaS application to Azure AD for SSO. Under the "Prerequisites" section, it clearly states the purpose: "To configure single sign-on for an application in your Azure AD tenant."
3. Microsoft Learn Azure Active Directory Documentation: "Remote access to on-premises apps through Azure AD Application Proxy". This document defines the purpose of Application Proxy: "Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications." This confirms it is not for SaaS app integration.
4. Microsoft Learn Azure Active Directory B2C Documentation: "What is Azure Active Directory B2C?". The overview states, "Azure Active Directory B2C is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day." This distinguishes its purpose from managing employee access.

Question: 25

HOTSPOT You have an Azure SQL database named DB1 that contains customer information. A team of database administrators has full access to DB1. To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information. You need to design a security strategy for D81. The solution must meet the following requirements: • When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record. • When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute. What should you include in the design? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

[image could not be rendered]

Explanation:

[image could not be rendered]

The security strategy requires two distinct controls for two different user roles:

• For the database administrators: The goal is to prevent even high-privilege users like DBAs from viewing sensitive data in plaintext. Always Encrypted achieves this by encrypting data within the client application before it's sent to the database. The encryption keys are managed by the client and are never exposed to the database engine or its administrators. This creates a clear separation between data owners and data managers, fulfilling the requirement.

• For the operators: The requirement is to show only a portion of the sensitive data (the last four digits). Dynamic Data Masking (DDM) is designed for this exact purpose. It works by obfuscating data in query results for specified users without changing the actual data stored in the database. A masking function can be applied to the Credit Card column to display it in the format xxxx-xxxx-xxxx-1234 for the operators' application user.

Transparent Data Encryption (TDE) is incorrect because it encrypts the entire database at rest but is transparent to authorized users like DBAs, who could still view the data. Row-Level Security (RLS) is incorrect as it filters which rows a user can see, rather than masking the data within a column.

References:

Microsoft. (2023). Always Encrypted - Azure SQL Database & SQL Managed Instance. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine
Reference Point: In the "Benefits" section, it states, "Always Encrypted enables clients to encrypt

sensitive data inside client applications and never reveal the encryption keys to the Database Engine... This provides a separation between those who own the data... and those who manage the data... but should have no access." This directly supports its use for protecting data from DBAs.

Microsoft. (2023). Dynamic Data Masking. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking

Reference Point: The documentation states, "Dynamic data masking (DDM) limits sensitive data exposure by masking it to non-privileged users... For example, a user in a call center may be able to identify a caller by several digits of their social security number or credit card number, but those data items shouldn't be fully exposed to the call center employee." This aligns perfectly with the requirement for operators.

Microsoft. (2024). Row-Level Security. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/sql/relational-databases/security/row-level-security

Reference Point: The introductory paragraph clarifies that RLS enables "control over access to rows in a database table... RLS simplifies the design and coding of security in your application. RLS helps you implement restrictions on data row access." This confirms it is for row filtering, not column masking.

Question: 26

You have a Microsoft 365 subscription. You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices. Which two services should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Cloud Apps

B. Azure AD Application Proxy

C. Azure Data Catalog

D. Azure AD Conditional Access

E. Microsoft Purview Information Protection

Answer:

A, D

Explanation:

This solution requires a two-part mechanism. First, Azure AD Conditional Access is used to identify the context of the access attempt. A policy is configured to target users accessing SharePoint Online from devices that are not hybrid Azure AD joined or marked as compliant (i.e., unmanaged). Second, instead of blocking access entirely, the Conditional Access policy redirects the session to Microsoft Defender for Cloud Apps by using the "Use Conditional Access App Control" session control. Defender for Cloud Apps then acts as a reverse proxy, applying a session policy specifically configured to monitor the user's activity and block any file download attempts, thus fulfilling the requirement without completely blocking access to the application.

Why Incorrect Options are Wrong:

B. Azure AD Application Proxy: This service is used to provide secure remote access to on-premises web applications, not for controlling access to cloud services like SharePoint Online.
C. Azure Data Catalog: This is a data governance service for data source discovery and metadata management. It is not involved in real-time access control or session policies.
E. Microsoft Purview Information Protection: This service classifies and protects documents and emails by applying labels and encryption. While it can protect data after download, it does not natively block the download action based on device state.

References:

1. Microsoft Learn, "Protect with Microsoft Defender for Cloud Apps Conditional Access App Control": This document states, "Conditional Access App Control enables you to monitor and control user app access and sessions in real time... For example, if a user is on an unmanaged

device... you can block them from downloading sensitive files." It further explains the integration: "Conditional Access App Control... is uniquely integrated with Azure AD Conditional Access." (See the "How it works" section).
2. Microsoft Learn, "Deploy Conditional Access App Control for featured apps": This guide details the prerequisite steps, which include configuring an identity provider (Azure AD) and then creating the necessary policies. It explicitly shows how a Conditional Access policy is the entry point that routes traffic to Defender for Cloud Apps for session control. (See the "Prerequisites" and "To deploy Conditional Access App Control for SharePoint" sections).
3. Microsoft Learn, "Create session policies in Microsoft Defender for Cloud Apps": This document describes how to create the policy that performs the action. Under the "To create a new session policy" section, it lists "Block download" as a "Session control type" and provides a template named "Block download based on real-time content inspection." This policy is applied after the session is routed from Azure AD Conditional Access.

Question: 27

You have an Azure subscription. Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions. What should you recommend using to enforce the governance requirement?

A. regulatory compliance standards in Microsoft Defender for Cloud

B. custom Azure roles

C. Azure Policy assignments

D. Azure management groups

Answer:

C

Explanation:

Azure Policy is the native Azure service designed to create, assign, and manage policies that enforce rules and effects over your resources. To meet the governance requirement of restricting resource creation to specific regions, you can use the built-in "Allowed locations" policy definition. By creating a policy assignment at the subscription scope and configuring it to allow only 'West Europe' and 'North Europe' with the Deny effect, any attempt to create a resource in a non-approved region will be blocked, thus enforcing the requirement.

Why Incorrect Options are Wrong:

A. regulatory compliance standards in Microsoft Defender for Cloud: Defender for Cloud assesses and reports on compliance against standards; it does not directly enforce resource creation rules like location restrictions.
B. custom Azure roles: Azure roles (RBAC) control user permissions and actions (the 'what'), not the configuration or properties (like location) of the resources being created.
D. Azure management groups: Management groups are a scoping mechanism used to apply policies and access controls across multiple subscriptions, but they do not enforce rules themselves. The policy is the enforcement tool.

References:

1. Microsoft Learn, "What is Azure Policy?": This document states, "Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources... Common use cases for Azure Policy include... requiring resources to be deployed to specific Azure regions."
Source: Microsoft Documentation, "Overview of Azure Policy".
2. Microsoft Learn, "Tutorial: Create and manage policies to enforce compliance": This tutorial uses the "Allowed locations" policy as a primary example of enforcing organizational standards. It

demonstrates assigning the policy with a Deny effect to block resource creation outside of the specified locations.
Source: Microsoft Documentation, "Tutorial: Create and manage policies to enforce compliance", Section: "Assign a policy".
3. Microsoft Learn, "Azure Policy and role-based access control": This document clarifies the distinction: "Role-based access control focuses on user actions at different scopes... Azure Policy focuses on resource properties during deployment and for already existing resources." This confirms that RBAC is incorrect for controlling resource properties like location.
Source: Microsoft Documentation, "Compare Azure Policy and role-based access control".
4. Microsoft Learn, "Organize your resources with Azure management groups": This document explains that management groups provide a scope above subscriptions for applying governance controls. It states, "You can apply policies to a management group that limits the regions where virtual machines (VMs) can be created." This highlights that the management group is a target for the policy, but the policy itself is the enforcement mechanism.
Source: Microsoft Documentation, "What are Azure management groups?".

Question: 28

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements: • Users must be able to request access to App1 by using a self-service request. • When users request access to App1, they must be prompted to provide additional information about their request. • Every three months, managers must verify that the users still require access to Appl. What should you include in the design?

A. Azure AD Application Proxy

B. connected apps in Microsoft Defender for Cloud Apps

C. Microsoft Entra Identity Governance

D. access policies in Microsoft Defender for Cloud Apps

Answer:

C

Explanation:

Microsoft Entra Identity Governance is the suite of capabilities designed to manage the identity and access lifecycle. It directly addresses all the requirements. Entitlement management, a feature within Identity Governance, allows the creation of access packages for applications like App1. These packages enable self-service requests. You can configure these requests to include custom questions to gather justification. Furthermore, the Access Reviews feature allows for scheduling recurring campaigns (e.g., quarterly) where managers must review and recertify their direct reports' continued need for access, ensuring the principle of least privilege is maintained over time.

Why Incorrect Options are Wrong:

A. Azure AD Application Proxy is used to publish on-premises web applications for secure remote access, which is not the scenario described.
B. Connected apps in Microsoft Defender for Cloud Apps are for discovering, monitoring, and governing cloud app usage, not for managing the access request and review lifecycle.
D. Access policies in Microsoft Defender for Cloud Apps control user sessions in real-time (e.g., block downloads), but do not manage the initial access request or periodic recertification process.

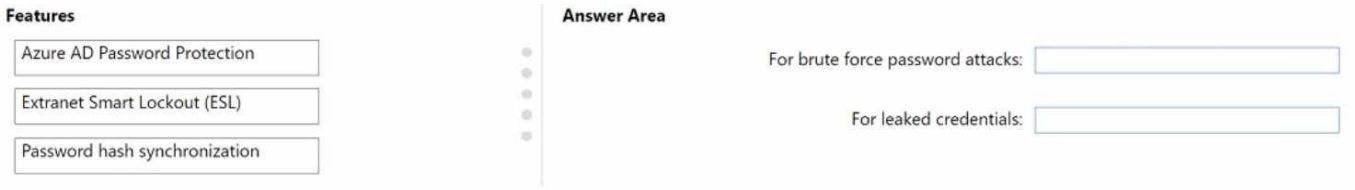
References:

1. Microsoft Entra Identity Governance: "Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources... Key features include Entitlement management and Access reviews."

Source: Microsoft Learn, "What is Microsoft Entra ID Governance?", Section: "What can you do with Microsoft Entra ID Governance?".
2. Entitlement Management (Self-Service & Custom Questions): "Microsoft Entra entitlement management can help you manage access to groups, applications, and SharePoint sites for internal users and also for users outside your organization... You can also configure questions that requestors must answer."
Source: Microsoft Learn, "What is Microsoft Entra entitlement management?", Section: "What can I do with entitlement management?".
3. Access Reviews (Manager Verification): "Microsoft Entra access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access... You can ask reviewers (such as business owners or the users themselves) to attest to (or certify) users' need for access."
Source: Microsoft Learn, "What are Microsoft Entra access reviews?", Section: "Why are access reviews important?".
4. Azure AD Application Proxy: "Microsoft Entra application proxy provides secure remote access to on-premises web applications. After a single sign-on to Microsoft Entra ID, users can access both cloud and on-premises applications through an external URL or an internal application portal."
Source: Microsoft Learn, "Remote access to on-premises applications through Microsoft Entra application proxy", Introduction paragraph.

Question: 29

DRAG DROP You have a hybrid Azure AD tenant that has pass-through authentication enabled. You are designing an identity security strategy. You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities. What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.



Explanation:

For brute force password attacks: Extranet Smart Lockout (ESL)

• Extranet Smart Lockout (ESL) is the direct mechanism designed to protect against password spray and brute-force attacks by intelligently locking out attackers based on risk signals (like unfamiliar locations), while allowing legitimate users to continue signing in. ESL (or its successor, Azure AD Smart Lockout, which integrates with P TA) prevents the cloud attacker from causing an account lockout on the sensitive on-premises AD where the password verification happens with PTA.

For leaked credentials: Azure AD Password Protection

• Azure AD Password Protection prevents users from setting passwords that are known to be compromised or are on a globally banned list of weak passwords. By preventing the use of passwords already found in data breaches, it directly minimizes the impact of attackers attempting to use leaked credentials against your users. This protection can be extended to the on-premises AD to work with PTA.

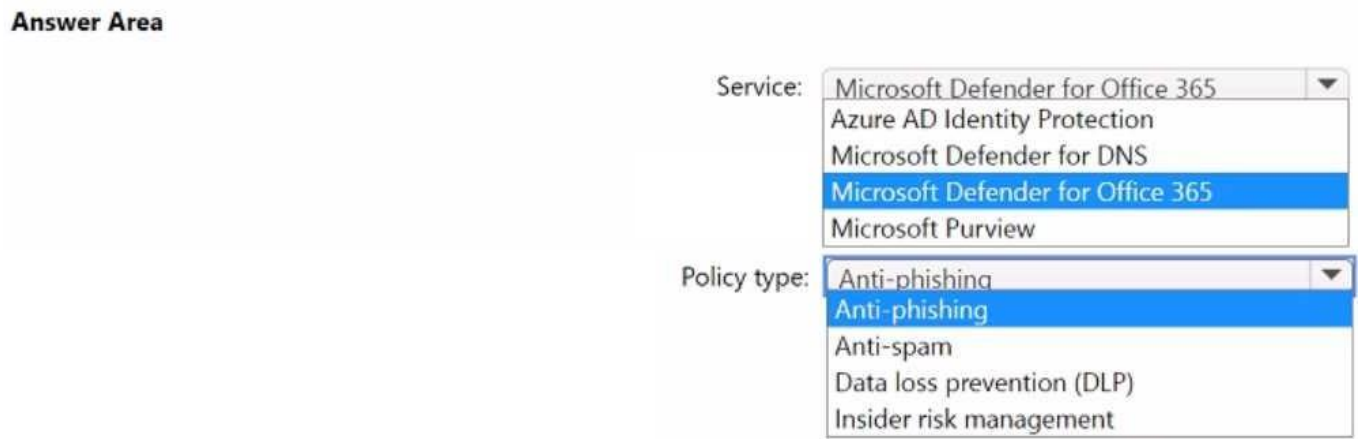
References:

Azure AD Smart Lockout (for Brute Force Mitigation):
Source: Microsoft Learn, "Prevent attacks using smart lockout."
Detail: "Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in... Smart lockout can be integrated with hybrid deployments that use... pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers." (Conceptual documentation on the feature's role).

Azure AD Password Protection (for Leaked Credential Mitigation):
Source: Microsoft Learn, "Enforce Azure AD Password Protection."
Detail: "Azure AD Password Protection detects and prevents the use of passwords that are known to be compromised, helping to minimize the impact of leaked or weak credentials." (Conceptual documentation section on purpose).
Hybrid Identity Security Principles:
Source: Microsoft Learn, "Steps to secure identities."
Detail: Lists the primary defenses against password attacks, classifying Smart Lockout as the tool for mitigating high-volume sign-in attacks and Password Protection (banned passwords) as the tool for mitigating dictionary and known compromised credentials.

Question: 30

HOTSPOT You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online. You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders. What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Explanation:

Microsoft Defender for Office 365 is the dedicated security service for protecting collaboration tools, including Exchange Online, from advanced threats. To prevent malicious actors from impersonating internal senders, you must configure an Anti-phishing policy. This specific policy type includes settings to combat impersonation attacks by allowing administrators to specify internal users (e.g., executives) and domains to protect. When an incoming email appears to be from one of these protected users or domains but originates from an external source, the policy applies protective actions, such as quarantining the message or tagging it as suspicious.

References:

Microsoft Learn. (2024). Anti-phishing policies in Microsoft 365. Microsoft Docs. In the section "Impersonation settings in anti-phishing policies in Microsoft Defender for Office 365," it states, "Impersonation is where the sender of an email message looks like a legitimate or expected sender...Impersonation settings are available in anti-phishing policies in Microsoft Defender for Office 365."

Microsoft Learn. (2024). Impersonation settings in anti-phishing policies in Microsoft Defender for

Office 365. Microsoft Docs. This document details the specific configurations for user and domain impersonation protection within Defender for Office 365 anti-phishing policies. It explicitly states, "In anti-phishing policies in Microsoft Defender for Office 365, you can configure impersonation protection to protect specified recipients from phishing attacks."